altaFlow

DORA Addendum

This Addendum ("**DORA Addendum**") amends and forms part of the Agreement (as defined below) between Provider and you ("**Customer**").

1. Definitions

For purposes of this DORA Addendum, the following terms will have the following meaning:

"Agreement" means any agreement between Provider and Customer for the Services. Such an agreement may have various titles, such as "Order Form," "Sales Order," "Terms of Use," "Terms of Service," "SaaS Agreement," "Services Agreement," "Data Processing Addendum".

"**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 and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

The following terms have the same meaning as in DORA: **"critical or important functions**", "**cyber attack**", "**cyber threat**", "**digital operational resilience**", "**ICT subcontractor established in a third country**", "**ICT risk**", "**ICT services**", "**ICT third-party risk**", "**ICT third-party service provider**", and "**major ICT-related incident**."

All other capitalized terms have the same meaning as in the relevant Agreement.

2. Scope and Application.

This DORA Addendum only applies where Customer is a covered entity under DORA, Provider is an ICT third-party service provider, and Provider's services provided to Customer under the Agreement are "ICT services." In the event of a conflict between this DORA Addendum and the Agreement, the DORA Addendum will prevail.

3. Provider's Obligations.

3.1 Sub-contracting. Provider engages ICT subcontractors established in a third country ("ICT subcontractors") to assist with processing Customer Data pursuant to the Agreement. The Provider must enter into contractual arrangements with such ICT subcontractors requiring an equivalent level of compliance with the terms described in this DORA Addendum and must maintain appropriate oversight and control of such ICT subcontractors. Provider must maintain an up-to-date list of ICT subcontractors at https://legal.altaflow.com/subprocessors (as updated from time to time). The Provider will inform about any updates to https://legal.altaflow.com/subprocessors concerning the addition or replacement of ICT subcontractors at least ten (10) calendar days before the new ICT subcontractor processes Customer Data. For their own convenience, the Customer may subscribe to a Subprocessor List update via the Subprocessor Action Request Form. Customer may object to such changes in writing within five (5) calendar days of such update, provided that such objection is based on a material risk such change poses to Customer under DORA (an "**Objection**"). In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution. If the parties are not able to achieve a resolution, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience, on the condition that Customer provides written notice to the Provider within five (5) calendar days of being informed of the engagement of the ICT subcontractor. Customer will not be entitled to any refund of fees paid prior to the date of any termination pursuant to this Section.

3.2 ICT Service Locations. The locations where the contracted and subcontracted functions of the ICT services are provided, including where data is processed or stored, are described at https://legal.altaflow.com/subprocessors (as updated from time to time). Any changes to such locations must be disclosed as described in 3.1 above.

3.3 Security of Data. The provisions on availability, authenticity, integrity, and confidentiality regarding the protection of data, including personal data, are further described in the Provider's DPA at https://legal.altaflow.com/dpa.

3.4 Data Recovery. In the event Provider becomes insolvent, discontinues business operations, or terminates the contract, it will make available features or provide support to Customer to ensure access, recovery, or return to Customer of Customer Data, including Personal Data and non-Personal Data processed by the ICT service.

3.5 Service Level Agreement. The ICT services service levels are provided to the Customer as described in the Agreement.

3.6 ICT Incident Response. Provider shall establish, maintain, and document an ICT incident management process capable of detecting, managing, recording, and resolving ICT-related incidents. This process shall cover all ICT-related incidents impacting the provision of the Service, including but not limited to those affecting the confidentiality, integrity, or availability of the ICT systems or services, as well as personal data breaches.

Provider shall classify all such incidents in accordance with the criteria and materiality thresholds for a "Major ICT-related incident" or a "Significant Cyber Threat" as specified in the DORA Regulation (Regulation (EU) 2022/2554) and the associated Regulatory Technical Standards (RTS) on incident classification.

In the event of a major ICT-related incident impacting the Service, the Provider shall promptly notify the Customer's designated incident response contact, becoming aware of the incident, to enable the Customer to meet its mandatory regulatory reporting obligations.

3.7 Cooperation with Competent Authorities. Provider will fully cooperate with Customer and its competent authorities in accordance with DORA Article 30(2)(g).

3.8 Termination. The parties (i) are entitled to terminate provisions of the Agreement related to the ICT services and (ii) will provide each other with notice of termination as specified in the Agreement. In addition to the termination rights provided in the Agreement, Customer will be permitted to terminate provisions of the Agreement relating to the ICT Services that meet one or more of the following conditions specified in DORA Article 28(7)(a):

a) significant breach by the ICT third-party service provider of applicable laws, regulations, or contractual terms;

b) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;

c) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and, in particular, in the way it ensures the availability, authenticity, integrity, and confidentiality of data, whether personal or otherwise sensitive data, or non-personal data;

d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.

Upon termination, Customer is responsible for ensuring that it has retrieved or retained all information and assets from the ICT services.

3.9 Security Training and Awareness. Provider will ensure its personnel responsible for the ICT services have received appropriate security awareness and digital operational resilience training. Where Customer identifies Provider's training is not sufficient to meet the ICT security awareness training programs and digital operational resilience training as specified in DORA's Article 13(6), Provider and Customer will mutually agree on any additional participation in ICT security awareness training programs and digital operational resilience training determined necessary for each party to meet its obligations under DORA.

4. General.

Except as modified by this DORA Addendum, all other terms of the Agreement remain unchanged.