VANTA EU DIGITAL OPERATIONAL RESILIENCE ACT ADDENDUM

This EU Digital Operational Resilience Act Addendum ("**DORA Addendum**") supplements and is incorporated by reference into the agreement by and between Vanta and Customer governing Customer's use of the Services, which may comprise (a) Vanta's Master Subscription Agreement available at https://www.vanta.com/legal/terms or otherwise executed by the Parties ("**MSA**"), (b) Vanta's Data Processing Addendum, either incorporated into the MSA or otherwise executed by the Parties and/or (c) a separate written agreement signed by Vanta and Customer (collectively, and as applicable, "**Agreement**"). Unless otherwise stated herein, capitalized terms shall have the meaning given in the Agreement.

1. SCOPE.

This DORA Addendum applies solely to the extent Customer or any Customer Affiliate that is within scope of the Agreement is a financial entity subject to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("**DORA**"). Vanta Inc. is an "ICT third-party service provider" as defined under DORA ("**Provider**") and shall comply with the provisions of this **DORA Addendum** in respect of the provision of the Services that consist of ICT Services.

2. DEFINITIONS

(a) "**Critical or Important Function**" means a function, the disruption of which would materially impair the financial performance of Customer, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of Customer with the conditions and obligations of its authorization, or with its other obligations under applicable financial services law.

(b) "**ICT Incident**" means a single event or a series of linked events unplanned by the Customer that compromises the security of the network and information systems, and have an adverse impact on (i) the availability, authenticity, integrity or confidentiality of data of Customer, or (ii) on the services provided by the Customer.

(c) "**ICT Services**" means digital and data services provided through ICT systems to Customer on an ongoing basis as part of the Service, including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

(d) "**ICT third-party service provider**" means an undertaking providing ICT Services.

(e) "**Lead Overseer**" means the European Supervisory Authority appointed in accordance with Article 31(1), point (b) of DORA.

(f) "**Service**" has the meaning set forth in the Agreement.

3. PROVISIONS APPLICABLE TO ALL SERVICES

The following provisions of this **Section 2** apply in respect of each Service:

(a) The Order Form describes all ICT Services to be provided by Provider.

(b) The locations where the contracted or subcontracted functions and ICT Services are to be provided and where Customer's data is to be processed, including the storage location, are as follows: the European Union, United Kingdom, the United States, Australia, Canada, and the location of Provider's authorized subprocessors as identified at trust.vanta.com/subprocessors, as may be updated from time to time by Provider in accordance with the Agreement, including, as set forth in Section 4 of the DPA. For clarity, Provider's use of subprocessors will be as set forth in Section 4 of the DPA. Provider will notify Customer to the extent it uses subcontractors to perform the Services as required under DORA. Customer may subscribe to receive notifications in connection with such updates as set forth in the Agreement. Where Customer determines that a Service supports a critical or important function, and the Agreement does not satisfy the requirements for the subcontracting of such a function as applicable under DORA, Customer shall have the right to request an amendment to the Agreement to ensure compliance with applicable regulatory obligations. If such a request is not met by the

Supplier within a reasonable period, Customer shall be entitled to terminate the Agreement (or individual Services as the case may be) after providing notice to Provider and a reasonable opportunity to cure such request.

(c) Provider shall take appropriate and effective security measures at all times with regard to the availability, authenticity, integrity and confidentiality of Customer Information processed by Provider in connection with the ICT Services, as further set forth in the Agreement. Additional detail regarding Provider's current security policies and processes are available at https://trust.vanta.com. Provider shall ensure that during Customer's subscription term that Customer Information (whether personal or non-personal data) can be accessed, recovered and returned in an easily accessible format in the case of the insolvency, resolution or discontinuation of business operations of Customer, or in the event of termination of the Agreement.

(d) The service level descriptions, including updates and revisions thereof, are set forth in the Service Level Agreement of the Agreement.

(e) Upon Customer's request, Provider shall provide commercially reasonable assistance to Customer when an ICT Incident that is related to the ICT Services occurs. Provider and Customer may agree upon a reasonable reimbursement rate calculated on a time and materials basis for Provider's assistance under this Section 2(e)5.

(f) Provider shall fully cooperate with the competent authorities and the resolution authorities of Customer, including persons appointed by them, provided that any audits will be subject to the requirements set forth in the Agreement.

(g) The applicable termination rights and related minimum notice periods for the termination of the Agreement and/or agreed Service(s), as applicable, are provided in Section 3.2 of the Master Subscription Agreement.

(h) In addition to the termination rights under the Agreement, Customer may terminate the Agreement in the following cases with respect to ICT Services that are subject to this Addendum, provided that Customer must give prior written notice describing the nature of the breach, and provided that Provider is unable to cure the breach within 30 days of receipt of Customer's written notice:

(i) Circumstances identified by Customer throughout the monitoring of Provider's ICT risk that are deemed capable of altering the performance of the functions provided by Provider, including material changes that affect the Agreement or the situation of Provider.

(ii) 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.

(iii) The competent authority being no longer able to effectively supervise Customer as a result of the conditions of, or circumstances related to, the Agreement.

(iv) The Provider is in significant breach of applicable law, regulations or contractual provisions.

In the event of a termination pursuant to this Section 2(h), Customer shall remain responsible for all unpaid fees under the currently-active Order Form.

(i) Provider personnel shall complete security awareness and digital operational resilience trainings consistent with Provider's security program and as further described in the Agreement, including in Vanta's Security Statement and DPA.

4. MISCELLANEOUS

Any claims brought in connection with this DORA Addendum will be subject to the terms and conditions of the Agreement, including, but not limited to, the exclusions and limitations set forth therein. In the event of any conflict or inconsistency between (a) the MSA, DPA or Order Form and (b) this DORA Addendum, the terms of this DORA Addendum will take precedence.