TAIGA DORA ADD-ON

Version: v1.0, effective 6 September 2026

1. WHEN THIS APPLIES

Banks and insurers cannot sign an ICT contract without the terms Article 30 of DORA prescribes. This add-on supplies them so that nobody has to draft them deal by deal.

This Add-on forms part of the Agreement where the Customer is a financial entity within the meaning of Regulation (EU) 2022/2554 (DORA); no election is needed. Section 3 applies additionally where the Customer has notified Taiga in writing that the Services support a critical or important function. Where it applies, this Add-on prevails over the Master Service Terms and Schedules on the matters it covers; where the Public Sector Rider is also activated, clause 1.1 of the Master Service Terms says which prevails on what. Terms defined in the Master Service Terms have the same meaning here.

2. TERMS FOR EVERY FINANCIAL ENTITY

The Article 30(2) list, in order: what we do, where, how we protect it, how you get it back, service levels, incident help, regulators, and how it ends.

(a) Description of the Services. Learn and Deliver + Operate as described in clause 3 of the Master Service Terms and the Service Description, in the hosting mode chosen in the Platform. Subcontracting of a Service supporting a critical or important function is permitted only to the subprocessors listed in Schedule B and to others the Customer has approved in writing under section 3(f).

(b) Locations. The Services are provided from, and Customer Content is processed and stored in, the European Union: AWS eu-central-1 (Frankfurt), with model inference through Amazon Bedrock in EU regions. Taiga gives the Customer not less than ninety (90) days’ written notice before changing a processing or storage location.

(c) Availability, authenticity, integrity and confidentiality. Schedule B (security), Schedule A (availability), clause 10 (confidentiality) and Schedule D (personal data) of the Master Service Terms apply, together with the tamper-evident audit trail retained for seven years.

(d) Access, recovery and return. On Taiga’s insolvency, resolution, discontinuation of its business or the termination of the Agreement, the Customer may access, recover and retrieve all Customer Content and Delivered Software in a structured, commonly used, machine-readable format, under Schedule C, without charge and without any condition as to payment.

(e) Service levels. Schedule A states the availability target, its measurement and the credits. Taiga updates the Customer without undue delay of any development that may materially affect its ability to meet them.

(f) Incident assistance. Where an ICT-related incident connected to the Services occurs, Taiga provides assistance at no additional cost within the support included in Schedule A, and beyond it at a cost agreed in writing before the work, which is known before the Services begin.

(g) Cooperation with authorities. Taiga cooperates fully with the Customer's competent authorities and resolution authorities, including by answering their requests and giving them the access described in section 3(d) where that section applies.

(h) Termination. In addition to its rights under the Master Service Terms, the Customer may terminate the Agreement or the affected Service with immediate effect on written notice where Taiga materially breaches applicable law, regulation or the Agreement; where circumstances identified in the Customer's ICT third-party risk monitoring alter the performance of the Services, including a material change to Taiga's ownership, control, subcontracting chain, financial position or processing locations; where Taiga shows evidenced weaknesses in its ICT risk management; or where the Customer's competent authority directs it. No charge, penalty or clawback attaches to such a termination, and Schedule C applies in full. Taiga does not terminate for convenience on less than three (3) months' written notice, six (6) where section 3 applies, and never before the end of a committed term.

(i) Training. On request, Taiga's staff who serve the Customer participate, on terms agreed in writing in advance, in the Customer's ICT security awareness and digital operational resilience training.

(j) Register of information. Taiga supplies, at onboarding and on change, the data the Customer needs for its register of information under Article 28(3) of DORA: Taiga's identifiers (EUID, and an LEI on request), its subcontracting chain, the processing and storage locations, the governing law, the function supported and the annual expenditure. Taiga notifies the Customer of any change in its ownership or subcontracting chain within thirty (30) days.

(k) Incident notification. For this Add-on the notification period in clause 12 of the Master Service Terms is twelve (12) hours from Taiga becoming aware.

3. CRITICAL OR IMPORTANT FUNCTIONS

The Article 30(3) layer. Unrestricted audit, penetration-test participation, tested contingency plans and a real exit plan. It costs us real time, and we say so.

Where the Customer has notified Taiga in writing that the Services support a critical or important function:

(a) Service levels. Schedule A and the Service Description apply with the precise quantitative targets stated there and any additional qualitative or quantitative target agreed in writing, with updates without undue delay.

(b) Contingency. Taiga maintains and tests annually a business contingency plan for the Services, including the loss of access to a model provider or a cloud region, and provides the test summary on request.

(c) Threat-led penetration testing. Taiga participates in and cooperates fully with threat-led penetration testing the Customer is required to carry out, on reasonable notice, with test execution costs borne by the Customer and remediation of Taiga-attributable findings at Taiga’s cost.

(d) Audit and inspection. The Customer, a third party it appoints, and its competent and resolution authorities have unrestricted rights of access, inspection and audit of the Services and of the premises and systems used to provide them, including the right to take copies, on reasonable notice save where an authority requires otherwise. Taiga may refuse as third-party auditor only a direct competitor. Nothing in clause 12 of the Master Service Terms narrows this right.

(e) Exit. Schedule C applies with a mandatory transition period of not less than the transitional period there, extended as the Customer’s exit plan reasonably requires, and Taiga maintains a documented exit strategy for the Services, reviewed annually, and provides it on request.

(f) Subcontracting. No subcontractor supports a critical or important function without the Customer’s prior written approval; Taiga gives not less than ninety (90) days’ notice of an intended change, and the Customer may object or terminate the affected Service without charge. This overrides the objection right in Schedule D.

4. WHAT THE CUSTOMER SHOULD KNOW

Taiga holds no ISO/IEC 27001 certificate and no SOC 2 report, and no third-party penetration test has been carried out; the information security management system is operating and certification is in progress, as Schedule B records. The first substantive external test of the Platform may be the Customer’s. Taiga’s position is that stating this plainly is worth more than a contract that reads better than the company.

Stated plainly so that the assessment starts from the truth.