## **Financial Services Addendum**

This Financial Services Addendum (“**FSA**” or “**Addendum**”) supplements the Agreement (defined below) between Digital.ai and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Customer**”). Customer and Digital.ai are collectively known as the “parties” or “Parties”.

As Customer is subject to DORA (as defined below), and to the extent that the Digital.ai Services constitute “ICT Services” as defined in DORA, the parties agree that the Agreement must contain certain provisions as set forth in this Addendum.

In consideration of the mutual obligations set out herein, the parties agree to comply with the following provisions, each acting reasonably and in good faith.

1. **DEFINITIONS**

Unless otherwise defined herein, all capitalized terms have the same meaning given to them in the Agreement. In addition, the following definitions apply:

“**Agreement**” means all current and future agreements between Digital.ai and Customer in connection with which Digital.ai provides Services (defined below) to Customer, such as a Master Subscription Agreement (“MSA”), including all Orders thereunder (directly or through an authorized partner) applicable to the Services. This DPA is incorporated into such Agreement(s) by this reference.

“**Digital.ai**” means Digital.ai Software Inc., or the applicable Digital.ai entity that is party to the Agreement.

“**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.

“**DPA**” means the data processing or data protection addendum, as applicable, between Customer and Digital.ai governing the processing of Personal Data by Digital.ai on behalf of Customer, which forms part of the Agreement.

“**Customer Data**” means, for purposes of this Addendum, any information that Customer provides to Digital.ai or otherwise authorizes access to in the course of accessing and using the Services, and includes all Customer Confidential Information and any information concerning Customer’s operations, customers, employees, contracting parties and other persons, including Personal Data, which Digital.ai receives from Customer or has access to in connection with the provision of the Services.

**“ICT-Related Incident”** means a single event or a series of linked events unplanned by the Customer, directly related to the Services, that compromises the security of the network and information systems, and have an adverse material impact on the availability, authenticity, integrity or confidentiality of Customer Data, or on the services provided by the Customer.

“**Personal Data**” means any Customer Data that relates to an identified or identifiable natural person which is protected under Data Protection Laws. “**Data Protection Laws**” means local, state, federal, or international laws, regulations, or treaties applicable to protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Personal Data under the Agreement, as may be defined in such laws, including, the European Area Law, the California Consumer Protection Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”), and any subsequent supplements, amendments, or replacements to the same.

“**Services**” means the provision of cloud services (such as software as a service (“**SaaS**”) and/or hosted or managed services), maintenance and support services in connection with the Software and/or cloud services licensed by Customer, and/or Professional Services made available by Digital.ai to Customer under the Agreement and for the purposes of which Digital.ai is an ICT provider of Customer pursuant to DORA. References to Services or ICT Services in this Addendum refers to Services that constitute ICT Services under DORA (referred to interchangeably in this Addendum as “Services” or “ICT Services”).

“**ICT Services**” has the meaning as defined under DORA.

**“Service Levels**” means to the extent applicable to the Services provided to Customer, the agreed upon service levels are set forth in the Agreement. For the avoidance of doubt, Service Levels, as applicable to Support and/or SaaS Offerings, are made available at: <https://digital.ai/support/support-and-maintenance/> .

“**Supervisory Authority**” or “**Regulator**” means any European financial service regulator or national competent authority that has the monitoring or supervisory rights over Customer and/or over Digital.ai as the provider of the ICT Services to Customer under the DORA Regulation.

“**Subcontractor**” means a third party engaged by Digital.ai in connection with the Services, which (i) perform and process operations that are involved in the delivery of the Services, and/or (ii) store or process Customer Data in connection with the ICT Services (also referred to as “Subprocessors”), in accordance with the Agreement.

1. **GENERAL OBLIGATIONS**
	1. Services Description. Services are as described in the Agreement and applicable Documentation.
	2. Service Levels. To the extent applicable to the Services provided to Customer under the Agreement, Digital.ai shall provide such Services in accordance with the Service Levels. Any updates and revisions to the agreed service levels must be documented in writing and signed by authorized representatives for both Parties in order to be valid.
	3. Cooperation. Digital.ai shall cooperate fully with Supervisory Authorities, including persons appointed by them, in all matters.
	4. Notification Obligation. Customer shall notify Digital.ai of any changes to DORA which affect the obligations of the Parties under this Addendum. If Digital.ai becomes aware of any changes in DORA regarding the ICT Services, independently of the Customer, and has reason to believe that Customer is not already aware, Digital.ai will promptly notify Customer. Further, in the event that Digital.ai is designated by a Supervisory Authority as a critical ICT third-party service provider as set out in DORA, Digital.ai shall without undue delay inform Customer of such designation in writing.
	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, then upon Customer’s request, the parties shall in good faith negotiate and agree on the incorporation of such standard contractual clauses (as applicable to the ICT Services provided to Customer under the Agreement) and replace any overlapping terms and conditions in this Addendum with the corresponding terms and conditions of the standard contractual clauses.
	6. Protection of Personal Data. The provisions on availability, authenticity, integrity, and confidentiality in relation to the protection of data, including Personal Data, as well as the terms ensuring access, recovery, and return of Personal Data, are stated in the Agreement and applicable DPA between Digital.ai and Customer. For the avoidance of doubt, Personal Data that Digital.ai processes on behalf of the Customer is processed, transferred, and stored as set forth in the Data Protection Addendum, located at <https://digital.ai/data-processing-addendum>.
2. **INFORMATION SECURITY**
	1. Digital.ai shall maintain an information security program (including relevant processes, measures, and tools) designed to protect Customer Data in Digital.ai’s possession and/or control and ensure its availability, confidentiality, authenticity and integrity. Digital.ai’s information security program shall comply with any information security requirements identified in the Agreement and are aligned with industry best practices. Digital.ai uses ISO 27001 and NIST 800-53 as a reference standard for its information security policies, implementation, and practices. A review of all Digital.ai information security policies, procedures and technical standards is conducted at least once annually. Additional information regarding Digital.ai’s security practices and certifications is made available via the [Digital.ai Security and Compliance FAQ](https://info.digital.ai/rs/981-LQX-968/images/Security%20%26%20Compliance%20FAQ%20%281%29.pdf?_ga=2.113518535.1183307676.1738172630-1837063590.1738172629).
	2. Digital.ai shall provide necessary assistance to Customer when an ICT-Related Incident that is related to the Services provided to Customer occurs. Unless other incident support or reporting procedures are agreed between Digital.ai and Customer, in the event of the occurrence of an ICT-Related Incident that could have a negative impact on the continuity or security of the Services, Digital.ai will, without undue delay: (i) notify Customer of the ICT-Related Incident; (ii) provide Customer with reasonably requested information Digital.ai has on the ICT-Related Incident that Customer needs to secure Customer's functions at risk due to such incident; and (iii) provide Customer with reasonably requested information on how Digital.ai handled the ICT-Related Incident. To the extent an ICT-Related Incident is caused by Customer, Digital.ai shall be entitled to compensation for such assistance on a time and material basis and at the hourly rates set out in the Agreement and/or agreed upon pursuant to an Order or scope of work under the Agreement.
	3. Digital.ai shall ensure Customer has access to Customer Data that Digital.ai stores, transmits, or otherwise processes in connection with the Services. Digital.ai encrypts data both at rest and while in transit using encryption methods that meet or exceed the Transport Layer Security (TLS) 1.2 or Advanced Encryption Standard (AES) 256. Customer Data can be recovered and returned in a standard readable format to Customer in the event of insolvency, resolution, discontinuation of Digital.ai’s business operations or termination of the Agreement.
3. **DIGITAL OPERATIONAL RESILIENCE & SECURITY AWARENESS TRAINING**
	1. Digital.ai shall ensure its personnel participate in ongoing IT security training courses in accordance with the regulations applicable to it. Where necessary, Digital.ai undertakes to participate in the appropriate security awareness programs and digital operational resilience training (for example: programs and/or training aligned with NIST 800-53 Rev 4 clause AT-2 or ISO 27002 Clause 7.2.2, 12.2.1,18.1.4). Digital.ai will provide Customer with sufficient information regarding the content of such training and present evidence of such participation. Customer will accept evidence from Digital.ai of its personnel’s participation in Digital.ai’s own or any other equivalent ICT security awareness programs and digital operational resilience training in lieu of requiring Digital.ai personnel to participate in Customer’s ICT security awareness training pursuant to subsection (b) below.

* 1. Where appropriate, Digital.ai’s personnel directly involved in providing Services to Customer may participate in Customer’s relevant security awareness programs and digital operational resilience training. In this case, the conditions for the participation of Digital.ai’s personnel in such programs shall be agreed in advance between the Customer and Digital.ai. Digital.ai shall reasonably assist Customer in identifying relevant participants from Digital.ai’s personnel that should participate in certain programs and/or training, based on such personnel’s authority and ability to access and process Customer Data. Digital.ai shall be entitled to compensation for its direct, unavoidable, reasonable and proven additional costs that arise in order to participate in Customer’s ICT-security awareness program and digital operational resilience training in accordance with article 13.6 in DORA.
1. **AUTHORIZED LOCATIONS & SUBCONTRACTORS**
	1. Unless otherwise specified in the Agreement or an applicable Order Form, Digital.ai may provide the ICT Services (including the subcontracted functions) to the Customer from, and/or Customer Data may be processed/stored in, the following location(s):

United States, Canada, United Kingdom, Netherlands, Germany, France, Spain, Lithuania, Israel, India, Japan, Australia, Singapore, Switzerland, Ireland, Indonesia.

* 1. Digital.ai shall notify Customer in writing in advance, and without undue delay, if Digital.ai or any of its Subcontractors change any of the aforementioned locations with respect to the provision of the ICT Services and/or the processing or storage of Customer Data in accordance with this section.
		1. The Customer Data processing locations are specified in the [Digtial.ai DPA](https://digital.ai/data-processing-addendum) and in Digital.ai’s [Data Protection FAQ](https://info.digital.ai/rs/981-LQX-968/images/Digital.ai-Data-Protection-FAQ-2021.pdf?_ga=2.256688139.1808523905.1740498803-1721126387.1740498803), in addition to Exhibit 1 of this FSA. Digital.ai shall notify Customer of any intended additions or replacements to the processing locations pursuant to the process set forth in the Digital.ai DPA.
		2. With respect to Digital.ai’s provision of the ICT Services, including data center functions related to the ICT Services, Digital.ai provides a current list of service locations, which is available at <https://digital.ai/why-digital-ai/global-footprint>. Digital.ai shall notify Customer of any intended additions or replacements to such data center locations by updating this published Global Footprint website prior to such change taking effect.
	2. Customer authorizes Digital.ai to engage Subcontractors in accordance with this Addendum, provided that Digital.ai shall enter into a written agreement with such Subcontractors which contains terms related to confidentiality, data protection and security that are at least as protective as those contained in this Addendum and the Agreement. Digital.ai shall be liable for the acts and omissions of any Subcontractor to the same extent as if performed by Digital.ai.
	3. A list of the Subcontractors and Subprocessors used by Digital.ai to provide functions in connection with the ICT Services is set forth in Exhibit 1.
1. **TERMINATION**

In addition to the termination rights set out in the Agreement, Customer may terminate the Agreement or applicable Order Form, in whole or in part, if:

1. Digital.ai is in material breach of applicable laws, regulations or this Addendum;
2. circumstances have been identified throughout the monitoring of ICT third-party risk that in Customer’s reasonable opinion are capable of materially negatively altering the performance of the functions of the Services for which Digital.ai provides an express warranty, including material changes that affect the Agreement, the arrangement or the situation of Digital.ai;
3. Digital.ai has evidenced material weaknesses pertaining to its overall ICT risk management capable of having an adverse impact on the way it ensures the availability, authenticity, integrity, and confidentiality, of Customer’s Confidential Information; or
4. a Supervisory Authority gives an instruction of termination, for example in case the Supervisory Authority can no longer effectively supervise Customer;

provided, however, (1) the aforementioned termination rights are limited to the Services that are subject to this Addendum, and (2) that Customer must give written notice describing the nature and basis of the breach to Digital.ai and Digital.ai has failed to cure the breach within 30 days after receipt of Customer´s breach notice.

Customer shall pay Digital.ai all amounts owed for the Services through the effective date of termination, which will become due immediately upon such termination, and no portion of any prepaid amounts (if applicable) shall be refunded.

1. **AUDIT**
2. Upon reasonable request, Customer may examine relevant audit reports and/or certifications (such as SOC 2 Type 2) that are available from Digital.ai and applicable to the Services to verify compliance with this Addendum and/or Digital.ai’s technical and organizational measures. Customer will have the right to submit security questionnaires to Digital.ai in the event any identified gaps or unresolved questions exist following Customer’s review of Digital.ai’s documentation.
3. In the event the ICT Services are considered by Customer as supporting critical or important functions and if Customer or one of its Supervisory Authorities requests to audit the Services to fulfill a regulatory requirement, Digital.ai shall permit Customer and/or such Supervisory Authority to conduct such audit during normal business hours at a date and time mutually agreeable to Digital.ai and Customer and/or such Supervisory Authority. Before a planned audit or on-site visit, Customer shall provide reasonable notice (at least 30 days in advance) to Digital.ai, as well as the details regarding the scope and duration of such audit. Customer shall provide Digital.ai with a copy of any final audit report (unless prohibited by applicable law) and shall use such report solely for the purpose of assessing Digital.ai’s compliance with the terms of the Agreement, this Addendum and any applicable laws. Unless otherwise required by a relevant Supervisory Authority or applicable law, the number of audits shall not exceed one (1) audit per year.
4. Customer may utilize an independent third party to perform such audits on Customer’s behalf, provided the third party is subject to confidentiality obligations at least as restrictive as those set forth in the Agreement and such third party auditor is required to execute an appropriate confidentiality agreement with Digital.ai. Customer will not utilize an independent party that is a competitor of Digital.ai to perform the audit. Customer must ensure that any personnel performing the inspection (whether internal or external to Customer) has appropriate and relevant skills and knowledge to perform the relevant audits and/or assessments effectively. Customer is responsible for the acts and omissions of its auditor when performing the audit.
5. If an audit is requested and performed by Customer’s Supervisory Authority and to the extent required under applicable law, Digital.ai shall reasonably cooperate with the Supervisory Authority, including with persons appointed by the Supervisory Authority, for requested information regarding the Services provided to Customer, so long as Customer does not otherwise have access to the relevant information. Customer will respond directly to a Supervisory Authority’s request(s) for Customer Data and shall not circumvent such requests by referring such matters to Digital.ai.
6. Any information provided by or obtained from Digital.ai pursuant to this Section 7 shall be considered Confidential Information of Digital.ai and is subject to the confidentiality obligations set forth in the Agreement. Any audits or inspections will be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and resilience of the inspected facilities, networks and systems, nor otherwise expose or compromise any data processed therein.
7. Expenses incurred by Digital.ai in connection with the performance of any inspections and audits in accordance with Section 7 shall be added to the remuneration to be paid to Digital.ai.
8. **BUSINESS CONTINUITY**

Digital.ai acknowledges that Customer may be required by its Supervisory Authorities to ensure that Customer is able to continue to carry on its business in the event of termination of the Agreement. Accordingly, Digital.ai and Customer agree as follows:

* 1. With respect to the ICT Services provided to Customer, Digital.ai shall implement and maintain adequate business continuity plans, ICT business continuity plans and response and recovery plans.
	2. Digital.ai shall review, test and update its business continuity plans, ICT business continuity plans and response and recovery plans regularly (at least once a year) as well as in the event of any substantive changes to ICT systems regarding their efficiency and adequacy and eliminate any material gaps or safety issues that have been identified without undue delay. Upon Customer’s reasonable request, Digital.ai shall inform Customer in writing about the status and results of such tests to the extent relevant to the ICT Services, including, if applicable, any material gaps or safety issues identified and a description of the corrective measures.
	3. To the extent applicable to the ICT Services provided to Customer, Digital.ai shall support and participate in Customer’s testing of the Customer’s ICT business continuity management. Digital.ai shall support Customer in the analyzing of test results and implementation of necessary remediation measures.
1. **MISCELLANEOUS**
	1. Termination. This Addendum shall terminate upon any termination or expiration of the Agreement.
	2. Miscellaneous. The section headings contained in this Addendum are for reference purposes only and shall not in any way affect the meaning or interpretation of this Addendum. Customer's sole and exclusive remedy for any breach by Digital.ai in relation to this Addendum is to terminate this Addendum and the applicable Agreement or Order for the affected ICT Services. 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. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is any conflict or inconsistency between this Addendum and the Agreement, this Addendum shall prevail to the extent that conflict or inconsistency relates to the subject matter herein. Except to the extent otherwise mandated by applicable laws, this Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement(s) between Customer and Digital.ai, as of Customer’s Signature Date below. If this document has been electronically signed by either party such signature will have the same legal effect as a hand-written signature.

|  |  |
| --- | --- |
| For [CUSTOMER] | For **Digital.ai Software, Inc.** |
| Signature: | Signature: |
| Name: | Name: |
| Title: | Title: |
| Date Signed: | Date Signed: |

**Exhibit 1**

**Subcontractor List**

Digital.ai may involve the following companies in the performance of providing Digital.ai’s products and/or services, including ICT Services, to the Customer.

|  |  |  |  |
| --- | --- | --- | --- |
| **Subprocessor**  | **Description of Service**  | **Business Address** | **Place of Data Storage & Processing** |
| Amazon Web Services (AWS) | Cloud infrastructure service provider  | 410 Terry Avenue North, Seattle, WA 98109-5210, USA | USA, Germany, UK, Canada, Ireland, Indonesia  |
| Pendo.io, Inc.   | Cloud based software support and analytics   | 301 Hillsborough St. Raleigh, NC, USA | USA |
| Zendesk   | Customer service software used for Digital.ai Support infrastructure  | 999 Market Street, San Francisco, CA 94103, USA | USA, Germany  |
| Sumo Logic, Inc.  | Cloud based software security and log analytics  | 305 Main Street, Redwood City, CA 94063, USA | USA, Ireland |
| Snowflake  | Database as a service provider  | 106 E. Babcock Street, Suite 3A, Bozeman, MT 59715 | USA |
| Maven AGI, Inc. | Customer support content services and support ticket analysis | 131 Dartmouth Street, 3rd Floor, Boston, MA 02116, USA  | USA |
| **Subcontractor** | **Description of Service** | **Business Address** | **Place of Co-Location Data Center** |
| Equinix Inc.\* | Data Center provider for Digital.ai Continuous Testing solutions  | One Lagoon Drive, Redwood City, CA 94065, United States | USA, Germany, Canada, Singapore  |
| Centrilogic\* | Data Center provider for Digital.ai Continuous Testing solutions  | 2 Robert Speck Pkwy #500, Mississauga, ON L4Z 1H8, Canada | United Kingdom, Australia |
| Coresite\*  | Data Center provider for Digital.ai Continuous Testing solutions | 1001 17th St, Suite 500, Denver, CO 80202, United States | USA |
| Digital Realty\* | Data Center provider for Digital.ai Continuous Testing solutions | 5707 Southwest Parkway, Building 1, Suite 275, Austin, TX 78735, United States | Switzerland |

\*Only applicable for customers that purchase Digital.ai’s Continuous Testing Software. These Subcontractors are Co-location data centers, whereby Digital.ai runs and maintains the software/hardware. As such, no Customer Data is processed by the Subcontractor.