ZealiD GDPR Policies and Procedures

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

1. Governance

1.1 Document owner

Document owner and contact person is the ZealiD AB Data protection officer (DPO): Philip Hallenborg, dpo@ZealiD.com, +46 768 374 200.

1.2 Data protection lead by DPO

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

1.3 Risk Assessment

ZealiD has a risk based approach to personal data processing and protection. This is called the Data Protection Impact Assessment (DPIA).

1.4 Approval of Residual Risks

The management board makes all decisions on data protection especially on activities to reduce and mitigate risks as proposed by the DPO and relevant forums. The management board also accepts all residual risks when counter measures have been implemented.

2. Choice and consent (GDPR Article 6)

The data subject shall have choices where appropriate to the use of personal data as far as possible. ZealiD services are by design constructed not only consent based by design but all services require active participation from the data subject.

ZealiD Product Type	**Purpose**	**Grounds for Processing**	**Method of consent collection**	**Data subject choices**
Bank or Tax Sign-in	To extract core Identity personal categories to satisfy anti money laundering	Consent & Legality	Information and link to terms at start. Active sign-in with method controlled by	Yes, a video conference option can be chosen instead of Bank.

	requirements (KYC).		data subject (authentication).	
Liveness check	To determine whether a natural person is physically present at the time of registration	Consent & Legality	Information and link to terms at start. Active user action with smartphone.	No choice. Mandatory according to certified method.
Micro Transfer	To execute in a bank interface controlled by data subject a 10 cent transfer to ZealiD	Consent & Legality	Information and link to terms at start. Active sign-in, choice of account.	No-requirements for a bank transfer controlled by Trustly Group AB
Private key control and qualified certificate	To issue a qualified certificate (qualified electronic certificate and signature to user)	Consent & Legality	Acceptance of TouchID or FaceID protection in app. Consent to TRA terms and conditions, QeID Terms and conditions.	No choice.
Photo and video of ID card	To verify identity and extract ID document attributes such as nationality, personal number, name and biometric photo.	Consent & Legality	Data subject needs to take photo+video using smartphone and a valid ID document.	All data processed. No choice. Not all data extracted.

2 Terms of Use and Privacy Policy

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.

3 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 a data subject will be granted unless a standardized process involving information and consent is completed. All consumers in system have consented to the service they are going through.

3.1. Can consents be easily provided?

Because the products are GDPR by design we demonstrate to the customer that enrolment/registration cannot be done without consent.

For general usage of ZealiD app, the user is in control of the data at all times. No sign-in or esignature can be issued without active use of the PIN or TouchID. If the data subject contacts the DPO ZealiD can provide timing and more in-depth details of when the consumer enrolled.

3.2. Under age users (article 8)

ZealiD policy restricts users younger than 18. This is checked as part of the TRA Service registration. It is stated in terms and conditions that we don't accept underaged (below 18).

4 Legitimate Purpose Specification and Use

ZealiD is a qualified trust service provider (QTSP) authorized by the Swedish Post & Telecoms Authority and on EU Trusted List under the eIDAS regulation. ZealiD will process data for the purpose of identity verification (registration), authentication, certificate issuance and creation of signatures. The legal basis for ZealiD processing is always consent and in most cases legality.
We serve regulated industries typically finance, signing, telecom, insurance and healthcare.

4.1 Collection of data

Screen scraping ("direct access")

Where ZealiD employs so called screen scraping techniques, or partners with those who do, all data on e.g. a bank account can be processed and the data subject needs to be informed that this is the case. All such practices are carried out in accordance with GDPR, PSD2 and eIDAS requirements. ZealiD is an authorized account information service provider by Swedish Financial Supervisory Body.

Although data can be processed as defined by law, the actual structuring and extraction of data is highly limited to a very narrow set of personal data demonstrating identity. ZealiD will not structure and extract any other data than data collected for identity verification purposes.

ID document processing

Where the data subject submits an ID-document, all data on the ID document can and will be processed. The data subject must be informed that this is the case in all information and consent texts.

Such personal data includes unique identifiers such as personal code, citizen service number, social security number. For example, Dutch BSN ("burgerservicenummer"), Swedish personal number ("personnummer") and Lithuanian personal code ("asmens kodas").

ZealiD is looking to validate the whole document for authenticity as well as using OCR or similar techniques to extract personal data from the documents. This is done according to a software setting that is setup and standardized for a wide variety of ID documents.

Limitation of use

All projects undergo initial and continuous DPIA review by the ZealiD Data Protection Taskforce. Limiting the scope and use of data is a standard discussion point in all monthly reviews and project setup processes.

5 Right to object

All ZealiD processes are voluntarily carried out by the active participation of the data subject. There is no need for a right to object.

6 Personal Information and Sensitive Information Life Cycle

6.1 Myzealid.com

ZealiD web service "myzealid.com" contains specific terms and conditions for what data is processed and stored. These may change from time to time.

6.2 ZealiD App

The ZealiD 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), published on the www.zealid.com/respository.

Certificates for trust services are issued for longer periods. Minimum 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 10 years.

6.3 Special Categories of Personal 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 the GDPR article 9 that prohibits all such processing unless an exemption is provided by law.

ZealiD basis its processing on two legal grounds under article 9:

- Article 9 (2) (a): the data subject has given explicit 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 customers are regulated and the requirements to process ID documents are defined by law (e.g. copy of ID document required, birth date, birth place)

6.4 Privacy and Security Policies Special Categories of personal Data

ZealiD has implemented many security measures to secure high risk ID document data. The measures are described in the CPS and TSPS. They are also resulting from DPIA. This includes but is not limited to minimizing access, enforcing 2FA authentication for all actors accessing system that contains Special Categories and finally encrypting all ID documents (work in progress).

7 Accuracy and Quality

Identity data cannot as a general rule not be amended, changed or edited, either by ZealiD, its customers or its users after the registration process is completed. The process is designed to be machine based with an extra layer of manual sampling. If an identity passes through the process it is deemed correct and can only be invalidated – never changed or edited.

7.1 Fraud

ZealiD adopts a number of public and confidential measures to prevent identity fraud. All fraud attempts are reported to law enforcement agencies.

8 Openness, Transparency and Notice

ZealiD products are built with GDPR by design. They are all consent and participation based – a data subject will actively drive the service. All services are provided with:

- Extensive information at start of service use
- Links to terms of use
- Links to privacy and practice statements

8.1 Rights, notices and questions

To further simplify for the customer the ZealiD.com website contains a number of resources aimed at facilitating understanding for the data subject see Subscriber information, terms and conditions for the TRA Service can be found at https://www.zealid.com/en/repository.

9 Individual Participation

9.1 Withdraw 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 – e.g. where ZealiD issues an 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.

9.2 Identification of Data subjects to obtain confirmation of held personal data

ZealiD App

ZealiD subscribers can sign-in to myzealid.com to see personal held. This combines a strong authentication/ identification function with access to data.

DPO

Data subjects are informed both on site, in terms and conditions and privacy documentation about the DPO and the contact details of the DPO. The DPO can also be reached by calling ZealiD switchboard.

10 Accountability

10.1 Documentation – Data Protection Hub (Articles 6(1), 6(3), 6(4))

ZealiD has all its documentation on data protection, information security, incident reporting, records of processing activities (controller and processer) and DPIA reviews in a central compliance hub. All activities go through yearly external audits by eIDAS conformity assessment bodies.

11 Data Protection Officer Instruction and Support (article 37, 38)

ZealiD Data Protection Hub contains an instruction that outline and determine the DPOs responsibilities. The management team is trained to support the DPOs work.

12 Consultation of authorities

Yes. ZealiD has a clear work flow for incident reporting and communicating to two authorities:

- Swedish IT and Telecoms Authority (PTS)
- Swedish Data Inspection Board (Integritetsskyddsmyndigheten)
- Swedish Financial Supervisory Body (FI)

13 Security Safeguards (Article 5, 24)

The information security standards set out in the IT security documentation are designed to secure the ZealiD information security environment against unauthorized and unlawful processing. They are designed to prevent accidental loss, destruction and damage.

13.1 Access controls

Personal data can be accessed by a small circle of ZealiD employees <5 and access is carefully controlled. All users of systems that involve personal data must use 2FA authentication devices. Updates are in progress to require the private key of the data subject (qualified certificate) to unlock personal data.

13.2 Encryption

ZealiD strives to encrypt as much information as possible. Especially special categories of personal data are undergoing encryption architecture changes so to allow only combination of access key sets.

13.3 Confidentiality agreements

All hired staff and external consultants sign confidentiality agreements, well documented, that restrict any transmission or sharing of information, IPR or other sources of personal data.

13.4 Training

- All new employees undergo introductions to personal data protection and information security.
- All employees are involved in DPIA and similar processes to create cross functional understanding and excellence when it comes to personal data – from a code level to a management and legal requirement level.

14 Monitoring, Measuring and Reporting (Article 39)

14.1 Compliance monitoring

Compliance is monitored on a monthly basis by data protection task force – see data protection hub calendar and meeting minutes.

14.2 Training (see 13.4)

14.3 DPIA

DPIAs are carried out at the start of each project and continuously in a cross functional Data protection task force meeting monthly.

14.4 Record of processing activities

ZealiD maintains to different records of processing activities:

1. Record of Processing Activities as Controller
2. Record of Processing Activities as Processor

15 Preventing Harm

Data subjects provide explicit consent in all ZealiD services.

15.1 Special categories

ID documents (and all data therein) and selfies (photos) are the only permitted special categories of data allowed to be processed by ZealiD. Any other data shall not be processed. The DPIA procedure shall provide sufficient evidence in all projects that no other processing activities take place.

15.2 Minimization of personal data

DPIA involve defining settings to minimize, on a project basis, the scope and length of storage of personal data in each project.

16 Third Party/ Vendor Management

16.1 Vendors (Data Processors)

ZealiD works with major vendors (Google, Amazon, Verisec, Tieto, Ascertia) and secures DPAs for each vendor. Vendors are selected with stability, information security and personal data management in mind).

16.2 Vendor Contracts

In addition to DPAs, the Vendor Contracts define service level and liabilities where breaches occur in information security or personal data.

17 Data Breach Management (Articles 33 and 34)

ZealiD DPO has training and understanding in how to notify supervisory authorities (PTS and Integritetsskyddsmyndigheten) with regards to incidents. Especially given the 72 hour time frame given. The Data Protection Task Force can be summoned with short notice by the DPO and the DPO has full authority to use all available resources to investigate and report breaches.