ZealiD

Amendment to Service Agreement – DORA Compliance Addendum

DORA Operational Resilience and ICT Risk Management

This Addendum ("Addendum") amends the Service Agreement between ZealiD AB ("ZealiD") and the Customer, who is a financial entity subject to Regulation (EU) 2022/2554 ("DORA"). This Addendum incorporates specific contractual provisions required under Articles 28–30 of DORA.

---

1. Scope and Nature of Services

ZealiD provides qualified electronic identification, authentication, and signature services, including remote identity verification and certificate lifecycle management. The nature and scope of the services are fully described in the following official ZealiD documents, available at zealid.com/repository which are incorporated by reference:

- **Service Specification**, version 202305, ZealiD Service Specification
- **QeID Certificate Practice Statement (CPS)** and **TSPS** statements
- **ZealiD SLAs**, version 2024
- **ZealiD TÜV Certificate of Conformity (ID: 97227.24)**

These documents detail the technical, legal, and operational characteristics of the service, including scope, delivery methods (e.g., ZealiD App, API, SDK, and white-label solutions), security controls, and identity proofing mechanisms.

---

2. Security and Resilience Obligations

ZealiD shall:

- Operate an ETSI 319 401 Information Security Management System (ISMS).
- Maintain 99.5% annual service availability for authentication and signing services ZealiD SLAs 2024.
- Use EU-based infrastructure with multi-layered physical and logical security controls (TSPS §5.1).
- Perform regular risk assessments and maintain an annual audit schedule (TSPS §5.4, CPS §8.1).

ZealiD

3. Audit and Inspection Rights

3.1 **Access for Customer and Supervisory Authorities**
ZealiD shall allow the Customer and relevant EU authorities, with 30 days prior written notice, to:

- Request access to policies, logs, test plans, and certifications.
- Interview personnel in trusted roles where relevant to compliance.
- Conduct inspections on premises, subject to Section 3.2 below.

3.2 **Audit Conditions**
To safeguard ZealiD's operational integrity, audits shall:

- Be limited to systems directly involved in providing the service.
- Be conducted during business hours (CET).
- Be subject to confidentiality agreements and pre-approved scopes.

3.3 **Cost Recovery**
ZealiD reserves the right to charge for audit facilitation services, including staff time and logistics, unless the audit arises from a material breach.

---

4. Incident Reporting and Collaboration

ZealiD shall:

- Notify the Customer within 24 hours of detecting a significant ICT-related incident.
- Provide detailed updates, root cause analysis, and post-incident reports.
- Cooperate with supervisory authorities as required under Article 19(1) of DORA.

---

5. Subcontracting and Location of Services

- ZealiD will not subcontract core ICT functions without prior notification to the Customer.
- All services are operated from secure facilities in Sweden and Lithuania.
- Cross-border transfers of data outside the EU/EEA will only occur with adequate safeguards.

---

6. Termination and Exit Support

Upon termination, ZealiD will:

- Ensure continuity of services during a transition period of up to 90 days.
- Provide access to all customer data and documentation necessary for orderly disengagement.
- Retain security and audit logs for a minimum of 12 years (TSPS §5.5).

---

7. Information Repository

All supporting documents available 24/7 at https://www.zealid.com/repository

---

8. Governing Law

This Addendum shall be governed by the laws of Sweden and interpreted in conjunction with the Service Agreement and Purchase Order. Compliance with DORA is deemed a material obligation.