ZEALID TRUST CIRCLE

ACCEPTABLE USE POLICY

Effective Date: 1 March 2026 | Version 1.0 | Applies to all Trust Circle Account Holders and Authorised Users

Purpose: This Acceptable Use Policy (AUP) establishes the rules of conduct that apply to all use of ZealiD Trust Circle. Its purpose is to keep the platform secure, lawful, and reliable for every Account Holder, Authorised User, and the broader community of users and relying parties who depend on ZealiD's qualified trust services.

Who this applies to: This AUP applies to all Account Holders (Individual and Business), all Authorised Users, all API integrators and SDK users, all white-label and partner deployments, and any other person or entity accessing Trust Circle or ZealiD's trust services in any capacity. Operators deploying ZealiD services to their own end users remain responsible for ensuring their users comply with this AUP.

Relationship to the GTC: This AUP is incorporated by reference into the ZealiD Trust Circle General Terms & Conditions (GTC) and forms part of the binding agreement between ZealiD and every Account Holder. In case of conflict between this AUP and the GTC, the GTC prevails. Capitalised terms used but not defined here have the meanings given in the GTC.

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	All Trust Circle users —	No — regulatory, audited, non-negotiable

		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.	mandatory prerequisite	
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. Separate from and not governed by the DPA. Published at the repository.	All persons interacting with ZealiD directly	No — ZealiD's own controller obligations
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. Permitted Use
3. General Prohibitions
4. Identity, Signing, and Certificate Use
5. Identity Proofing (TRA)
6. Content and Data Standards
7. Platform Integrity and Security
8. API, SDK, and Integration Use
9. Fair Use
10. Operator and Reseller Obligations
11. Reporting Obligations
12. Enforcement
13. Quick Reference — Permitted and Prohibited Use
14. Document Reference

1. DEFINITIONS

Terms defined in the GTC have the same meaning in this AUP. In addition, for this AUP:

(a) "Account Holder" includes both natural persons and legal entities who have registered a Trust Circle Account.

(b) "Authorised User" means any person permitted by an Account Holder to access Trust Circle on its behalf.

(c) "Operator" means a Business Account Holder that deploys Trust Circle functionality (including via API, SDK, or white-label) to its own end users.

(d) "Prohibited Content" means any material whose upload, transmission, or storage is prohibited under Section 6 of this AUP.

(e) "Qualified Signing" means the creation of a qualified electronic signature using a subscriber's qualified certificate and QSCD under QeID.

(f) "Relying Party" has the meaning given in the QeID Certificate Practice Statement (CPS), being any natural or legal person that relies on a qualified certificate or qualified electronic signature.

2. PERMITTED USE

Trust Circle may be used for lawful, good-faith professional and personal purposes consistent with the Service's design. Permitted uses include:

- storing, organising, and managing documents and files for personal or business purposes;
- sharing documents securely with authorised counterparts, colleagues, or collaborators;
- initiating and completing document signing workflows, including qualified electronic signing via QeID;
- managing identity credentials and certificate-related information in connection with ZealiD App;
- integrating Trust Circle functionality into business processes via the ZealiD API or SDK, subject to Section 8;
- using Trust Circle to manage signing processes on behalf of a legal entity where the individual signing has their own valid qualified certificate and is duly authorised to sign; and
- any other use expressly authorised in writing by ZealiD or described in the Service Specification.

3. GENERAL PROHIBITIONS

Account Holders and Authorised Users must not use Trust Circle to engage in any of the following. This list is illustrative and not exhaustive — ZealiD reserves the right to determine that any use is prohibited where it poses a legal, regulatory, security, or reputational risk.

ILLEGAL AND HARMFUL CONDUCT

- ✕ Violate any applicable law or regulation, including data protection, export control, sanctions, or anti-money laundering laws.
- ✕ Engage in fraud, misrepresentation, identity theft, or any deceptive practice.
- ✕ Facilitate or participate in any form of financial crime, including money laundering or terrorist financing.
- ✕ Stalk, harass, threaten, or abuse any individual or entity.
- ✕ Infringe the intellectual property rights of any third party, including copyright, trade marks, patents, or trade secrets.

PROHIBITED CONTENT

- ✕ Upload, store, transmit, or share unlawful, defamatory, obscene, hateful, discriminatory, or privacy-invasive content.
- ✕ Process or transmit content that constitutes child sexual abuse material or any content that sexually exploits minors.
- ✕ Upload content containing malware, ransomware, viruses, Trojan horses, spyware, or any other harmful or malicious code.
- ✕ Transmit unsolicited commercial communications (spam), phishing messages, or any deceptive content.

IMPERSONATION AND MISREPRESENTATION

- ✕ Impersonate ZealiD, any ZealiD employee, any other Account Holder, or any third party.
- ✕ Misrepresent your identity, authority to sign, or affiliation with any organisation.
- ✕ Create or use an Account under false pretences or with false registration information.
- ✕ Use another person's ZealiD App identity, certificate, or credentials.

UNAUTHORISED ACCESS AND SECURITY

- ✕ Attempt to gain unauthorised access to Trust Circle, any other Account, ZealiD's infrastructure, or any connected system or network.
- ✕ Circumvent, disable, or interfere with any security control, authentication mechanism, rate limit, or access restriction.
- ✕ Conduct or facilitate any denial-of-service attack, distributed denial-of-service attack, or any other form of attack against ZealiD or any third party.
- ✕ Scan, probe, or test the vulnerability of ZealiD systems or networks without ZealiD's prior written consent.

4. IDENTITY, SIGNING, AND CERTIFICATE USE

4.1 Solo Application Requirement

Each individual must apply for and hold their own qualified certificate under QeID. Applications for qualified certificates must be made personally by the individual to whom the certificate will be issued. Applying for a certificate on behalf of another person is prohibited.

4.2 No Credential or Key Sharing

Each user must access Trust Circle and conduct Qualified Signing using only their own ZealiD App identity and qualified certificate. Private keys and authenticating factors (PIN, biometric) must never be shared with any other person or system. Enabling or facilitating any other person's access to a subscriber's private key is a serious violation of this AUP, the QeID CPS, and applicable law.

4.3 No Automated or Bot Signing

Automated, scripted, or programmatic execution of Qualified Signing using a subscriber's keys or credentials is strictly prohibited. Every qualified electronic signature must be the result of an active, individual, real-time decision by the human subscriber, initiated using their own ZealiD App and confirmed with their personal PIN or biometric. No robotic signing, unattended signing, or batch signing using subscriber credentials is permitted under any circumstances.

4.4 Age Requirement

All Account Holders and Authorised Users must be eighteen (18) years of age or older. ZealiD's TRA identity proofing process verifies this requirement. Accounts identified as belonging to users under eighteen will be suspended.

4.5 Certificate Validity Checks — Relying Parties

Any Relying Party wishing to rely on a qualified electronic signature or qualified certificate issued under QeID must verify certificate status before relying, using ZealiD's OCSP service at https://ocsp.zealid.com. Reliance on certificates without performing a validity and revocation check is at the Relying Party's own risk. Detailed reliance rules are set out in the QeID CPS published at https://www.zealid.com/en/repository.

4.6 Revocation Obligations

Subscribers must promptly request revocation of their qualified certificate if: (a) their private key has been compromised or is suspected of compromise; (b) they become aware of any unauthorised use of their certificate or signing credentials; or (c) any information in the certificate becomes inaccurate. Certificate revocation requests must be submitted via https://www.zealid.com/en/revocation.

5. IDENTITY PROOFING (TRA)

5.1 Accurate Information

When using ZealiD's TRA identity proofing service, Account Holders and Authorised Users must provide accurate, current, and complete information. Any attempt to provide false, misleading, or altered information during the identity proofing process — including submission of forged, altered, or borrowed identity documents — is a serious violation of this AUP and may constitute a criminal offence.

5.2 Cooperation with Liveness and Document Checks

Users undergoing TRA onboarding must cooperate fully and in good faith with all liveness detection, document scanning, and NFC chip verification processes. Attempts to circumvent, defeat, or manipulate liveness detection (for example by using photographs, videos, masks, or deepfakes) are strictly prohibited.

5.3 TRA Event Logs

ZealiD maintains event logs of all TRA identity proofing sessions in accordance with its regulatory obligations under the TSPS and applicable law. These logs are retained for the mandatory periods defined in the TSPS and ZealiD's Privacy Policy.

6. CONTENT AND DATA STANDARDS

6.1 Lawful Content Only

Account Holders may only upload, store, or transmit content that they have the legal right to use and share. This includes ensuring that any third-party content uploaded does not infringe the intellectual property rights of others, and that any personal data of third parties is processed in compliance with applicable data protection law.

6.2 Special Category and Sensitive Data

Where Account Content includes special category personal data within the meaning of GDPR Article 9 (including health data, biometric data, or data revealing racial or ethnic origin, political opinions, or religious beliefs), Account Holders must ensure: (a) a valid legal basis and explicit consent where required; (b) appropriate technical and organisational safeguards as required by the DPA; and (c) compliance with any applicable sector-specific regulation.

6.3 No Prohibited Content

Account Holders must not upload, store, transmit, or share any Prohibited Content as described in Section 3. ZealiD reserves the right (but has no obligation) to remove Prohibited Content and to suspend or terminate Accounts from which Prohibited Content is uploaded.

6.4 Lawful Basis for Processing

Account Holders who process personal data of third parties within Trust Circle (for example, by uploading documents containing personal data of counterparties) act as data controllers in respect of that data. They must ensure they have a valid lawful basis for such processing and have provided appropriate privacy notices to the data subjects concerned, in compliance with applicable data protection law and the DPA.

7. PLATFORM INTEGRITY AND SECURITY

7.1 No Reverse Engineering

Account Holders must not attempt to reverse engineer, decompile, disassemble, or otherwise derive source code or underlying algorithms from any part of Trust Circle or the ZealiD App. This includes any API, SDK, white-label component, or related software.

7.2 No Scraping or Automated Data Extraction

Automated scraping, crawling, mirroring, or bulk data extraction from Trust Circle is prohibited without ZealiD's prior written consent. This includes using bots, spiders, or other automated means to access or extract data from the Service.

7.3 No Scanning or Load Testing

Account Holders must not conduct vulnerability scanning, penetration testing, load testing, or performance testing of ZealiD's infrastructure, systems, or APIs without prior written approval from ZealiD. Requests for security testing authorisation should be directed to legal@zealid.com.

7.4 No Cross-Tenant Access

Account Holders must not attempt to access, view, copy, alter, or delete data belonging to any other Account or any other tenant of the Trust Circle platform. Any accidental access to another tenant's data must be reported immediately to support@zealid.com.

7.5 Responsible Disclosure

If an Account Holder discovers a security vulnerability or suspected security issue in Trust Circle or ZealiD's systems, they must report it promptly to support@zealid.com and must not exploit, publicise, or disclose the vulnerability to

any third party without ZealiD's prior written consent. ZealiD will acknowledge all security reports and respond within a reasonable time.

8. API, SDK, AND INTEGRATION USE

8.1 Developer Portal

API and SDK integrations must be implemented in accordance with the technical documentation published in the ZealiD Developer Portal at https://developer.zealid.com and the ZealiD Service Specification. Account Holders are responsible for maintaining their integrations and keeping them current with ZealiD's published API versions.

8.2 Rate Limits and Fair API Use

API calls must remain within the rate limits and fair-use parameters published in the Service Specification for the applicable plan tier. Account Holders must not attempt to circumvent rate limits by distributing requests across multiple accounts, IP addresses, or API keys. Sustained API usage that materially exceeds normal patterns may result in throttling, additional charges, or suspension pending discussion.

8.3 No Competing Use

Account Holders must not use API or SDK access to the Service to develop or improve a product or service that directly competes with ZealiD, where such development involves the use of ZealiD's Confidential Information or the derivation of competitive insights from ZealiD's technical implementation.

8.4 No Benchmarking

Account Holders must not access or use the Service for benchmarking purposes — whether for internal competitive analysis or publication — without ZealiD's prior written consent.

8.5 White-Label and SDK Derivatives

Account Holders deploying white-label or SDK derivatives of the ZealiD App must implement them in accordance with ZealiD's integration guidelines and must ensure that end users of such derivatives are bound by terms of use that incorporate the obligations of this AUP.

9. FAIR USE

Trust Circle is provided for good-faith use within the scope of the applicable plan tier. Account Holders agree that their use — including document storage volumes, signing transaction volumes, number of Authorised Users, and API call rates — shall remain within the bounds of normal, reasonable use consistent with the selected plan and the Service's intended purpose.

ZealiD reserves the right to:

- **(a)** apply rate limits, storage caps, or usage controls where an Account's use materially exceeds fair-use norms for its plan tier;
- **(b)** contact the Account Holder to discuss usage patterns before taking any enforcement action; and
- **(c)** require upgrade to a higher plan tier as a condition of continued use at elevated volumes.

Fair-use parameters and plan-tier limits are published in the ZealiD Trust Circle Service Specification at https://www.zealid.com/en/repository. ZealiD will update these parameters with reasonable notice where changes are material.

10. OPERATOR AND RESELLER OBLIGATIONS

10.1 Flow-Down of AUP Obligations

Operators and resellers who deploy Trust Circle to their own end users are responsible for ensuring that those end users comply with this AUP. Operators must incorporate the substantive obligations of this AUP into their own end-user terms of service and must take reasonable steps to enforce compliance.

10.2 No Expanded Rights

Operators may not grant their end users any rights in respect of Trust Circle that exceed the rights granted to the Operator under its agreement with ZealiD. Operators may not represent to their end users that any use prohibited under this AUP is permitted.

10.3 Notification of Breaches

Operators must promptly notify ZealiD at support@zealid.com if they become aware of any end user using Trust Circle in violation of this AUP, and must cooperate with ZealiD in investigating and remediating such violations. ZealiD may suspend an Operator's access to Trust Circle where an end-user AUP violation poses a security or regulatory risk and the Operator fails to act promptly.

11. REPORTING OBLIGATIONS

Account Holders must report the following to ZealiD promptly upon becoming aware:

- Any suspected or confirmed compromise of ZealiD App credentials, private keys, or qualified certificates — report to support@zealid.com and request revocation at https://www.zealid.com/en/revocation.
- Any security vulnerability, suspected breach, or unauthorised access to Trust Circle — report to support@zealid.com.
- Any use of Trust Circle that the Account Holder suspects may be unlawful, abusive, or in violation of this AUP by any Authorised User or third party.
- Any third-party claim or legal process received by the Account Holder in connection with their use of Trust Circle — report to legal@zealid.com.

Security Contact: For urgent security issues or suspected breaches, contact support@zealid.com. For certificate revocation, use https://www.zealid.com/en/revocation. For legal matters, contact legal@zealid.com.

12. ENFORCEMENT

12.1 ZealiD's Rights

ZealiD may take any of the following actions in response to a suspected or confirmed violation of this AUP, applicable law, or the GTC, with notice where practicable:

(a) issue a written warning to the Account Holder;

(b) remove or disable access to Prohibited Content;

(c) suspend access to part or all of Trust Circle pending investigation or remediation;

(d) permanently terminate the Account in accordance with Section 21 of the GTC;

(e) notify relevant regulatory authorities or law enforcement where required by applicable law or where ZealiD determines that notification is appropriate to protect the safety of persons or the integrity of the trust service; or

(f) in the case of certificate-related violations, initiate revocation of the relevant qualified certificate in accordance with the QeID CPS.

12.2 Immediate Suspension

Notwithstanding Section 12.1, ZealiD may suspend access to Trust Circle immediately and without prior notice where: (a) continued access poses a material security risk to the Service or other users; (b) the violation involves suspected fraud, identity theft, or criminal activity; or (c) ZealiD is required to act immediately under applicable regulatory obligations.

12.3 No Obligation to Monitor

ZealiD has no obligation to proactively monitor Account Content or Account Holder activity for AUP violations. The absence of enforcement action in respect of any particular conduct does not constitute ZealiD's approval or acceptance of that conduct.

12.4 Appeals

Account Holders who believe a suspension or enforcement action has been taken in error may appeal by contacting legal@zealid.com with full details of the circumstances. ZealiD will review appeals in good faith and respond within ten (10) business days. Submission of an appeal does not automatically suspend an enforcement action.

13. QUICK REFERENCE — PERMITTED AND PROHIBITED USE

The table below provides a summary for reference only. The detailed provisions of this AUP prevail in all cases.

Area	✓ Permitted	✕ Prohibited
Signing	Signing with your own ZealiD App identity and personal PIN/biometric	Sharing credentials, proxy signing, automated/robot signing, signing for another person
Identity Proofing	Accurate, genuine ID documents; good-faith liveness checks	Forged or altered documents; deepfakes or photos used for liveness; applying for certificates on behalf of others
Content	Lawful documents you have the right to use; properly consented personal data	Unlawful, defamatory, infringing, or privacy-invasive content; malware; spam

API / Integration	API use within rate limits for your plan; developer portal compliance	Circumventing rate limits; reverse engineering; benchmarking; competing product development using ZealiD IP
Security	Responsible disclosure of vulnerabilities; prompt reporting of incidents	Scanning/probing without consent; cross-tenant access; defeating security controls
Data	Lawful processing with valid basis; DPA compliance	Processing without lawful basis; uploading special category data without safeguards
Certificate Reliance	OCSP checks before relying; following CPS reliance rules	Relying on certificates without status check; ignoring revocation notices

14. DOCUMENT REFERENCE

This AUP should be read together with the following ZealiD documents, all published at https://www.zealid.com/en/repository:

- ZealiD Trust Circle General Terms & Conditions (GTC) — the primary commercial terms of which this AUP forms part
- ZealiD Trust Circle Data Processing Agreement (DPA) — governing personal data processing
- ZealiD Trust Circle Service Specification — plan tiers, fair-use parameters, and feature descriptions
- TSPS — TRA Service Practice Statement — governing ZealiD's identity proofing service
- QeID Certificate Practice Statement (CPS) — governing qualified certificate issuance and reliance
- ZealiD Privacy Policy — how ZealiD processes personal data as data controller

Updates: This AUP may be updated by ZealiD at any time. Material changes will be notified via the Trust Circle portal or by email in accordance with Section 6.1 of the GTC. The current version is always available at https://www.zealid.com/en/repository.

ZealiD Trust Circle — Acceptable Use Policy

Effective 1 March 2026 | ZealiD AB, Reg. No. 556972-4288 | www.zealid.com

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