

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

1.	GOVERNANCE	5
1.1	DOCUMENT OWNER	5
1.2	DATA PROTECTION TASK FORCE	5
1.3	DECISION MAKING.....	5
2.	CHOICE AND CONSENT (GDPR ARTICLE 6)	5
2	TERMS OF USE AND PRIVACY POLICY	6
3	DOCUMENTATION AND MAINTENANCE OF CONSENT	6
3.1.1	<i>Can consents be easily provided?</i>	6
3.1.2	<i>Under age users (article 8)</i>	6
4	LEGITIMATE PURPOSE SPECIFICATION AND USE	7
4.1	COLLECTION OF DATA.....	7
4.1.1	<i>Screen scraping (“direct access”)</i>	7
4.1.2	<i>ID document processing</i>	7
4.1.3	<i>Limitation of use</i>	7
5	RIGHT TO OBJECT	7
6	PERSONAL INFORMATION AND SENSITIVE INFORMATION LIFE CYCLE	8
6.1	ZEALID WEB MODULES.....	8
6.2	ZEALID APP.....	8
6.3	SPECIAL CATEGORIES OF PERSONAL DATA	8
6.4	PRIVACY AND SECURITY POLICIES SPECIAL CATEGORIES OF PERSONAL DATA	8
7	ACCURACY AND QUALITY	9
7.1	FRAUD	9
8	OPENNESS, TRANSPARENCY AND NOTICE	9
8.1	RIGHTS, NOTICES AND QUESTIONS	9
9	INDIVIDUAL PARTICIPATION	10
9.1	WITHDRAW CONSENT	10
9.2	JOINT CONTROLLERSHIP.....	10
9.3	IDENTIFICATION OF DATA SUBJECTS TO OBTAIN CONFIRMATION OF HELD PERSONAL DATA.....	10
9.3.1	<i>ZealiD Web</i>	10
9.3.2	<i>ZealiD App</i>	10
9.3.3	<i>DPO</i>	10
10	ACCOUNTABILITY	10
10.1	DOCUMENTATION – DATA PROTECTION HUB (ARTICLES 6(1), 6(3), 6(4))	10
11	DATA PROTECTION OFFICER INSTRUCTION AND SUPPORT (ARTICLE 37, 38)	11
12	CONSULTATION OF AUTHORITIES	11
13	SECURITY SAFEGUARDS (ARTICLE 5, 24)	11
13.1	ACCESS CONTROLS	11
13.2	ENCRYPTION	11
13.3	CONFIDENTIALITY AGREEMENTS.....	11
13.4	TRAINING	12
14	MONITORING, MEASURING AND REPORTING (ARTICLE 39)	12
14.1	COMPLIANCE MONITORING	12
14.2	TRAINING (SEE 13.4).....	12
14.3	DPIA.....	12
14.4	RECORD OF PROCESSING ACTIVITIES	12

15 PREVENTING HARM.....12
15.1 SPECIAL CATEGORIES.....12
15.2 MINIMIZATION OF PERSONAL DATA12
16 THIRD PARTY/ VENDOR MANAGEMENT13
16.1 VENDORS (DATA PROCESSORS)13
16.2 VENDOR CONTRACTS13
17 DATA BREACH MANAGEMENT (ARTICLES 33 AND 34)13

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 task force

The DPO leads a Data Protection Task Force consisting of Director of Operations (Tomas Zuoza) and Chief Technical Officer (Ignas Karpiejus).

1.3 Decision making

The management team makes all decision on data protection especially on activities to reduce and mitigate risks as proposed by the DPO. These meetings take place according to the DPIA meeting calendar (at least once monthly for all projects and before any new project launch).

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 requirements (KYC).	Consent	Information and link to terms at start. Active sign-in with method controlled by data subject (authentication).	No – basic required data always collected
Micro Transfer	To execute in a bank interface controlled by data subject a 10 cent transfer to ZealiD	Consent	Information and link to terms at start. Active sign-in, choice of account	No-requirements for a bank transfer controlled by Trustly Group AB
Mobile ID (PIN code selection)	To issue a mobile ID (Advanced	Consent	Choice of PIN code and	No choice.

	electronic certificate and signature to user)		acceptance of TouchID or FaceID protection in app. Consent to privacy and user terms and conditions.	
Photo of ID card	To verify identity and extract ID document attributes such as nationality, personal number, name and biometric photo.	Consent	Data subject needs to take use smartphone or desktop to take a picture of 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.

3.1.1 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.

3.1.2 Under age users (article 8)

As a general rule ZealiD restricts users younger than 18 in our service terms. This is part of the algorithms in the software that check ID document. It is also a part of the algorithms that check bank data. It is stated in terms and conditions that we don't accept underaged (below 18).

4 Legitimate Purpose Specification and Use

As a general rule, ZealiD will process data for the purpose of identity verification. One of ZealiD's legacy products also executes payment. So the legal purpose of processing is with one of the customers that acts as controller. The legal basis for our processing is consent. We serve regulated industries typically finance, betting, telecom, insurance and health. The purpose of identity verification is for our customers to comply with legal standards as defined in three major legal packages:

- a) Anti-money laundering and combatting of financing of terrorism
- b) GDPR – securing personal data online
- c) PSD2 – securing payments

4.1 Collection of data

4.1.1 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.

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 cannot structure and extract any other data than their data collected for identity verification purposes.

4.1.2 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.

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 software setting that is setup and standardized for a wide variety of ID documents.

4.1.3 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 ZealiD Web Modules

The ZealiD web modules are designed such that all information is deleted within max 7 days at present the setting is 1 day. This can be changed on a project basis. The information is to be held for the shortest possible time period – yet enabling the option to repair and maintain the service and software when errors are discovered. What typically will affect cycles for Web modules is the volume of data processed and the overall risk identified in the DPIA processes.

6.2 ZealiD App

The ZealiD App service is a mobile ID type issuing of an advanced electronic signature. The characteristics of the service is to produce electronic signatures. As such the signatures 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).

Certificates for trust services are issued for longer periods. Minimum 2 years. In some instances, the certificates can be issued for up to 10 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 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 and continues to install security measures to secure high risk ID document data. The measures are described in DPIA documentation and refers to minimizing access,

enforcing 2FA authentication for all actors accessing system that contains Special Categories and finally encrypting all ID document (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

As in any business, fraud is a reality for ZealiD. There are different types of fraud use cases but a fraudulent data subject may try to setup a profile in the name of another data subject. The measures in place to keep data accurate are machine and manual based. Where these constantly updated measures fail to detect and combat fraud, there may be a portion of the transactions and hosted identities that are fraudulent at any given time. There are functions in the system for customers to deactivate suspicious identities.

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 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:

- Consumer information (<https://www.ZealiD.com/en/consumer>) – this is a site dedicated for frequently asked questions and the basic functionality of our service. It aims at a consumer that is not educated as to the content on our service and explains in simple words e.g.:
 - What the service is about
 - What the purpose is of personal data processing is and that it is consent based
 - How consent is provided
 - What screen scraping means
 - What data is processed and stored

- How we restrict and minimize processing
- Where data is processed (no third country transfer)
- How long data is stored
- What data can be edited, right to be forgotten etc
- Data subject rights and how to contact the DPO

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 advanced electronic signature and maintains the signature package.

9.2 Joint Controllorship

ZealiD has a present one joint controllership in the ZealiD App process in that a bank login and where applicable a micro transaction can be carried out with ZealiD partner Trustly Group AB. In those instances the data subject is informed at the beginning of the user flow that Trustly will manage the bank login process under its own information, terms and privacy statements.

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

9.3.1 ZealiD Web

No data is stored for longer than 1 day (max 7 days). Confirming personal data stored is out of scope for ZealiD Web.

9.3.2 ZealiD App

ZealiD provides a web site where a user can sign-in to see all personal held on the data subject. This combines a strong authentication/ identification function with access to data.

9.3.3 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 processor) and DPIA reviews in a central Data Protection Hub.

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 Data Inspection Board (Datainspektionen)
- Swedish IT and Telecoms Authority (PTS)

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 (mobile ID) 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 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 Datainspektionen) 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.