TRUSTY DORA ADDENDUM

Digital Operational Resilience Act (Regulation (EU) 2022/2554)
Non-Critical ICT Third-Party Service Provider

1. Purpose and Scope

This Digital Operational Resilience Act Addendum (the **"DORA Addendum"**) supplements the Trusty Terms of Service and any applicable Additional Terms (together, the **"Agreement"**) entered into between **Trusty AG, Hünenberg, Switzerland** (the **"Provider"**) and the legal entity subscribing to the Application (the **"Client"**).

This DORA Addendum applies where the Client qualifies as, or acts on behalf of, a **financial entity** within the meaning of Regulation (EU) 2022/2554 on digital operational resilience in the financial sector (**"DORA"**), and where the services provided by the Provider constitute **ICT services** within the meaning of Article 3(21) DORA.

For the purposes of DORA, the Provider acts as a **non-critical ICT third-party service provider**.

2. Regulatory Context and Interpretation

1. This DORA Addendum is intended to support the Client's compliance with applicable requirements of DORA, in particular Articles 11–12 and Articles 28–30.
2. Capitalised terms not defined herein shall have the meanings given to them in the Agreement or in DORA.
3. Nothing in this DORA Addendum shall be interpreted as designating the Provider as a critical or important ICT third-party service provider within the meaning of DORA.
4. In the event of any conflict between this DORA Addendum and the Agreement, this DORA Addendum shall prevail solely to the extent required to ensure compliance with DORA.

3. Description of ICT Services

1. The scope, nature, and characteristics of the ICT services provided by the Provider are described in the Agreement and the applicable Application Additional Terms.
2. Information regarding service availability, incident handling, business continuity, and disaster recovery is governed contractually by the Agreement and operationally by the Provider's internal policies.
3. The locations of data processing and storage are defined in the Agreement and the Data Processing Agreement. The Provider shall notify the Client without undue delay of any material changes thereto.

4. ICT Risk Management and Information Security

1. The Provider maintains appropriate administrative, technical, and organisational measures designed to ensure the availability, authenticity, integrity, and confidentiality of data and ICT services.
2. The Provider maintains an information security and risk management framework aligned with recognised standards, including ISO/IEC 27001 or equivalent.
3. Upon reasonable request, the Provider shall make available high-level information enabling the Client to assess the Provider's ICT risk management and security posture for DORA purposes.
4. The Provider maintains internal programmes for ICT security awareness and digital operational resilience, including periodic training of relevant personnel. Upon reasonable request, the Provider shall make available high-level

TRUSTY

information regarding such programmes for the purpose of the Client's DORA compliance. Where the Client requires participation in its own awareness or training programmes, the Provider may rely on equivalent training already performed, where such equivalence can be reasonably demonstrated.

5. ICT-Related Incident Management

1. The Provider maintains internal procedures for the identification, classification, handling, and remediation of ICT-related incidents affecting the ICT services.
2. The Provider shall notify the Client without undue delay after becoming aware of any ICT-related incident that materially affects, or is reasonably likely to materially affect, the provision of ICT services to the Client.
3. Where an ICT-related incident triggers regulatory reporting obligations for the Client under DORA, the Provider shall provide reasonable cooperation and information support to enable such reporting.
4. Detailed incident response timelines, escalation mechanisms, and resolution targets are governed by the Agreement and the Provider's internal incident management framework and do not constitute guaranteed service levels unless expressly agreed.
5. The Provider shall notify Clients of ICT-related incidents in accordance with this Section via the Provider's designated incident reporting channels, as communicated to the Client from time to time, including via the Provider's support portal or designated security contact address. Clients shall designate appropriate contact details for the receipt of incident notifications. Unless otherwise agreed, incident notifications shall be deemed received when sent to the contact details last provided by the Client.
6. Where an ICT-related incident constitutes a personal data breach within the meaning of applicable data protection law, the Provider shall notify the Client in accordance with the Data Processing Agreement and via the Provider's designated data protection contact channels.

6. Business Continuity and Disaster Recovery

1. The Provider maintains business continuity and disaster recovery arrangements proportionate to the nature, scale, and complexity of the ICT services provided.
2. Such arrangements are designed to support the continuity and recoverability of critical ICT services following severe disruptions.
3. The Provider tests its continuity and recovery arrangements periodically and reviews them in light of test results, incidents, and changes to the ICT environment.
4. Upon reasonable request, the Provider shall provide the Client with high-level information regarding the existence and governance of its continuity and recovery framework.

7. Sub-Outsourcing

1. The Provider may engage subcontractors for the provision of ICT services in accordance with the Agreement and the Data Processing Agreement.
2. The Provider remains fully responsible for the performance of subcontracted ICT services vis-à-vis the Client.
3. The Provider ensures that material subcontractors are subject to contractual obligations that are substantially equivalent to those applicable to the Provider under this DORA Addendum.

8. Access, Audit, and Information Rights

1. The Provider shall make available to the Client information reasonably necessary to assess the Provider's compliance with this DORA Addendum and applicable DORA requirements. Such information may include documentation, certifications, questionnaires, policies, or third-party audit reports.

2. Where required by applicable law or by a competent supervisory authority, the Provider shall permit audits or inspections relating to the ICT services provided to the Client. Audits may be conducted remotely or on-site, as appropriate, and shall be subject to reasonable notice unless a shorter notice period is required by law or a supervisory authority.
3. Audits and inspections shall be conducted in a manner that is proportionate, reasonably limited in scope, and designed to minimise disruption to the Provider's operations and to protect the confidentiality, security, and integrity of the Provider's systems and of other clients' data.
4. The Client shall bear the reasonable and documented costs incurred by the Provider in connection with audits or inspections requested by the Client including preparation time, personnel involvement, and reasonable external advisory or audit support, provided that:
    (a) no fees shall be charged for the provision of existing certifications, standard documentation, or responses to routine information requests;
    (b) any chargeable costs shall be proportionate to the scope and duration of the audit and, where reasonably practicable, agreed in advance; and
    (c) no fees shall be charged for audits or inspections mandated directly by a competent supervisory authority, except to the extent permitted by applicable law.

9. Cooperation with Supervisory Authorities

1. The Provider shall cooperate in good faith with competent supervisory authorities where required to enable the Client to comply with its obligations under DORA, including by providing relevant information relating to the ICT services.
2. The Provider shall inform the Client without undue delay of any circumstance that may materially impair the provision of the ICT services or materially affect the Provider's ability to comply with this DORA Addendum.
3. Where cooperation with competent supervisory authorities or regulator-driven requests requires material additional effort beyond the Provider's standard operational and compliance activities, the Provider may charge the Client for the reasonable and documented costs incurred, provided that such charges do not restrict, delay, or prevent compliance with binding legal or regulatory obligations.

10. Charges for Audit and Regulatory Support

1. Where the Provider is entitled to charge costs in accordance with Articles 8 and 9 of this DORA Addendum, such services shall be provided on a time-and-materials basis at the Provider's standard professional services rate.
2. Unless otherwise agreed in writing, the Provider's standard rate for audit, inspection, and regulatory cooperation services is CHF 250 per hour.
3. Billing shall be based on actual time spent, rounded to the nearest half hour. Reasonable out-of-pocket expenses incurred in connection with on-site audits or inspections may be charged separately where applicable.

11. Termination and Exit

1. The Client may terminate the Agreement where required by applicable law or upon binding instruction by a competent supervisory authority under DORA.

2. Upon termination, the Provider shall provide reasonable cooperation for a limited transition period to support the orderly transfer of ICT services or Client data, in accordance with the Agreement.

3. Data return and deletion shall be governed by the Agreement and the Data Processing Agreement.

12. Amendments

The Provider may update this DORA Addendum where necessary to reflect changes in applicable law or regulatory guidance. Updated versions shall be published on the Provider's website and apply in accordance with the Terms of Service.

12. Governing Law

This DORA Addendum shall be governed by and construed in accordance with the governing law specified in the Trusty Terms of Service.

PUBLISHED ON January 29, 2026