ZealiD Privacy Policy
EN 2026 v 2.20

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
2026-03-11	2.20	Updates on guide, products and wording..	PH

ZealiD

ZealiD

Reader's Guide — At a Glance

The table below gives a complete overview of every context in which ZealiD processes personal data: what data is collected, the legal reason, how long it is kept, and where in this document to find the full explanation. For the Trust Service specifically, processing is mandated by law (eIDAS + ETSI standards) — not a choice ZealiD makes freely. Each row links to the relevant section.

Service / Context	What data ZealiD collects	Why / Legal basis	How long kept	Section
Trust Service – Identity registration (ZealiD QeID)	Full name, date of birth, gender, nationality Government ID document (type, country, number, authority, dates) Personal identity number Biometric data: facial image, liveness facemap, NFC signature Email, mobile number Session / device data	Required by law: eIDAS Regulation (EU 910/2014) + ETSI EN 319 401, EN 319 411-1/2, TS 119 461 Lawful basis: Art. 6(1)(c) GDPR (legal obligation) + Art. 6(1)(a) / Art. 9(2)(a) (explicit consent for biometric data)	Failed application: 30 days Active certificate: 12 years after expiry Revoked certificate: 14 years from revocation OCSP records: 15 years	**§ 2**
ZealiD Trust Circle (formerly my.zealid.com)	**As controller:** Account data (name, work email, role), session logs, device data **As processor (on customer instructions):** KYC/identity verification data for end-users; customer portal access data; document content (sharing / signing workflows); local hosting instance data	**As controller:** Art. 6(1)(b) contract + Art. 6(1)(f) legitimate interest **As processor:** Customer's instructions under Art. 28 GDPR data processing agreement	Account data: duration of customer relationship + 1 year Processor data: per customer DPA + CPS floors	**§ 3**
Microsoft Entra Verifiable Credential Wallet	Derived from already-verified identity (no new document collection) VC issuance log (subscriber ID, timestamp, credential type)	Consent + contract performance Art. 6(1)(a) and 6(1)(b) GDPR Privacy by design: selective disclosure — relying parties receive only the attributes they request	Per Trust Service certificate lifecycle (§ 2.4)	**§ 4**

Website (www.zealid.com)	IP address (truncated), browser type, device OS, pages visited, approximate geolocation, referrer, session counts Collected only with opt-in consent	Consent + legitimate interest (service security) Art. 6(1)(a) and 6(1)(f) GDPR	26 months from last visit	**§ 5**
Mobile App (analytics / performance)	Connection ID, language, document issuing country, device type, registration and usage events	Legitimate interest (service quality)	26 months	**§ 6**
Document signing (ZealiD as processor)	Content of documents uploaded, shared, or submitted for signing (incl. third-party upload requests) — processed on the uploading/sharing user's behalf only	Uploading/sharing user is data controller (where so categorised under GDPR) ZealiD acts as data processor under Art. 28 GDPR	Per customer's instructions + certificate lifecycle	**§ 8**
Employees, Job Applicants, Subcontractors	Name, ID, address, qualifications, payroll data, performance data Job applicants: CV, ID copy, contact details	Legal obligation + contractual necessity + consent Art. 6(1)(b), 6(1)(c) GDPR	Employees: per labour / tax law Applicants: 1 year from rejection Subcontractors: per contract	**§ 7**

Why the Trust Service is Different

The ZealiD Trust Service (qualified certificates, qualified electronic signatures, identity verification) is a regulated trust service under eIDAS. This means the processing of personal data within the Trust Service is not optional — it is defined and required by the eIDAS Regulation and the ETSI standards to which ZealiD is certified. ZealiD cannot issue a Qualified Electronic Certificate without first verifying, to a level of assurance equivalent to in-person identification, that the subscriber is the person they claim to be. That verification requires biometric data.

The non-regulated services — ZealiD Trust Circle, the website, the mobile app analytics layer, and the Verifiable Credential wallet — are governed by GDPR in the conventional sense. Consent can be withdrawn, retention periods are shorter, and no biometric data is collected beyond what the Trust Service registration already captured.

- If you are asking why ZealiD holds your biometric data: because eIDAS and ETSI TS 119 461 require it for the issuance of a Qualified Electronic Certificate. The legal basis is Art. 6(1)(c) GDPR (legal obligation) in combination with Art. 9(2)(a) (explicit consent for biometric processing).
- If you are asking why ZealiD cannot delete your data immediately upon request: because the evidence package supporting a qualified electronic signature must be retained for the validity period of that signature — up to 12 years — so that the

signature remains verifiable by relying parties. ZealiD is legally prohibited from destroying this evidence early.
- If you are asking about your data on the Trust Circle platform, the website, or the VC wallet: standard GDPR rights apply in full. Contact dpo@zealid.com.

Legal References

Instrument	Relevance to ZealiD data processing
eIDAS Regulation (EU No 910/2014)	Primary legal basis for the ZealiD Trust Service. Defines requirements for qualified trust services, qualified electronic certificates, and qualified electronic signatures. Mandates identity proofing at face-to-face equivalent assurance level.
ETSI EN 319 401	General policy requirements for all Trust Service Providers. Governs ZealiD's information security, personnel, records, and operational practices.
ETSI EN 319 411-1 ETSI EN 319 411-2	Policy and security requirements for certificate-issuing TSPs. Part 2 covers requirements for EU qualified certificates specifically.
ETSI TS 119 461	Identity proofing requirements for trust service subjects. Defines the minimum data that must be collected and verified during subscriber registration.
ETSI TS 119 431-1	Requirements for TSPs operating a remote qualified signature creation device (QSCD), which ZealiD uses to provide qualified signatures via the mobile app.
GDPR (EU 2016/679)	Primary data protection law applicable to all ZealiD processing. Governs lawful bases, data subject rights, retention, security, and the DPO requirement. The Trust Service relies primarily on Art. 6(1)(c) (legal obligation) and Art. 9(2)(a) (explicit consent for biometric data). Non-regulated services rely on Art. 6(1)(a) (consent) and 6(1)(b) (contract).
NIS2 Directive (EU 2022/2555)	Cybersecurity obligations applicable to ZealiD as a trust service provider. Informs ZealiD's information security measures and incident reporting requirements.
Swedish law (SFS)	ZealiD is incorporated in Sweden and subject to Swedish implementation of GDPR and applicable employment, tax, and corporate law.
TüV Nord certification (audit ref. 97267)	Conformity assessment by TüV Nord confirms ZealiD's compliance with the above ETSI standards. Audit covers ETSI EN 319 401, EN 319 411-1, EN 319 411-2, and EN 119 431-1. Supervised by PTS.

The full and authoritative description of data processing for the Trust Service is in the ZealiD TSPS (v19) and CPS (v23), available at www.zealid.com/repository. This Privacy Policy summarises those obligations but does not replace them. In the event of any conflict, the TSPS and CPS prevail for Trust Service processing.

A note on how this document is structured. ZealiD operates two distinct types of service, and the rules governing personal data processing differ meaningfully between them.

- The ZealiD Trust Service (qualified certificates, electronic signatures, timestamping, and identity verification) is a regulated service. The processing of personal data within this service is defined by law — primarily the eIDAS Regulation (EU No 910/2014) and its implementing acts — and by the technical and procedural

standards to which ZealiD is certified (ETSI EN 319 401, EN 319 411-1, EN 319 411-2, EN 119 431-1). The detailed rules, data categories, lawful bases, and retention periods applicable to the Trust Service are set out in the ZealiD Trust Service Practice Statement (TSPS) and Certificate Practice Statement (CPS), both publicly available at www.zealid.com/repository. This Privacy Policy summarises those obligations but the TSPS and CPS are the authoritative instruments.

- The ZealiD Platform (ZealiD Trust Circle, formerly my.zealid.com), the ZealiD Website (www.zealid.com), and the Microsoft Entra Verifiable Credential wallet feature are non-regulated products or services in the conventional sense. Processing of personal data in these contexts is governed by GDPR and explained in full in sections 5, 6 and 7 of this document.

Where a user question relates to why ZealiD collects particular data during identity verification or certificate issuance, the answer is: because it is required to do so by eIDAS and the ETSI standards to which ZealiD is certified. This Privacy Policy and the supporting TSPS/CPS provide the full legal and technical explanation.

1. General

ZealiD AB (registration no. 556972-4288, Norrlandsgatan 10, 111 56 Stockholm, Sweden) is a Qualified Trust Service Provider (QTSP) supervised by PTS (Post- och Telestyrelsen) under the eIDAS Regulation and certified by TüV Nord as a conformity assessment body against ETSI standards.

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

This Privacy Policy covers all contexts in which ZealiD processes personal data about individuals who interact with ZealiD in any capacity: subscribers to the Trust Service, users of the ZealiD Platform and mobile app, visitors to www.zealid.com, job applicants, employees, and counterparties. It does not cover processing carried out by third-party services or partners.

All capitalised terms in this document carry the meanings given to them in the TSPS and CPS. Both documents are available at www.zealid.com/repository.

1.1. Data Controller

The data controller for all personal data collected directly by ZealiD is ZealiD AB, Norrlandsgatan 10, 111 56 Stockholm, Sweden.

Where ZealiD processes personal data on behalf of a customer (e.g. when a customer uploads documents for signing), ZealiD acts as data processor and the customer is the data controller. In those cases, any data subject requests should be directed to the relevant customer.

1.2. Data Protection Officer

ZealiD has a Data Protection Officer (DPO) appointed and registered with Swedish IMY. The DPO leads data protection activities and works closely with Compliance, IT Security, and the Management Board.

DPO contact: dpo@zealid.com

2. ZealiD Trust Service — Why Certain Data Processing is Required by Law

This section addresses the most common question ZealiD receives: why does ZealiD collect so much personal data, including biometric data, during the registration and certificate issuance process?

The short answer is: because the law requires it.

2.1. The Legal Framework

ZealiD's Trust Service is governed by:

Regulation (EU) No 910/2014 (eIDAS), which establishes the requirements for qualified trust services including qualified electronic signatures (QES) and qualified electronic certificates;

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers);
- ETSI EN 319 411-1 and EN 319 411-2 (Policy and Security Requirements for Certificate-issuing TSPs);
- ETSI TS 119 461 (Identity Proofing of Trust Service Subjects);
- ETSI TS 119 431-1 (Policy and Security Requirements for TSPs operating a remote QSCD).

ZealiD is certified against all of these standards by TüV Nord as conformity assessment body, and is supervised by PTS.

To issue a Qualified Electronic Certificate, ZealiD must verify, with a level of assurance at least equivalent to an in-person face-to-face identification, that the subscriber is who they claim to be. This cannot be achieved without collecting and verifying identity documents and biometric data.

The detailed obligations, data categories, lawful bases, and retention schedules applicable to the Trust Service are set out in full in the TSPS (v19 or later) and CPS (v23 or later), both available at www.zealid.com/repository. This Privacy Policy summarises those rules; the TSPS and CPS are the primary instruments.

2.2. Personal Data Processed in the Trust Service

During registration (identity proofing) and certificate issuance, ZealiD collects and processes the following data categories:

- Full name, date of birth, gender, nationality
- Government-issued national identity document (type, country, number, issuing authority, issue date, expiry date)
- Personal identity number (personal number, document number, or tax identification number)
- Biometric picture and signature on identity document; facial image (liveness check); facial map (facemap); NFC signature and validation result (where NFC chip is present)
- Email address and mobile phone number
- Session data (device type, timestamps, transaction identifiers)

All verification steps and results are logged and retained by ZealiD in its own backend infrastructure, solely within ZealiD-controlled servers.

Anonymity and pseudonymity are not permitted for the Trust Service. All names must be real and verified.

2.3. Special Categories of Data (GDPR Article 9)

The processing of identity document images and selfie/liveness data constitutes processing of biometric data for the purpose of uniquely identifying a natural person, which falls within the special categories of personal data under GDPR Article 9.

ZealiD processes this data on two legal grounds:

- Article 9(2)(a) GDPR: the subscriber has given explicit consent, freely, specifically, and in an informed manner, through the ZealiD mobile app prior to commencing registration; and
- Necessity under applicable law: eIDAS and the ETSI standards require identity proofing at a level equivalent to face-to-face verification, which cannot be achieved without biometric verification.

Automated decision-making applies during the registration process (age verification, document validity check, liveness verification, NFC validation where applicable). Subscribers are informed of the outcome and may request human review in accordance with the TSPS.

Security measures for special category data include: minimised access controls, mandatory two-factor authentication for all personnel with access to evidence packages, and encryption of all evidence packages at rest and in transit. Further details are in the CPS and TSPS.

2.4. Lawful Bases and Retention

The table below summarises the main processing activities in the Trust Service. The full and authoritative schedule is in the TSPS and CPS.

Applicants (registration attempt, unsuccessful): Consent + legal obligation. Retained for 30 days from application date.

Subscribers (certificates issued): Consent + legal obligation. Retained for at least 12 years after the certificate expires; audit logs for 10 years; archived records (including evidence package) for at least 12 years after certificate validity. OCSP records retained for 15 years.

Subscribers whose certificate was revoked: Consent + legal obligation. Retained for 14 years from revocation date.

Users of ID verification by Money Transfer Service: Consent. Transfer data retained 30 days; subscriber relationship data retained 2 years.

Note: Retention periods reflect ZealiD's obligations under eIDAS to maintain evidence of certificate issuance and revocation for as long as signatures produced using those certificates remain legally valid. ZealiD cannot unilaterally shorten these periods.

2.5. Consent and its Limitations in the Trust Service

ZealiD's services are designed with GDPR by design and by default in mind. Registration cannot proceed without active consent at each stage in the ZealiD mobile app.

However, once a Qualified Electronic Certificate has been issued, the consent to retain supporting data cannot in all cases be fully withdrawn. This is because:

- The evidence package underpinning a qualified electronic signature must be retained for the duration of the signature's validity (up to 12 years) so that the signature can be validated by relying parties;
- ZealiD is legally required to maintain records of certificate issuance and revocation;
- Key pairs and certificates are archived as part of ZealiD's mandatory backup and continuity procedures.

A subscriber may request revocation of their certificate at any time via www.zealid.com/en/revocation. Revocation does not delete retained data but terminates the certificate's validity.

3. ZealiD Trust Circle (Formerly my.zealid.com)

ZealiD Trust Circle (formerly my.zealid.com) is a web-based platform for businesses and organisations that use ZealiD's identity and trust services. It enables customers to identify and KYC their own end-users, set up branded customer portals, share documents, upload documents for qualified electronic signing, and — where contractually agreed — deploy a locally hosted instance of the platform within the customer's own infrastructure. This section covers personal data processed by ZealiD in connection with the Trust Circle platform, distinct from the Trust Service registration and certificate lifecycle (Section 2).

3.1. Platform Features and Associated Data Processing

3.1.1. Identity Verification and KYC of End-Users

Customer organisations use Trust Circle to trigger identity verification and Know Your Customer (KYC) checks on their own end-users via the ZealiD TRA Service. In this workflow:

- The customer organisation is the data controller for their end-user's personal data. ZealiD acts as data processor performing the identity verification on the customer's behalf, under a written data processing agreement (Art. 28 GDPR).
- Data collected during verification follows the same categories as the TRA Service (Section 2.2): identity document data, biometric image, liveness facemap, personal identity number, contact details. Where the extended KYC ("KYC Extension") API is used, additional data fields may be transmitted to the customer as contractually specified.
- End-users who have questions about how their data is used in the context of a customer's KYC process should contact that customer organisation directly. ZealiD will forward any misdirected data subject requests to the relevant customer.

3.1.2. Customer Portals

Customers may configure a branded portal within Trust Circle for their own end-users. Personal data processed in connection with portal access (account credentials, access logs, session identifiers) is processed by ZealiD as data processor on behalf of the customer, under the applicable Art. 28 GDPR data processing agreement. The customer determines the purposes and means of processing within their portal.

3.1.3. Document Sharing and Upload for Signing

Trust Circle enables two related document workflows: sharing documents with other users, and uploading documents for qualified electronic signing (including inviting other parties to sign or upload). In both cases, the user who uploads or shares the document — to the extent that user is acting as a data controller under GDPR in relation to any personal data contained in those documents — bears the responsibilities of data controller for that personal data. ZealiD processes document content solely as a data processor acting on that user's instructions, under the applicable Art. 28 GDPR data processing agreement.

This applies equally where the uploading user invites a third party to view, sign, or upload documents in response — the initiating user remains responsible as data controller for the personal data they have caused to be processed. Users should ensure they have a lawful basis for sharing or processing any personal data of others through these workflows before doing so.

ZealiD retains document metadata (upload timestamp, document identifier, signing status) and signing event logs for the duration required by the certificate lifecycle rules in the CPS (Section 2.4). Document content is retained only for the period instructed by the data controller and specified in the data processing agreement.

3.1.4. Local Hosting Option

Where contractually agreed, a customer may deploy a locally hosted instance of the Trust Circle platform within their own IT infrastructure. In this configuration:

- Personal data processed within the customer's locally hosted instance is processed on infrastructure controlled by the customer. The customer is the data controller for all such processing. ZealiD's role is limited to providing and maintaining the software.
- Where the local instance connects back to ZealiD's Trust Service infrastructure (e.g. for certificate issuance or OCSP validation), the data flows relevant to those operations are governed by Section 2 of this Privacy Policy and the TSPS/CPS.
- The customer's responsibilities as data controller, including their own data subject rights obligations, are set out in the local hosting agreement and the applicable data processing agreement.

3.2. Personal Data Processed by ZealiD as Controller (Trust Circle)

In connection with the Trust Circle platform itself (as distinct from customer-instructed processing), ZealiD processes the following data as data controller:

- Account data of customer organisation representatives: name, work email, role, login timestamps
- Platform usage logs: session identifiers, connection IDs, feature usage events, Customer Care interactions
- Device data: type of device, browser, language preference, operating system

3.3. Lawful Basis and Retention

ZealiD as controller (platform account and usage data): Art. 6(1)(b) GDPR (contract performance) + Art. 6(1)(f) (legitimate interest in platform security and improvement). Retained for the duration of the customer relationship and for 1 year thereafter, or as required by applicable law.

ZealiD as processor (identity verification, customer portal, document signing, local hosting): Processing is on the customer's instructions under Art. 28 GDPR. Retention follows the customer's data processing agreement, subject to the minimum retention floors imposed by the CPS for signing-related evidence (Section 2.4).

3.4. Cookies in ZealiD Trust Circle

ZealiD Trust Circle uses cookies and similar local storage technologies to provide and secure the platform. The full list of cookies in use, their purpose, provider, and lifetime is maintained in ZealiD's Cookie List, which is accessible from the Trust Circle platform interface and reviewed at least annually. The following two categories apply:

- **Strictly necessary cookies.** These are set automatically and cannot be disabled. They are required for authentication, session management, security (CSRF protection, fraud prevention), and basic platform functionality. Without these cookies the platform cannot operate. Lawful basis: Art. 6(1)(b) GDPR (contract performance) / Art. 6(1)(f) (legitimate interest in platform security). These cookies are set by ZealiD and do not involve third-party processors beyond ZealiD's authorised hosting infrastructure.
- **Optional cookies.** These are set only with your consent via the cookie consent banner displayed on first access to Trust Circle. They include analytics and performance cookies that help ZealiD understand how the platform is used and improve its features. You may withdraw consent at any time from the cookie settings accessible within the platform. Withdrawing consent will not affect cookies already set prior to withdrawal. Lawful basis: Art. 6(1)(a) GDPR (consent). The full list of optional cookies, including third-party providers and cookie lifetimes, is in the Cookie List.

3.5. International Data Transfers

ZealiD processes and stores all personal data within the European Economic Area (EEA). ZealiD's primary data centre infrastructure is located in Sweden (Bahnhof AB data centre, Stockholm). No personal data processed through the Trust Circle platform or the Trust Service is transferred to, or accessible from, countries outside the EEA as part of ZealiD's standard operations.

In the event that any future change to ZealiD's infrastructure, sub-processors, or service delivery would involve a transfer of personal data outside the EEA, ZealiD will ensure that an appropriate safeguard under GDPR Chapter V is in place before any such transfer occurs — whether an adequacy decision under Art. 45, standard contractual clauses under Art. 46(2)(c), or another approved mechanism. Affected data subjects will be informed of material changes in accordance with Section 12 of this Privacy Policy.

4. Microsoft Entra Verifiable Credential Wallet

ZealiD offers subscribers the option to receive, manage, and present Verifiable Credentials (VCs) through a Microsoft Entra-compatible digital wallet. This feature enables subscribers to hold a digitally verifiable representation of their verified identity, which can be presented to third parties (relying parties) without sharing the underlying identity document data.

4.1. How It Works

When a subscriber elects to use the Verifiable Credential feature:

- ZealiD issues a Verifiable Credential derived from the subscriber's already-verified identity data (verified during Trust Service registration). No additional identity document data is collected at this stage.
- The VC is stored in the subscriber's Microsoft Entra wallet on their device. ZealiD does not retain the private keys associated with the VC; key material is held by the subscriber's wallet.
- When the subscriber presents a VC to a relying party, the transaction is subscriber-initiated and subscriber-controlled. ZealiD's role is limited to issuing the credential and, where required, providing a verification endpoint.
- ZealiD retains a log of VC issuance events (subscriber identifier, issuance timestamp, credential type) for audit and legal purposes, consistent with the retention schedule in Section 2.4.

4.2. Data Minimisation

The VC architecture is designed to support selective disclosure: relying parties receive only the specific attributes they require (e.g. proof of age over 18, nationality) without receiving the full identity document data. This is a privacy-by-design feature of the service.

4.3. Microsoft Entra

The wallet component is provided by Microsoft via Microsoft Entra Verified ID. Microsoft processes data as a data processor under its own agreements and privacy terms. ZealiD has a data processing agreement in place with Microsoft governing the relevant processing. Subscribers who use the wallet feature should also review Microsoft's privacy documentation.

5. Website (www.zealid.com)

This section covers processing of personal data in connection with visits to www.zealid.com only. It does not apply to the Trust Service or the Platform.

5.1. Analytics

When you visit www.zealid.com, ZealiD uses Google Analytics, Hubspot, and Hotjar to collect standard internet log information and visitor behaviour data (page visits, session counts, device type, approximate geolocation, referrer, browser type, time zone). This data is processed in a way that does not directly identify individual visitors. No attempt is made to identify visitors. Data is collected only where visitors opt in via the cookie consent tool. Analytics data is retained for 26 months from the visitor's last visit.

5.2. Cookies

ZealiD uses cookies for navigation, authentication, session management, and service improvement. Cookies necessary for functionality and security are set without consent. Optional analytics cookies are set only with consent via the cookie consent tool on the website. You may withdraw consent at any time via the tool or through your browser settings, though this may affect service functionality. Third-party cookies set by embedded services (e.g., analytics providers) are subject to those providers' own policies.

5.3. Security and Performance

ZealiD uses a web application firewall (Hubspot) to monitor and protect website traffic. This service processes traffic data in real time to detect and block malicious behaviour in accordance with OWASP Top 10 guidelines. Traffic data is retained for 26 months.

6. Mobile App

The ZealiD Mobile App (available on Google Play Store and Apple App Store) is the primary interface for the Trust Service and the Platform. Processing of personal data within the app in connection with identity proofing, certificate management, and qualified signing is governed by Section 2 of this Privacy Policy and the TSPS/CPS.

For analytics and performance monitoring within the app, ZealiD processes:

- Log records (connection ID), date of birth, language preference, identity document issuing country, customer name, app registration and usage data
- The lawful basis is legitimate interest in maintaining and improving service quality. Retention: 26 months.

No sign-in, certificate use, or electronic signature can be performed without active use of the subscriber's PIN or biometric authentication on the device. ZealiD does not store PIN codes.

7. Other Personal Data Processing Activities

7.1. Employees, Trainees, and Job Applicants

ZealiD processes personal data of current and former employees, trainees, and job applicants for HR, payroll, safety, legal compliance, and performance management purposes. The lawful bases are consent, contractual necessity, and legal obligation. Retention follows applicable employment and tax legislation. Job applicant data is retained for 1 year from rejection date.

Video surveillance data of Registration Officers (for service quality and fraud prevention) is processed on the basis of legal obligation and retained in accordance with applicable regulations.

7.2. Subcontractors and Suppliers

Contact data of individuals representing subcontractors and suppliers is processed for contract performance purposes. Retained in accordance with relevant contractual and regulatory requirements.

7.3. Complainants, Requesters, and Whistleblowers

Data provided in the context of complaints, data subject requests, or whistleblowing reports is processed for investigation and resolution purposes on the basis of legal obligation. Complaint data is retained for 5 years from submission date (or 14 years if the complaint results in certificate revocation). Whistleblowing case data is retained for 5 years from case closure.

7.4. Newsletter Subscribers

Email addresses collected for the ZealiD newsletter are processed on the basis of consent and retained until consent is revoked.

8. Sharing Personal Data

ZealiD shares personal data only in the following circumstances:

- Data processors: ZealiD uses third-party processors (e.g. IT service providers, accountants) under written data processing agreements. These processors act solely on ZealiD's instructions and are required to maintain appropriate security measures.
- Legal obligations: ZealiD will disclose data in response to a valid court order, law enforcement request, or requirement from a supervisory authority (e.g. PTS, IMY, data protection authorities in the EU). ZealiD will satisfy itself of the lawful basis before disclosing.
- Relying parties (Trust Service): information contained in a certificate issued by ZealiD is public by nature and not considered private for GDPR purposes. Certificate status (valid/revoked) is accessible via the OCSP service.
- Document sharing and signing (processor role): when a user uploads or shares documents via Trust Circle, or invites others to sign or upload, ZealiD processes those documents as data processor on behalf of that user. The user who uploads or shares, to the extent they qualify as a data controller under GDPR in relation to any personal data in those documents, is responsible as data controller. Any data subject requests relating to document content should be directed to that user.

ZealiD does not share personal data with third parties for direct marketing purposes.

Links to third-party websites from www.zealid.com are not covered by this Privacy Policy. ZealiD encourages users to review the privacy notices of those websites.

9. Data Security

ZealiD implements a layered combination of technical, organisational, administrative, and physical safeguards to protect personal data. These include:

- Mandatory multi-factor authentication for all personnel with access to systems containing special category data
- Encryption of evidence packages at rest and in transit (TLS for transport; LUKS and equivalent for storage)
- Role-based access controls and segregation of duties
- Immutable, append-only audit logs with tamper detection
- Physical security controls at data centre and office premises
- Annual security reviews, vulnerability assessments, and penetration testing

These safeguards are tested and reviewed as part of ZealiD's annual ETSI conformity assessment and are described in detail in the CPS and TSPS. Data Protection Impact Assessments (DPIAs) have been conducted for high-risk processing activities (including biometric identity verification).

10. Your Data Protection Rights

Under GDPR, you have the following rights in relation to personal data ZealiD holds about you. The availability of specific rights depends on the lawful basis for processing and the nature of the service.

- Right of access (Article 15): you have the right to request a copy of the personal data ZealiD holds about you.
- Right to rectification (Article 16): you have the right to request correction of inaccurate or incomplete data.
- Right to erasure (Article 17): you have the right to request deletion of your data in certain circumstances. Note: for the Trust Service, data retained under legal obligation (eIDAS, ETSI standards) cannot be deleted before the mandatory retention period expires.
- Right to restriction of processing (Article 18): you may request that ZealiD restricts processing in certain circumstances.
- Right to object (Article 21): where processing is based on legitimate interest, you may object. ZealiD will review and respond.
- Right to data portability (Article 20): this right does not apply to Trust Service processing. For other processing activities, please contact the DPO to discuss applicability.
- Rights related to automated decision-making (Article 22): ZealiD performs automated processing during identity verification (age check, document validation, liveness check). You have the right to request human review of an automated decision that significantly affects you.

Note on the Trust Service specifically: some rights (erasure, portability) are constrained by the mandatory retention requirements of eIDAS and the ETSI standards. ZealiD will explain the specific limitation in any response to a data subject request.

11. How to Exercise Your Rights and Complain

To make a data subject request, please email dpo@zealid.com. Include details of the service or product your request relates to, and any identifying information (e.g. subscriber or customer number) to help ZealiD process your request. ZealiD will verify your identity before providing any information.

If you believe ZealiD has not complied with its data protection obligations, you have the right to lodge a complaint with the relevant supervisory authority:

- In Sweden: Integritetsskyddsmyndigheten (IMY) — www.imy.se
- In other EU/EEA member states: the supervisory authority of your country of residence or place of work.

12. Updates to this Privacy Policy

ZealiD reviews this Privacy Policy at least annually and whenever significant changes occur to its services or the applicable legal framework. Changes that affect subscribers or relying parties are communicated in accordance with the Routine External Communication [RoExCom v12] and at least 14 days before taking effect, via the ZealiD website and/or push notification.

The current version of this Privacy Policy, together with the TSPS, CPS, and all other public documents, is always available at www.zealid.com/repository. Previous versions are retained in the ZealiD repository for reference.