DORA ADDENDUM

This Digital Operational Resilience Act Addendum ("Addendum") supplements the Master Services Agreement, Order Form, or other written or electronic terms (the “Agreement”) under which Nintex ("Nintex") supplies the Services to the customer identified in the Agreement ("Customer"). This Addendum applies exclusively to Customers subject to Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("DORA") and takes precedence over any conflicting terms in the Agreement with respect to the subject matter herein.

1. DEFINITIONS

Unless otherwise defined in this Addendum, capitalized terms shall have the meanings set forth in the Agreement.

"Competent Authority" or "Regulator" means any government, regulatory body, or competent authority in the European Economic Area with binding authority to regulate Customer's activities as a Financial Entity under DORA, including any resolution authority.

"Customer Data" means data uploaded, stored, or submitted for processing by Customer through the Services, including personal and non-personal data.

"DORA" means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

“DPA” means the data processing agreement or data processing addendum, as applicable, between Customer and Nintex governing the processing of personal data by Nintex on behalf of Customer.

"Financial Entity" means an entity captured by Article 2(2) of DORA and which is not excluded from the scope of DORA by Article 2(3) or 2(4) of DORA.

"ICT-Related Incident" means a single event or a series of linked events unplanned by Customer that compromises the security of network and information systems and has an adverse impact on the availability, authenticity, integrity, or confidentiality of Customer Data, or on the services provided by Customer.

"ICT Services" has the meaning given in DORA and, for purposes of this Addendum, refers to the Services provided under the Agreement that constitute ICT services under DORA.

"Service Levels" means the service level commitments set forth in the Agreement.

"Subcontractor" means a third party engaged by Nintex in connection with the ICT Services which performs operations involved in the delivery of the Services and/or processes Customer Data.

2. SCOPE AND APPLICABILITY

2.1 This Addendum applies only to the extent that (a) Customer qualifies as a Financial Entity under DORA, and (b) the Services constitute ICT Services under DORA.

2.2 Customer acknowledges and agrees that the Services do not support a critical or important function of Customer within the meaning of DORA. Accordingly, the Parties agree that the Services are subject to the contractual provisions set forth in Article 30(2) of DORA and are not subject to the additional contractual obligations set forth in Article 30(3) of DORA.

3. KEY CONTRACTUAL PROVISIONS

3.1 Description of Services. The description of the ICT Services is set forth in the Agreement.

3.2 Location of Services and Data Processing. Nintex provides the Nintex Services from global locations. Processing locations for the ICT Services are more specifically identified in relevant Service documentation, Agreement, and DPA. Nintex shall not materially change the country or region for provision of the ICT Services without providing reasonable prior notice to Customer. In addition, the data storage and processing locations of Customer Data might be added or changed in connection with the Service in cases where Nintex engages a new subcontractor and Customer will be informed in line with the process agreed under the DPA.

3.3 Data Security. Nintex will implement and maintain appropriate technical and organizational measures designed to protect the availability, authenticity, integrity, and confidentiality of Customer Data as described in the Agreement and the DPA. Nintex maintains an information security program aligned with industry standards. Information regarding Nintex's security practices and certifications is available at the Nintex Trust Vault (https://security.nintex.com/).

3.4 Data Access, Recovery, and Return. Nintex provides Customer with the ability to access, export, and delete Customer Data during the term of the Agreement through functionality available within the Service. In the event of termination of the Agreement for any reason, or in the event of Nintex's insolvency, resolution, or discontinuation of business operations, Nintex will provide Customer with access to Customer Data as provided for in the Agreement.

3.5 Service Levels. Nintex shall provide the ICT Services in accordance with the Service Levels. Nintex monitors the availability of the Services and documents availability at https://status.nintex.com/.

3.6 ICT-Related Incident Assistance. Nintex shall provide assistance to Customer when an ICT-Related Incident occurs that is related to the ICT Services. In the event of an ICT-Related Incident that could have a material adverse impact on the continuity or security of the Services, Nintex will without undue delay:

(a) notify Customer of the ICT-Related Incident;

(b) provide Customer with reasonably requested information that Nintex has regarding the ICT-Related Incident that Customer needs to secure Customer's functions at risk; and

(c) provide Customer with reasonably requested information on how Nintex handled the ICT-Related Incident.

To the extent an ICT-Related Incident is caused by Customer or assistance is requested beyond the scope of the Agreement, Nintex shall be entitled to compensation for such assistance and reasonable costs at Nintex's then-current rates.

3.7 Cooperation with Competent Authorities. To the extent required under DORA, Nintex shall cooperate with Customer's Competent Authorities, including persons appointed by them, in connection with the ICT Services provided to Customer, provided that Customer does not otherwise have access to the relevant information.

3.8 Termination Rights. In addition to any termination rights set forth in the Agreement, Customer may terminate the Agreement with respect to the ICT Services by providing written notice to Nintex in the following circumstances:

(a) Nintex is in material breach of applicable laws, regulations, or this Addendum, and Nintex fails to cure such breach within 30 days after receipt of written notice from Customer specifying the breach in sufficient detail;

(b) Customer identifies objectively evidenced circumstances that are directly attributable to Nintex that are capable of materially altering the performance of the ICT Services, including material changes to the Agreement or material change in Nintex's situation, such as change of control, commencement of insolvency or resolution proceedings, or material adverse regulatory action directly impacting Nintex's ability to perform the ICT services, and Nintex fails to remediate such circumstances within 30 days after receipt of written notice from Customer;

(c) Nintex has evidenced pertaining to its overall ICT risk management, in particular in the way it ensures the availability, authenticity, integrity, and confidentiality of Customer Data, and Nintex fails to take reasonable steps to remediate such weaknesses within 30 days after receipt of written notice from Customer; or

(d) Customer's Competent Authority instructs Customer to terminate the Agreement, provided that Customer provides Nintex with reasonable evidence of such instruction.

Termination shall not relieve Customer of any payment obligations for Services rendered prior to termination. Payment of fees shall be governed as set forth in the Agreement.

3.9 Security Awareness Training. Upon written request by Customer, Nintex may provide Customer with details regarding Nintex's own security awareness training programs appropriate for the purpose of DORA. Where additional training is required, Customer may, subject to mutually agreed terms and at Customer's expense, request Nintex to participate in Customer's virtual security awareness programs or digital operational resilience training where appropriate.

4. CONFIDENTIALITY

Information shared in connection with this Addendum, including responses, audit reports, security documentation, and any other information provided by Nintex or by Customer in connection with this Addendum, shall be treated as Confidential Information in accordance with the Agreement.

5. MISCELLANEOUS

5.1 Conflict. In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail with respect to ICT Services subject to DORA, except that the DPA shall control with respect to personal data as specified therein. For the purposes of this Addendum, the rights and obligations of the parties in this Addendum are in addition to, and not in re placement of, the rights and obligations of the parties in the Agreement, except that this Section will prevail over any conflicting term in the Agreement. For the avoidance of doubt, the liability of the parties arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. Except as amended by this Addendum, the Agreement will remain in full force and effect.

5.2 Termination of Addendum. This Addendum shall terminate automatically upon the expiration or termination of the Agreement.

5.3 Sole Remedy. Customer's sole and exclusive remedy for any breach by Nintex in relation to this Addendum is to terminate this Addendum and the applicable Agreement for the affected ICT Services in accordance with Section 3.8.

5.4 Updates to DORA. Where a provision of DORA or delegated legislation made pursuant to DORA is superseded, invalidated, or replaced by law or regulation, the Parties shall negotiate in good faith to update this Addendum accordingly.

5.5 Standard Contractual Clauses. To the extent that any standard contractual clauses are developed by competent authorities or European Union institutions under DORA concerning the subject matter of this Addendum, the Parties shall negotiate in good faith to incorporate such standard contractual clauses as applicable.

5.6 Governing Law. This Addendum shall be governed by and construed in accordance with the governing law provisions in the Agreement.