ZEALID TRUST CIRCLE

DATA PROCESSING AGREEMENT

Effective Date: 1 March 2026 | Version 1.0 | GDPR Article 28 Compliant

DATA CONTROLLER

Account Holder

The individual or legal entity identified as Account Holder in the Registration Flow or applicable Order Form.

By completing the Registration Flow or executing an Order Form, the Account Holder accepts this DPA as a binding part of its agreement with ZealiD.

For Individual Accounts where processing falls within GDPR Article 2 scope, the individual is deemed the Controller.

DATA PROCESSOR

ZealiD AB

Reg. No. 556972-4288
Visiting: Norrlandsgatan 10, 111 43 Stockholm, Sweden
Postal: Box 3437, 111 56 Stockholm, Sweden
DPO: dpo@zealid.com
Supervisory Authority: IMY (Integritetsskyddsmyndigheten)
Qualified Trust Service Provider under eIDAS

Important — Scope of this DPA: This DPA governs ZealiD's processing of personal data as Processor on behalf of Account Holders (Controllers) in connection with the Trust Circle platform. It does not govern ZealiD's separate processing as independent Controller for its own purposes (identity verification via TRA, qualified certificate issuance via QeID, billing, security, analytics, marketing, and employment), which is governed by ZealiD's Privacy Policy published at https://www.zealid.com/en/repository.

Privacy Policy: ZealiD's Privacy Policy describes how ZealiD processes personal data as Controller — including data collected from website visitors, leads, customers, employees, and users of the ZealiD App in connection with TRA/QeID trust services. The Privacy Policy is separate from this DPA and is published at https://www.zealid.com/en/repository.

ZEALID TRUST CIRCLE — DOCUMENT ARCHITECTURE OVERVIEW

The ZealiD Trust Circle legal framework consists of five layers of documents. This overview is reproduced in every document in the framework so that any reader — whether Account Holder, legal counsel, auditor, data protection authority, or supervisory body — can immediately understand the full structure regardless of which document they are reading.

Layer	Document	Purpose	Applies to	Negotiable?
1	**TSPS — TRA Service Practice Statement**	Governing document for ZealiD's Trusted Registration Authority service. Defines identity proofing procedures, subscriber obligations, liability, and event log retention. TRA identity proofing via the ZealiD App is a mandatory prerequisite for all Trust Circle Account activation — every user completes this step before their Account becomes active. Audited annually by accredited conformity assessment body.	All Trust Circle users — mandatory prerequisite	No — regulatory, audited, non-negotiable
1	**QeID Certificate Practice Statement (CPS)**	Governing document for ZealiD's qualified certificate and signing service. Defines certificate issuance, management, revocation, and reliance rules under eIDAS. A QeID qualified certificate is issued to every user as part of the mandatory ZealiD App onboarding — it is the cryptographic credential underpinning all authentication and signing in Trust Circle. Audited annually.	All Trust Circle users — mandatory prerequisite	No — regulatory, audited, non-negotiable
2	**Trust Circle Service Specification**	Defines what Trust Circle delivers: plan tiers, freemium inclusions, feature descriptions, fair-use parameters, API rate limits, storage allowances, data retention periods, and post-termination export windows. This is the single authoritative source for operational parameters referenced throughout the commercial documents.	All Account Holders	No — published by ZealiD, updated with notice per GTC §6.1
3	**General Terms & Conditions (GTC)**	Primary commercial agreement governing the Trust Circle platform. Covers definitions, service description, transition from my.zealid.com, order of precedence, fees, IP, confidentiality, acceptable use, liability, termination, and dispute resolution. Accepted click-through at Registration Flow.	All Account Holders	No (standard) / Limited (Order Form)
3	**Addendum A — Natural Persons**	Supplementary terms for Individual Account Holders. Covers consumer rights, solo certificate requirement, biometric consent, device security, and freemium/paid payment mechanics. Takes precedence over GTC for Individual Accounts.	Individual Account Holders only	No — standard terms
3	**Addendum B — Legal Entities**	Supplementary terms for Business Account Holders. Covers multi-user administration, resale, API licensing, 24-month liability cap, trademark consent, invoicing by agreement, and 90-day termination notice. Takes precedence over GTC for Business Accounts.	Business Account Holders only	Limited — Order Form may vary specific terms
3	**Order Form**	Executed commercial instrument for negotiated Business Accounts. Specifies custom pricing, invoiced billing, SLA commitments, integration scope, and any agreed deviations from Addendum B. Only applies where explicitly agreed. Takes precedence over Addendum B and GTC.	Negotiated Business Accounts only	Yes — fully negotiable
4	**Data Processing Agreement (DPA)**	GDPR Article 28-compliant processor agreement governing ZealiD's processing of personal data on behalf of Account Holders (Controllers). Includes four Annexes: processing particulars (Annex I), technical and organisational measures (Annex II), sub-processor framework (Annex III), and international transfer mechanism/SCCs (Annex IV). Accepted click-through at Registration Flow.	All Account Holders where GDPR Article 2 applies	Limited — SCC module selection; sub-processor objection right
4	**Privacy Policy**	Governs ZealiD's own processing as independent Controller: website visitors, leads, analytics, employees, TRA/QeID subscribers, and billing.	All persons interacting with ZealiD directly	No — ZealiD's own controller obligations

		Separate from and not governed by the DPA. Published at the repository.		
5	**Acceptable Use Policy (AUP)**	Defines permitted and prohibited conduct for all platform users: identity/signing rules, content standards, platform integrity, API use, fair use, operator obligations, and enforcement. Applies to all Account Holders, Authorised Users, API integrators, and white-label deployments.	All Account Holders and Authorised Users	No — standard conduct rules

Conflict Resolution: In the event of any conflict between documents, the document higher in the layer table prevails to the extent of the inconsistency. Within Layer 3, the Order Form prevails over Addendum B, which prevails over the GTC. Standard Contractual Clauses (Annex IV of the DPA) prevail over the DPA for international transfers. All documents are published at https://www.zealid.com/en/repository.

Data Hosting Default: Unless otherwise agreed in writing (via an Order Form or separate written agreement), all Account Content is hosted and stored exclusively in ZealiD-managed, sole-operational-control infrastructure within the European Economic Area. No third party has independent access to unencrypted Account Content. This reflects both ZealiD's commercial commitment and its mandatory obligations as a Qualified Trust Service Provider under eIDAS, audited annually under ETSI EN 319 401. The governing provisions are GTC §10.3 and DPA §11.1.

WHICH DOCUMENTS APPLY TO EACH ACCOUNT TYPE

Document	Freemium Individual	Paid Individual	Self-Serve Business	Negotiated Business / Enterprise
TSPS / CPS	✓ Mandatory prerequisite	✓ Mandatory prerequisite	✓ (each user)	✓ (each user)
Service Specification	✓	✓	✓	✓
GTC	✓	✓	✓	✓
Addendum A	✓	✓	—	—
Addendum B	—	—	✓	✓
Order Form	—	—	—	✓
DPA	If GDPR Art. 2 applies	If GDPR Art. 2 applies	✓	✓
AUP	✓	✓	✓	✓
Privacy Policy	✓ (ZealiD as Controller)	✓ (ZealiD as Controller)	✓ (ZealiD as Controller)	✓ (ZealiD as Controller)

Acceptance mechanism: All documents except the Order Form and the TSPS/CPS are accepted by click-through during the Registration Flow. The Order Form is executed in writing between ZealiD and the Business Account Holder. The TSPS and CPS are non-negotiable regulatory documents — use of TRA or QeID services constitutes acceptance of their terms by operation of law.

TABLE OF CONTENTS

1. Definitions
2. Scope, Role Separation, and Privacy Policy
3. Nature, Purpose, and Legal Basis of Processing
4. Duration and Termination

5. Processor Obligations
6. Controller Responsibilities
7. Data Subject Rights Assistance
8. Personal Data Breach Notification
9. Data Protection Impact Assessments
10. Sub-Processing
11. International Data Transfers
12. Audit and Compliance
13. Data Retention and Deletion
14. Liability and Precedence
15. US State Privacy Addendum
16. Governing Law and Supervisory Authority
17. Contact and Notices
Annex I. Details of Processing Activities (GDPR Art. 28(3))
Annex II. Technical and Organisational Measures (TOMs)
Annex III. Sub-Processor Framework
Annex IV. International Transfer Mechanism

1. DEFINITIONS

Capitalised terms in this DPA have the meanings given in the ZealiD Trust Circle General Terms & Conditions (GTC). The following additional terms apply:

Controller	The natural person or legal entity that determines the purposes and means of processing personal data. For Trust Circle, the Controller is the Account Holder in respect of personal data within their Account.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Data Subject	An identified or identifiable natural person to whom personal data relates.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
IMY	Integritetsskyddsmyndigheten, the Swedish Authority for Privacy Protection, being ZealiD's lead supervisory authority under GDPR.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in GDPR Article 4(1).
Privacy Policy	ZealiD's Privacy Policy governing ZealiD's own processing of personal data as independent Controller, published at https://www.zealid.com/en/repository.
Processor	A natural or legal person that processes personal data on behalf of a Controller. For Trust Circle, ZealiD is the Processor in respect of personal data processed on the Account Holder's instructions.

Processing	Any operation performed on personal data, including collection, storage, retrieval, use, disclosure, or deletion.
SCCs	The Standard Contractual Clauses for the transfer of personal data to third countries adopted by the European Commission under GDPR, as applicable.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for unique identification), health data, or data concerning sex life or sexual orientation, as defined in GDPR Article 9.
Sub-processor	Any processor engaged by ZealiD to process personal data on behalf of the Controller under this DPA.
TOMs	Technical and Organisational Measures — the security measures described in Annex II.
Trust Circle	ZealiD's multi-tenant SaaS platform for trusted document storage, collaboration, and qualified signing workflows, as further described in the GTC and Service Specification.

2. SCOPE, ROLE SEPARATION, AND PRIVACY POLICY

2.1 Scope — Processor Role

This DPA governs all processing of personal data by ZealiD as Processor on behalf of the Account Holder (Controller) in connection with ZealiD's provision of the Trust Circle platform. ZealiD processes such personal data only on the documented instructions of the Controller and for no other purpose, except where required by applicable law.

2.2 ZealiD as Independent Controller — Privacy Policy

ZealiD processes certain personal data as an independent Controller for its own purposes, entirely separately from its role as Processor under this DPA. These include:

- **(a)** personal data of website visitors, leads, and prospective customers collected through www.zealid.com (including analytics via Google Analytics, Hubspot, and Hotjar; cookies; and contact forms);
- **(b)** personal data of Account Holders processed for billing, account administration, fraud prevention, security monitoring, and legal compliance;
- **(c)** personal data of Subscribers processed in connection with TRA identity proofing and QeID qualified certificate issuance and management, governed by the TSPS and CPS;
- **(d)** personal data of employees, contractors, job applicants, and whistleblowers; and
- **(e)** personal data processed pursuant to legal obligations, court orders, or regulatory requirements.

All of the above is governed by ZealiD's Privacy Policy, not this DPA. The Privacy Policy is published at https://www.zealid.com/en/repository and should be read by all data subjects who interact with ZealiD directly.

2.3 Individual Account Holders — GDPR Article 2

Where a natural person uses Trust Circle in a manner that falls within the material scope of GDPR Article 2 (i.e. processing is not purely personal or household in nature), that individual qualifies as a Controller under this DPA and ZealiD processes the relevant personal data as Processor on their behalf. Individual Account Holders uncertain whether their use constitutes controller-level processing should contact dpo@zealid.com.

2.4 Separate Accounts, Separate Controllers

Each Account Holder is a separate and independent Controller for its own Account. No Account Holder has any access to, or controller authority over, personal data in another Account Holder's Account. ZealiD does not combine personal data across Accounts for Controller-directed purposes.

3. NATURE, PURPOSE, AND LEGAL BASIS OF PROCESSING

3.1 Nature of Processing

ZealiD processes personal data on behalf of the Controller solely to provide, operate, maintain, secure, and improve the Trust Circle platform in accordance with the Controller's instructions. Processing operations include: hosting and storage of Account Content; access management and authentication logging; document workflow facilitation; backup and disaster recovery; technical support and incident investigation; and performance monitoring.

3.2 Purpose Limitation

ZealiD will not process personal data for any purpose other than those specified in this DPA and the Controller's documented instructions, except where required by applicable EU or EU Member State law, in which case ZealiD will inform the Controller before processing unless prohibited by law.

3.3 Legal Basis

The legal basis for ZealiD's processing as Processor is the performance of the Trust Circle service agreement with the Controller (GDPR Article 6(1)(b) and 6(1)(f) as applicable). The Controller is solely responsible for identifying and maintaining the lawful basis for its own processing of personal data within Trust Circle, and for communicating that basis to data subjects in its privacy notices.

3.4 Instructions

The Controller's documented instructions are: (a) the configuration of the Account and use of Trust Circle features; (b) these Terms and this DPA; and (c) any written instructions provided during the term. If ZealiD believes an instruction would infringe GDPR or other applicable data protection law, it will promptly notify the Controller. ZealiD is not required to follow an instruction that would require it to act unlawfully.

4. DURATION AND TERMINATION

Processing under this DPA continues for the duration of the Account and for the post-termination period defined in Section 13 of this DPA, after which ZealiD will delete or return data as described therein. This DPA terminates automatically upon expiry or termination of the GTC, subject to the survival of any provisions expressly stated to survive.

5. PROCESSOR OBLIGATIONS

ZealiD as Processor undertakes to:

5.1 Instruction Compliance

Process personal data only on documented instructions from the Controller, which are set out in the GTC, this DPA, and any written instructions provided during the term. ZealiD will promptly notify the Controller if it believes any instruction infringes applicable data protection law.

5.2 Confidentiality

Ensure that all personnel authorised to process personal data under this DPA are subject to binding confidentiality obligations (whether statutory or contractual) and have received appropriate data protection training. ZealiD will maintain and make available to the Controller on request a record of the confidentiality undertakings applicable to its personnel.

5.3 Security — TOMs

Implement and maintain the technical and organisational security measures described in Annex II. ZealiD will review and, where necessary, update these measures on a regular basis and no less than annually. ZealiD will notify the Controller of any material change to the TOMs that could adversely affect the level of protection with reasonable advance notice.

5.4 Data Subject Rights Assistance

Assist the Controller in responding to data subject rights requests under GDPR Articles 15–22, as described in Section 7 of this DPA. ZealiD will promptly forward any data subject rights requests received directly from data subjects in connection with the Controller's Account to the Controller without undue delay.

5.5 Breach Notification

Notify the Controller of any personal Data Breach in accordance with Section 8 of this DPA.

5.6 DPIA and Prior Consultation Assistance

Provide all reasonably requested information and assistance to support the Controller in carrying out Data Protection Impact Assessments (DPIAs) under GDPR Article 35 and in prior consultation with supervisory authorities under GDPR Article 36, to the extent that such assistance relates to ZealiD's processing activities under this DPA.

5.7 Record of Processing Activities

Maintain records of processing activities carried out on behalf of each Controller as required by GDPR Article 30(2) and make such records available to the relevant supervisory authority upon request. ZealiD will cooperate with the Controller in ensuring the accuracy of the Controller's own ROPA to the extent it relates to ZealiD's processing activities.

5.8 Post-Termination Obligations

At the Controller's choice, upon termination of this DPA, delete or return all personal data processed on behalf of the Controller, and delete all existing copies, unless retention is required by applicable EU or EU Member State law. The post-termination export and deletion mechanics are described in Section 13 of this DPA.

6. CONTROLLER RESPONSIBILITIES

The Controller is solely responsible for:

- **(a)** ensuring it has a valid, documented lawful basis under GDPR Article 6 (and Article 9 for Special Category Data) for all processing of personal data within its Account, and communicating that basis to data subjects through its own privacy notices;
- **(b)** the accuracy, completeness, and lawfulness of all personal data uploaded to or processed within the Account;
- **(c)** providing privacy notices to all data subjects (including Authorised Users, document counterparties, and any other individuals whose data is uploaded or shared within the Account) that describe the Controller's use of Trust Circle as a processing tool;

(d) carrying out DPIAs where required by GDPR Article 35 in connection with its use of Trust Circle, and consulting ZealiD as Processor in that process;

(e) ensuring that invited participants, counterparties, and other persons whose data is uploaded to or processed within the Account have been informed of and (where required) consented to such processing;

(f) maintaining its own ROPA to the extent required by GDPR Article 30(1); and

(g) notifying ZealiD of any limitation on the processing instructions it is entitled to give, arising from applicable law or its own data protection assessments.

7. DATA SUBJECT RIGHTS ASSISTANCE

7.1 Forwarding Requests

ZealiD will forward to the Controller any data subject rights requests received by ZealiD that relate to personal data processed on behalf of the Controller, without undue delay and in any event within three (3) business days of receipt.

7.2 Technical Assistance

ZealiD will provide the following technical assistance to help the Controller respond to data subject rights requests:

(a) Right of access (GDPR Art. 15) — ZealiD will provide the Controller with the ability to export Account Content and processing logs sufficient to enable the Controller to respond to access requests.

(b) Right to rectification (GDPR Art. 16) — ZealiD will enable Controllers and Authorised Users to update personal data fields within the Account to the extent technically feasible.

(c) Right to erasure (GDPR Art. 17) — ZealiD will, on the Controller's written instruction, delete specified personal data within the Account, subject to mandatory retention obligations and to the extent technically feasible given the nature of the Service.

(d) Right to restriction (GDPR Art. 18) — ZealiD will, on the Controller's written instruction, restrict processing of specified personal data to storage only, pending the Controller's decision or applicable legal proceedings.

(e) Right to data portability (GDPR Art. 20) — ZealiD will provide Account Content export functionality in a structured, commonly used, machine-readable format to support the Controller's portability obligations where applicable.

(f) Right to object (GDPR Art. 21) — ZealiD will cease or restrict processing on the Controller's written instruction where the Controller has determined that an objection must be upheld.

7.3 Timelines for Assistance

ZealiD will respond to any written request for technical assistance from the Controller in connection with data subject rights within ten (10) business days of receipt of the written instruction. Where ZealiD requires additional time due to technical complexity, it will notify the Controller within the ten-day period with a proposed timeline.

7.4 Direct Requests from Data Subjects

Where ZealiD receives a data subject rights request directly from a data subject in relation to personal data processed on behalf of a Controller, ZealiD will inform the data subject that their request has been forwarded to the relevant Controller. ZealiD will not respond substantively to such requests on the Controller's behalf without the Controller's prior written authorisation.

8. PERSONAL DATA BREACH NOTIFICATION

8.1 Notification to Controller

ZealiD will notify the Controller without undue delay, and in any event within forty-eight (48) hours of becoming aware of a personal Data Breach affecting personal data processed on behalf of the Controller. This timeline is set at 48 hours to enable the Controller to assess its own 72-hour notification obligation to the competent supervisory authority under GDPR Article 33.

8.2 Content of Notification

The initial notification will include, to the extent then available:

- **(a)** a description of the nature of the Data Breach, including the categories and approximate number of data subjects and personal data records concerned;
- **(b)** the contact details of ZealiD's DPO (dpo@zealid.com) and, where applicable, the data protection contact point for the affected service;
- **(c)** a description of the likely consequences of the Data Breach; and
- **(d)** a description of the measures taken or proposed to address the Data Breach, including measures to mitigate its possible adverse effects.

Where all required information cannot be provided in the initial notification, ZealiD will provide it in phases as it becomes available, without further undue delay.

8.3 Cooperation

ZealiD will cooperate fully with the Controller and provide all reasonably requested information to assist the Controller in fulfilling its own breach notification obligations to the competent supervisory authority and to affected data subjects under GDPR Articles 33 and 34.

8.4 ZealiD's Own Breaches — Privacy Policy

Data Breaches affecting personal data processed by ZealiD as independent Controller (for example, TRA, QeID, or website data) are governed by ZealiD's own regulatory obligations as a QTSP and by its Privacy Policy. ZealiD will notify the competent supervisory authority (IMY) and affected data subjects as required by applicable law.

9. DATA PROTECTION IMPACT ASSESSMENTS

ZealiD will provide the Controller with all reasonably requested information about ZealiD's processing activities, TOMs, and sub-processor arrangements that the Controller requires to carry out a DPIA in connection with its use of Trust Circle. Where a DPIA indicates a high residual risk that requires prior consultation with a supervisory authority under GDPR Article 36, ZealiD will cooperate with the Controller and, where requested, with the supervisory authority in that consultation process.

ZealiD conducts its own DPIAs in connection with new or changed Trust Circle processing activities and makes DPIA summaries available to Controllers on request, subject to confidentiality obligations protecting the integrity of ZealiD's security controls.

10. SUB-PROCESSING

10.1 General Authorisation

By accepting this DPA, the Controller provides general written authorisation to ZealiD to engage sub-processors for the performance of specific processing activities on behalf of the Controller, subject to the conditions in this Section 10.

10.2 Sub-processor Requirements

ZealiD will:

- **(a)** impose on each Sub-processor, by written agreement, data protection obligations equivalent to those set out in this DPA, including obligations relating to confidentiality, security, and assistance with Controller obligations;
- **(b)** remain fully liable to the Controller for the acts and omissions of each Sub-processor as if ZealiD had performed the processing directly; and
- **(c)** ensure that Sub-processors process personal data only within the European Economic Area or in a jurisdiction providing an adequate level of protection, or subject to the safeguards described in Section 11.

10.3 Sub-processor List and Change Notification

The current list of Sub-processors engaged by ZealiD in connection with Trust Circle is published in the ZealiD repository at https://www.zealid.com/en/repository and is detailed in Annex III. ZealiD will provide Controllers with not less than thirty (30) days' advance written notice of any intended change (addition, replacement, or removal) to its Sub-processor arrangements. Such notice will be provided by email to the Account Holder's registered address or via an in-product notification.

10.4 Controller Objection Right

Upon receipt of notice of a new or replacement Sub-processor, the Controller may object to the change by written notice to ZealiD (legal@zealid.com) within the thirty (30) day notice period, stating the reasonable grounds for the objection. If the Controller objects and ZealiD is unable to accommodate the objection without materially impairing the provision of the Service, the Controller may terminate the relevant Services on written notice, and ZealiD shall provide a pro-rata refund of any prepaid fees for the remaining unused period.

11. INTERNATIONAL DATA TRANSFERS

11.1 Default Hosting — ZealiD-Managed, Sole-Control, EEA

Unless otherwise agreed in writing in an Order Form or separate written agreement, all hosting, storage, and processing of Account Content under this DPA takes place exclusively in ZealiD-managed infrastructure under ZealiD's sole operational control, located within the European Economic Area (EEA). The following principles apply as the default position for all Account Holders:

- **(a)** Sole-control environment — Account Content is processed and stored in infrastructure that ZealiD manages and controls exclusively. No Sub-processor or third party has independent, unilateral access to unencrypted Account Content. Where ZealiD uses Sub-processors for underlying cloud compute or storage (as listed in Annex III), those Sub-processors operate strictly under ZealiD's access controls, encryption keys, and contractual restrictions — they do not have a separate, independent relationship with the Account Holder's data.
- **(b)** EEA by default — all primary hosting and storage of Account Content is within the EEA. No Account Content is transferred to or stored in a jurisdiction outside the EEA without the Account Holder's explicit prior written agreement, except where required by applicable law.
- **(c)** QTSP regulatory basis — ZealiD's sole-control, EEA-based infrastructure posture reflects not only commercial best practice but ZealiD's mandatory obligations as a Qualified Trust Service Provider under the eIDAS

Regulation, audited annually under ETSI EN 319 401. These obligations apply to the trust service environment as a whole and cannot be waived.

(d) Alternative arrangements — Account Holders requiring a dedicated single-tenant environment, a specific EEA member state, or a different hosting configuration must agree this in writing via an Order Form. Any alternative arrangement is subject to ZealiD's assessment of compatibility with its QTSP obligations and information security standards.

Scope of this clause: This clause governs the hosting of Account Content processed by ZealiD as Processor on behalf of the Account Holder. ZealiD's qualified trust service infrastructure (TRA/QeID), which processes personal data as independent Controller, is subject to separate and more stringent mandatory security requirements under the eIDAS Regulation and cannot under any circumstances be hosted in customer-designated or shared third-party environments.

11.2 Transfer Safeguards

Where ZealiD or any of its Sub-processors transfers personal data to a country outside the EEA that does not benefit from an adequacy decision under GDPR Article 45, ZealiD will ensure that the transfer is subject to appropriate safeguards in accordance with GDPR Article 46. Applicable safeguards include:

(a) the European Commission's Standard Contractual Clauses (SCCs) for the transfer of personal data to third countries, as incorporated in Annex IV;

(b) the EU–U.S. Data Privacy Framework, where applicable; or

(c) such other transfer mechanism as may be approved under GDPR Article 46 from time to time.

11.3 UK and Swiss Transfers

For transfers of personal data to or from the United Kingdom or Switzerland, ZealiD will rely on the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU SCCs, or the Swiss Standard Contractual Clauses as applicable, or such other mechanism as may be approved by the relevant competent authority.

11.4 Transfer Impact Assessment

ZealiD conducts Transfer Impact Assessments (TIAs) for all third-country transfers to assess whether the legal framework in the destination country offers a level of protection essentially equivalent to that of the EEA. TIA summaries are available to Controllers on request, subject to confidentiality.

12. AUDIT AND COMPLIANCE

12.1 Audit Rights

ZealiD will make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations of this DPA. Upon reasonable written request (no more than once per calendar year, unless required by a supervisory authority or material security incident), ZealiD will:

(a) provide its most recent third-party audit reports (ISO 27001, ETSI EN 319 401/411/421, SOC 2 Type II where available) under appropriate confidentiality obligations; and

(b) allow the Controller (or a third-party auditor appointed by the Controller and approved in writing by ZealiD, such approval not to be unreasonably withheld) to conduct an on-site or remote audit of ZealiD's processing activities under this DPA, subject to reasonable prior notice (not less than thirty (30) days), agreement on scope and methodology, and execution of a confidentiality agreement protecting ZealiD's and other customers' information.

12.2 Audit Costs

The costs of any audit conducted pursuant to Section 12.1(b) shall be borne by the Controller, unless the audit reveals a material non-compliance by ZealiD with this DPA, in which case ZealiD will bear its own reasonable costs of facilitating the audit.

12.3 Regulatory Cooperation

ZealiD will cooperate with and provide reasonable assistance to the Controller in connection with any investigation or audit by the competent supervisory authority (IMY) relating to ZealiD's processing under this DPA. ZealiD will notify the Controller promptly of any supervisory authority inquiry or enforcement action that relates to the processing covered by this DPA, to the extent permitted by law.

13. DATA RETENTION AND DELETION

13.1 Trust Circle Account Content

ZealiD retains Account Content for the post-termination period defined in the ZealiD Trust Circle Service Specification (published at https://www.zealid.com/en/repository). This period is set in the Service Specification rather than in this DPA so that it can be updated without requiring a full DPA revision. At the end of the retention period, ZealiD will permanently and securely delete all Account Content, unless:

- **(a)** a longer retention period is required by applicable EU or EU Member State law;
- **(b)** the data relates to TRA or QeID trust service records, which are subject to mandatory regulatory retention periods defined in the TSPS and CPS; or
- **(c)** the Controller has provided written instruction to retain the data for a specified additional period.

13.2 TRA and QeID Trust Service Records

Personal data processed in connection with TRA identity proofing or QeID certificate issuance is subject to mandatory retention obligations under the eIDAS Regulation, the TSPS, and the CPS. These retention obligations are independent of this DPA and cannot be overridden by Controller instructions. In the event of certificate revocation, extended retention periods apply as specified in the applicable practice statement and ZealiD's Privacy Policy.

13.3 ZealiD's Own Controller-Capacity Records

Personal data processed by ZealiD as independent Controller (for billing, security, analytics, website, and employment purposes) is retained in accordance with the retention schedules published in ZealiD's Privacy Policy. These records are not subject to Controller instructions under this DPA.

13.4 Deletion Confirmation

Upon completion of the deletion process following Account termination, ZealiD will provide the Controller with written confirmation of deletion on request, identifying the categories of data deleted and the deletion method used.

14. LIABILITY AND PRECEDENCE

14.1 Liability

The limitation of liability provisions set out in Section 18 of the GTC apply equally to this DPA. For the avoidance of doubt, ZealiD's liability cap under Section 18.2 of the GTC applies in aggregate to all claims under both the GTC and this DPA.

14.2 Regulatory Fines

Nothing in this DPA limits either party's liability for administrative fines imposed by a competent supervisory authority under GDPR, which are governed by applicable law and cannot be contractually excluded or capped.

14.3 SCC Precedence

In the event of any conflict between this DPA and the Standard Contractual Clauses set out in Annex IV (as applicable to international transfers), the SCCs prevail to the extent of the inconsistency and solely in respect of the international transfer to which they apply.

14.4 GTC Precedence

In all other respects, the order of precedence in Section 4 of the GTC applies to this DPA. This DPA is incorporated into and forms part of the agreement between ZealiD and the Account Holder.

15. US STATE PRIVACY ADDENDUM

15.1 Applicability

This Section 15 applies where the Account Holder, or individuals whose personal data is processed within the Account, are subject to US state privacy laws including the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CTDPA), the Utah Consumer Privacy Act (UCPA), or any substantially similar US state privacy law enacted after the Effective Date (collectively, "US Privacy Laws").

15.2 Service Provider / Processor Role

ZealiD acts as a "service provider" or "processor" (as those terms are defined in the applicable US Privacy Law) with respect to personal data processed on behalf of the Account Holder under this DPA. ZealiD will process personal data only for the business purposes specified in this DPA and will not:

- **(a)** sell or share personal data within the meaning of applicable US Privacy Laws;
- **(b)** retain, use, or disclose personal data for any purpose other than providing the Trust Circle service, except as required by applicable law; or
- **(c)** combine personal data received from the Controller with personal data received from or collected in connection with other sources, except as permitted by applicable US Privacy Law.

15.3 Consumer Rights Assistance

ZealiD will assist the Controller in responding to consumer rights requests under applicable US Privacy Laws by providing the same technical assistance described in Section 7 of this DPA (access, deletion, correction, portability, and opt-out where applicable).

15.4 CCPA Certification

ZealiD certifies that it understands the obligations of a service provider under the CCPA/CPRA and will comply with them. ZealiD will notify the Controller if it determines that it can no longer meet these obligations.

15.5 Controller Rights of Audit

The Controller may, in accordance with applicable US Privacy Laws, take reasonable and appropriate steps to ensure ZealiD processes personal data consistent with the Controller's obligations, including conducting audits as described in Section 12 of this DPA.

16. GOVERNING LAW AND SUPERVISORY AUTHORITY

This DPA is governed by Swedish law and the European Union's General Data Protection Regulation (GDPR). The competent supervisory authority is the Swedish Authority for Privacy Protection (IMY), Box 8114, 104 20 Stockholm, Sweden (www.imy.se). This does not affect the rights of data subjects to lodge complaints with the supervisory authority competent in their jurisdiction.

17. CONTACT AND NOTICES

All notices and communications under this DPA shall be made in writing. ZealiD's DPA contact points are:

DPO: dpo@zealid.com — for all data protection queries, data subject rights requests, DPIA cooperation, and breach-related communications.

Legal: legal@zealid.com — for Sub-processor objections, audit requests, SCC queries, and formal legal notices.

Supervisory Authority: IMY (Integritetsskyddsmyndigheten) — www.imy.se — Box 8114, 104 20 Stockholm, Sweden.

ZealiD Trust Circle — Data Processing Agreement

Effective 1 March 2026 | ZealiD AB, Reg. No. 556972-4288 | GDPR Article 28 Compliant

For the current version of this document visit https://www.zealid.com/en/repository

ANNEX I

Details of Processing Activities

GDPR Article 28(3) — required particulars of processing

Purpose: This Annex sets out the mandatory particulars of processing required under GDPR Article 28(3) and the applicable Standard Contractual Clauses. It forms an integral part of this DPA.

I.1. PARTIES

Controller: The Account Holder identified in the Registration Flow or Order Form. Processor: ZealiD AB, Reg. No. 556972-4288, Norrlandsgatan 10, 111 43 Stockholm (visiting) / Box 3437, 111 56 Stockholm (postal).

I.2. SUBJECT MATTER AND NATURE OF PROCESSING

Subject matter: Provision of the Trust Circle SaaS platform for trusted document storage, collaboration, access management, and qualified signing workflows, as described in the GTC and Trust Circle Service Specification.

Nature of processing operations: collection (upload), storage, retrieval, access management, transmission (sharing), logging, backup, deletion, and technical support. Processing is carried out exclusively on documented Controller instructions.

I.3. PURPOSE OF PROCESSING

The sole purpose of ZealiD's processing under this DPA is to provide the Trust Circle service to the Controller in accordance with the GTC, this DPA, and the Controller's configuration of the Account.

I.4. CATEGORIES OF DATA SUBJECTS

ZealiD App — Mandatory Prerequisite: Every natural person who accesses Trust Circle has already completed TRA identity proofing and QeID certificate issuance via the ZealiD App as a mandatory prerequisite to Account activation. That onboarding processing (identity documents, biometric/liveness data, certificate issuance) is carried out by ZealiD as independent Controller under the TSPS, CPS, and ZealiD's Privacy Policy — it is not processing carried out on the Account Holder's instructions and is therefore not governed by this DPA. This DPA governs only the processing ZealiD performs as Processor on behalf of the Account Holder once the Account is active and in use.

- Authorised Users of the Controller's Account (employees, contractors, and other individuals granted access by the Account Holder). Each Authorised User with signing or authentication access will have individually completed TRA/QeID onboarding via the ZealiD App prior to being granted that access.
- Invited participants and counterparties — natural persons invited to view, collaborate on, or sign documents within the Controller's Account. Where such persons are signatories, they will also hold their own ZealiD App identity and qualified certificate.
- Any other natural persons whose personal data is contained within documents or other Account Content uploaded or processed by the Controller within Trust Circle.

I.5. CATEGORIES OF PERSONAL DATA

The categories of personal data processed depend on the content uploaded by the Controller and may include:

- Identity and contact data: names, email addresses, telephone numbers, postal addresses, and professional information.
- Authentication and access logs: login timestamps, IP addresses, session identifiers, and access records generated by Trust Circle.
- Document metadata: document names, upload timestamps, access history, signing events, and workflow status.
- Document content: personal data of any kind contained within documents uploaded by the Controller for storage, collaboration, or signing, which may include financial information, legal information, health information, or other personal data depending on the Controller's use case.
- Qualified signing data: where Trust Circle workflows invoke QeID, signing completion confirmations and transaction identifiers may be processed. The qualified certificate itself and its associated personal data are processed by ZealiD as independent Controller under the QeID CPS, not under this DPA.

Special Category Data: ZealiD does not knowingly process Special Category Data on behalf of Controllers unless explicitly configured to do so by the Controller. Controllers that upload documents containing Special Category Data are responsible for ensuring they have a valid legal basis under GDPR Article 9 and that appropriate additional safeguards are in place, as required by the DPA and the AUP.

I.6. DURATION OF PROCESSING

Processing under this DPA continues for the duration of the Account and for the post-termination period defined in the ZealiD Trust Circle Service Specification and Section 13 of this DPA. This is separate from and independent of the retention obligations applicable to TRA identity proofing records and QeID certificate records, which are retained by ZealiD as independent Controller for mandatory regulatory periods of up to 14 years (revoked certificates) and 12 years (issued certificates) as described in ZealiD's Privacy Policy and the applicable practice statements.

ANNEX II

Technical and Organisational Measures (TOMs)

GDPR Article 32 — measures to ensure appropriate security of processing

Certification: ZealiD's security controls are independently audited under ISO 27001 (Information Security Management) and ETSI EN 319 401/411/421 (Qualified Trust Service Provider standards). Current audit certificates are published in the ZealiD repository at https://www.zealid.com/en/repository.

II.1. DATA CENTRE AND INFRASTRUCTURE SECURITY

Control	Measure
Data location and sole control	All primary hosting, storage, and processing of Account Content takes place within ZealiD-managed, sole-operational-control infrastructure located in the European Economic Area (EEA), certified to ISO 27001 and ETSI EN 319 401. No third party has independent access to unencrypted Account Content. Sub-processors providing underlying infrastructure operate under ZealiD's encryption keys and access controls. Alternative hosting arrangements require written agreement per GTC §10.3 and DPA §11.1.
Encryption at rest	All Account Content is encrypted at rest using AES-256 or equivalent symmetric encryption. Database encryption is applied at the storage layer.
Encryption in transit	All data transmission between client and server is encrypted using TLS 1.2 or higher. Outdated cipher suites are disabled and configurations are reviewed regularly.
Physical security	Data centre facilities are protected by multi-layer physical access controls including badge access, biometric authentication, CCTV monitoring, and 24/7 security staffing.
Backup and recovery	Account Content is backed up daily with encrypted off-site copies. Recovery procedures are tested at least annually. Recovery time and recovery point objectives are defined in the SLA where applicable.

II.2. ACCESS CONTROL AND IDENTITY MANAGEMENT

Control	Measure
Least privilege	Access to personal data is restricted on a strict need-to-know basis. Role-based access control (RBAC) is applied to all systems processing personal data.
Multi-factor authentication	MFA is enforced for all ZealiD personnel accessing systems that process personal data, including all administrators and support personnel.
Privileged access management	Privileged and administrative access is subject to additional controls including session recording, just-in-time access provisioning, and regular access reviews.
User provisioning/deprovisioning	Automated provisioning and deprovisioning processes ensure timely removal of access rights upon termination of employment or role change.

Password policy	Strong password policies are enforced across all systems, including minimum length, complexity requirements, and prohibition of credential reuse.
Multi-tenancy isolation	Strict logical tenant isolation is enforced at the application and database layers to prevent any cross-Account data access.

II.3. APPLICATION SECURITY

Control	Measure
Secure SDLC	Security requirements are incorporated throughout the software development lifecycle (SDLC), including design review, threat modelling, code review, and pre-deployment security testing.
Vulnerability management	Continuous vulnerability scanning is performed across all production systems. Critical and high-severity vulnerabilities are remediated within defined SLAs. Penetration testing is conducted at least annually by independent third parties.
Web application firewall	A web application firewall (WAF) is deployed to detect and block malicious traffic, aligned with OWASP Top 10 guidance.
API security	API endpoints are protected by authentication, rate limiting, input validation, and output encoding controls.
Dependency management	Third-party dependencies and libraries are monitored for known vulnerabilities. Security patches are applied promptly.
Change management	All changes to production systems follow a documented change management process including security review, testing, and rollback procedures.

II.4. INCIDENT RESPONSE AND BUSINESS CONTINUITY

Control	Measure
Incident response plan	A documented incident response plan (IRP) is in place, covering detection, containment, eradication, recovery, and post-incident review. The IRP is tested at least annually.
Security monitoring	Continuous security monitoring and alerting is in place across all production systems, including SIEM, intrusion detection, and anomaly detection capabilities.
Breach notification procedure	Internal breach escalation procedures ensure that ZealiD's DPO is notified of any suspected Data Breach within twenty-four (24) hours of internal detection, enabling ZealiD to meet its 48-hour Controller notification obligation under Section 8 of this DPA.
Business continuity	A business continuity plan (BCP) and disaster recovery plan (DRP) are maintained and tested annually. Failover and recovery capabilities are designed to minimise service interruption and data loss.

II.5. ORGANISATIONAL MEASURES AND GOVERNANCE

Control	Measure
Data Protection Officer	ZealiD has appointed a Data Protection Officer (DPO) responsible for overseeing GDPR compliance. The DPO can be contacted at dpo@zealid.com.
Staff training	All ZealiD personnel receive data protection and information security training upon joining and at least annually. Personnel with access to personal data receive role-specific training.
Confidentiality undertakings	All personnel and contractors with access to personal data are bound by written confidentiality undertakings as part of their employment or engagement contracts.
Vendor due diligence	All Sub-processors and significant suppliers are subject to data protection due diligence before engagement and periodic review. Written DPA-equivalent agreements are in place with all Sub-processors.
Policy framework	ZealiD maintains a documented information security policy framework, data protection policies, and acceptable use policies that are reviewed and updated at least annually.
ISO 27001 / ETSI	ZealiD's information security management system is certified to ISO 27001 and its trust service operations are audited under ETSI EN 319 401/411/421. Current certificates are published at https://www.zealid.com/en/repository.

ANNEX III

Sub-Processor Framework

Current sub-processor list and change notification mechanics

Current List: The current list of Sub-processors engaged by ZealiD in connection with Trust Circle is maintained and published in the ZealiD repository at https://www.zealid.com/en/repository. Account Holders may subscribe to notifications of Sub-processor changes by registering at support@zealid.com.

III.1. SUB-PROCESSOR CATEGORIES

ZealiD currently engages Sub-processors in the following functional categories for Trust Circle. The specific entities, data processed, and transfer mechanisms are set out in the current Sub-processor list in the repository.

Category	Purpose	Data Location / Transfer Mechanism
Cloud Infrastructure / Hosting	Primary hosting, compute, and storage for Trust Circle platform	EU-based (EEA) — no third-country transfer
Backup and Disaster Recovery	Encrypted off-site backup and disaster recovery infrastructure	EU-based (EEA) — no third-country transfer
Security Monitoring (SIEM)	Log aggregation, intrusion detection, and security event monitoring	EU-based or SCCs where applicable
Customer Support Platform	Ticketing system for processing support queries that may reference Account details	EU-based or SCCs where applicable
Email Delivery	Transactional email (notifications, breach alerts, account communications)	SCCs / EU-U.S. Data Privacy Framework where applicable
Payment Processing	Credit card payment processing (Account Holder billing data only — no Account Content)	PCI-DSS certified; SCCs where applicable

III.2. CHANGE NOTIFICATION PROCESS

ZealiD will notify Controllers of any intended addition, replacement, or removal of a Sub-processor by:

(a) updating the Sub-processor list in the repository and publishing the effective date of the change;

(b) sending an email notification to the Account Holder's registered email address at least thirty (30) days before the change takes effect; and

(c) where a Business Account is subject to an Order Form, also notifying the named legal contact in that Order Form.

Controllers wishing to object to a Sub-processor change must do so within thirty (30) days of notification in accordance with Section 10.4 of this DPA.

ANNEX IV

International Transfer Mechanism

Standard Contractual Clauses and applicable transfer safeguards

Scope: This Annex applies to any transfer of personal data from the European Economic Area (EEA) to a third country in connection with ZealiD's processing as Processor under this DPA. Where all processing takes place within the EEA, this Annex does not apply.

IV.1. APPLICABLE SCCS

Where a transfer of personal data from the EEA to a third country is required in connection with ZealiD's performance of the Trust Circle service, the transfer shall be governed by the Standard Contractual Clauses for the transfer of personal data to third countries, as set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021. The applicable module shall be:

(a) Module 2 (Controller to Processor) — where the Account Holder is a Controller and ZealiD is acting as Processor transferring data to a third-country Sub-processor; or

(b) Module 3 (Processor to Processor) — where ZealiD is acting as Processor and is transferring data to a third-country Sub-processor.

The SCCs are incorporated into this DPA by reference. In the event of any conflict between this DPA and the SCCs, the SCCs prevail as provided in Section 14.3 of this DPA.

IV.2. COMPLETION OF SCC ANNEXES

For the purposes of the SCC Annex I, the particulars of the transfer are:

(a) Data exporter: the Account Holder (Controller) for Module 2 transfers; ZealiD AB for Module 3 transfers.

(b) Data importer: the relevant Sub-processor as identified in Annex III.

(c) Categories of data subjects and personal data: as described in Annex I of this DPA.

(d) Competent supervisory authority: IMY (Integritetsskyddsmyndigheten) where the data exporter is established in Sweden; the supervisory authority of the EEA Member State in which the data exporter is established for other cases.

The TOMs in Annex II of this DPA constitute the technical and organisational measures for SCC Annex II purposes.

IV.3. UK AND SWISS TRANSFERS

For transfers to or from the United Kingdom, the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs applies, as appropriate. For transfers to or from Switzerland, the Swiss Standard Contractual Clauses or such mechanism as approved by the Swiss Federal Data Protection and Information Commissioner (FDPIC) applies. The relevant transfer instrument is available on request from legal@zealid.com.

IV.4. TRANSFER IMPACT ASSESSMENTS

ZealiD has conducted Transfer Impact Assessments (TIAs) for all third-country transfers made in connection with Trust Circle. TIA summaries covering each Sub-processor's third-country transfer, the legal framework in the destination country, any supplementary measures applied, and ZealiD's conclusion on essential equivalence are available to Controllers on written request to legal@zealid.com, subject to execution of a confidentiality undertaking.

ZealiD Trust Circle — Data Processing Agreement

Annexes I–IV | Effective 1 March 2026 | ZealiD AB, Reg. No. 556972-4288

For the current version of this document visit https://www.zealid.com/en/repository