Digital Operational Resilience Act Addendum

THIS DORA ADDENDUM ("**DORA Addendum**") forms part of the Agreement (as this term is defined in Aptum's Terms of Business available at https://aptum.com/legal/. Unless otherwise expressly defined herein, capitalized terms in this DORA Addendum shall have the meaning ascribed to them elsewhere in the Agreement.

1. APPLICATION / FINANCIAL ENTITY

1.1 This DORA Addendum only applies if the Customer uses the Service and is subject to the 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**"). For clarity, the use of the term "applicable law or regulations" in this DORA Addendum includes DORA.

1.2

(a) To the extent that there is a direct conflict between any express term elsewhere in the Agreement and any express term in this DORA Addendum, the express term in this DORA Addendum shall take precedence, govern and control the subject matter.

(b) To the extent that there is a direct conflict between any express term in this DORA Addendum and any express term in DORA (as this term is defined herein) applicable to the Parties, the express term in DORA applicable to the Parties shall take precedence, govern and control the subject matter.

1.3 This DORA Addendum is effective as of January 17, 2025 (the "**Effective Date**") and applies to active Services after the Effective Date and (a) only as long as the Customer is a Financial Entity; or (b) if the Customer is not a Financial Entity but uses the entirety of the Services for its client who is a Financial Entity ("**Client**") or its Beneficiary Affiliate(s).

2. INTERPRETATION

2.1 Unless defined otherwise in this DORA Addendum, terms shall have the meaning set out in the other parts of this Agreement. In this DORA Addendum:

"**Affiliate(s)**" means a company or corporation that is controlled by, controls, or is under common control with a Party.

"**Beneficiary Affiliate(s)**" means an Affiliate of the Customer for whom the Services were wholly or partly purchased for by the Customer.

"**ICT Third-Party Service Provider**" is as defined in DORA and means an ICT Third-Party Service Provider designated as critical in accordance with Article 31 of DORA.

"**Competent Authority**" means a designated regulator in each European Union (EU) member state that enforces DORA's requirements.

"**Critical or Important Function**" is as defined in DORA and means a function, the disruption of which would materially impair the financial performance of a financial entity, 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 a financial entity with the conditions and obligations of its authorization, or with its other obligations under applicable financial services law.

"Financial Entity" means a person who meets the definition of financial entity in DORA and is thereby subject to DORA.

"**ICT**" is defined in DORA and means information and communication technologies and tools that process and transmit information.

"**ICT-Related Incident**" is as defined in DORA and means a single event or a series of linked events unplanned by the Financial Entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the Financial Entity.

"**ICT Services**" is as defined in DORA and means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

"**ICT Third-Party Service Provider**" is as defined in DORA and means an undertaking providing ICT Services.

"**ICT Third-Party Service Provider Established in a Third Country**" is as defined in DORA and means an ICT third-party service provider that is a legal person established in a third country and that has entered into a contractual arrangement with a financial entity for the provision of ICT Services.

"**Regulator**" means any European Union financial service regulator or a Competent Authority (including any authority defined in DORA) that has the monitoring or supervisory rights over the Customer, its Client and/or its Beneficiary Affiliates.

"**TLPT**" or "**Threat-led Penetration Testing**" is as defined DORA.

3. APTUM AS AN ICT PROVIDER

3.1 When the Customer is a Financial Entity and Aptum provisions Services to the Customer under the Agreement, Aptum is an ICT Third-Party Service Provider; and as Aptum is established in the UK, Aptum is an ICT Third-Party Service Provider Established in a Third Country.

3.2 The Services do not support a Critical or Important Function and Aptum has not been designated as a Critical ICT Third-Party Service Provider. If Aptum is designated as a Critical ICT Third-Party Service Provider, it shall either establish a subsidiary in the European Union within a12-month period of such designation or terminate the Agreement without liability of any kind to the Customer within such period.

4. DORA TERMINATION RIGHTS

4.1 Without prejudice to the Customer's rights to terminate the Services as set forth elsewhere in Agreement, the Customer may terminate the Agreement, including the Services on thirty (30) days prior written notice to Aptum ("**DORA Notice**") if:

(a) the Customer identifies circumstances through the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the Agreement, including material changes that affect the arrangement or the situation of Aptum as an ICT third-party service provider;

(b) evidenced weaknesses pertaining to Aptum's 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; or

(c) where a Competent Authority can no longer effectively supervise the Customer as a Financial Entity as a result of the conditions of, or circumstances related to the Agreement.

4.2 To the extent that the Customer serves a DORA Notice to Aptum, such notice shall reasonably provide a fulsome level of detail with a high degree of specificity as to how the Customer determined its right to terminate the Agreement in accordance with the foregoing section of this DORA Addendum (collectively, the "**DORA Concern**").

4.3 If Aptum resolves the DORA Concern to the Customer's reasonable satisfaction within the thirty (30) days of Aptum receiving the DORA Notice, the DORA Notice will be deemed to have been automatically withdrawn.

4.4 In the event that the Services are terminated in accordance with DORA Notice, the Customer shall pay Aptum all Fees accrued up to the effective date of such termination. Given the subjectivity of the termination rights in this Article 4, there shall be no refund of any pre-paid Fees or accrued Service Credits if the Agreement is terminated under this Article 4.

5. ASSISTANCE & COOPERATION

5.1 Upon request of a Regulator or the Customer, the following assistance and cooperation shall be made available to them in regards to the Services at the Customer's cost at Aptum's then-current support rate, but not more than £250 per hour charged in half-hour increments ("**Support Rate**"):

(a) Aptum shall provide reasonable assistance to the Customer when there is an occurrence of an ICT-Related Incident in connection with the Services.

(b) Aptum shall fully cooperate with a Regulator, including persons appointed by them in respect of the Services provisioned for the Customer.

(c) Aptum's personnel directly involved in provisioning the Services shall participate in the Customer's ICT security awareness programs and digital operational resilience training. In this case, such participation shall be agreed to in advance by the Parties.

(d) Unless otherwise included with the Services as expressly evidenced in the applicable Order, when requested by the Customer or a Regulator, Aptum shall produce requested report(s) relating circumstances that materially impacts the confidentiality, integrity, or availability of the Services.

(e) Customer may run a TLPT against the Services provided that it is agreed to in advance and with the assistance of Aptum so as to ensure such TLPT does not impact Aptum's services for other customers. Aptum shall reasonably participate and cooperate with Customer in accordance with the process required to be followed for a TLPT.

6. SUBCONTRACTORS

6.1 To the extent that Aptum uses any subcontractors to perform all or part of the Services, such subcontractors shall be identified on the Order for such Services. To the extent that such subcontractors need to be replaced during the Term of the Order, Aptum will work with the Customer to ensure that the replacement subcontractor is acceptable to the Customer.

7. Audits

7.1 If a Regulator requests information about the Services or the Customer's use of the Services, Customer shall in the first instance, use the standard features of the Services (if any) to respond to such request, as well as any third-party audit reports applicable Service that are made available by Aptum.

7.2 Subject to and in accordance with the other provisions of this Article, if the Services are designated by a Regulator as supporting Critical or Important Functions and if a Regulator requests to audit the Services, Aptum shall allow the Regulator to perform such audit. In this regard, reasonable access will be given to all relevant business premises (e.g., head offices, operation centers), relevant devices, systems, networks, information, Aptum's personnel, Aptum's external auditors and data used for providing the Customer with the Services, including related financial dealings between the Parties.

7.3 Before a planned audit or on-site visit, Customer shall provide reasonable notice to Aptum, but not less than fourteen (14) days, as well as the details on the scope and duration of such audit or visit and shall adhere to relevant commonly accepted national and international audit standards.

7.4 If required by DORA, the Customer (or Regulator's auditor as the case may be) shall have the right to take copies of relevant documentation used by Aptum in provisioning the Services. In any case, any audit may not be performed in a manner that would compromise the privacy, confidentiality or security of other Aptum other customers or their data, or that which would threaten or adversely impact the stability or performance of Aptum's services for its other customers.

7.5 Customer ensures to verify that whoever is performing audit, whether it is internal auditor, the pool of auditors, or external auditors acting on its behalf, has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. Customer may use a third-party auditor with Aptum's agreement, which shall not be unreasonably withheld. Prior to any audit, the auditor shall be required to execute an appropriate confidentiality agreement with Aptum. Customer shall be responsible for the acts and omissions of the auditors who perform audits hereunder.

7.6 All references to the term "audit(s)" in this DORA Addendum shall only be for audits required in order to comply with DORA. The Customer shall bear all of its costs relating to the audits, including paying Aptum the Support Rate and reimbursing Aptum for any out-of-pocket costs associated with any audit. All Aptum information, including documentation made available to the Customer, Regulators and/or Transferee (as this term is defined below) hereunder for any reason, including for or during any audit shall constitute Aptum's Confidential Information, and the Customer shall be responsible for the handing of such information in accordance with the terms of the Agreement and shall reasonably ensure that Regulators and/or Transferee do the same.

7.7 Customer shall provide Aptum with a copy of any final report of any audit unless prohibited DORA or other applicable law or regulation; shall treat the findings thereof as Aptum's Confidential Information in accordance with the terms of the Agreement; and use it solely for the purpose of assessing Aptum's compliance with this DORA Addendum and to meet its obligations under DORA.

8. Business Continuity

8.1 Aptum acknowledges that the Customer may be required by Regulator to ensure that Customer is able to continue to carry on its business in the event of termination of the Agreement. Accordingly, the Parties agree as follows:

(a) Upon intervention of Customer by the Regulator pursuant to applicable laws or regulations, Aptum shall comply with the requirements of the Regulator, and to the extent Aptum is reasonably able to, assist the Regulator at Customer's expense to preserve business continuity of Customer by assisting the Regulator to gain full administrator controls over the Services.

(b) In the event of insolvency, reorganization (pursuant to applicable insolvency or bankruptcy law), liquidation, or some other action impacting Customer or its Beneficiary Affiliates, as provided by applicable law or regulation ("**Distress Event**"), and to the extent required to maintain continuity of Services for the Customer under the Agreement, Aptum shall consent to Customer assigning or transferring Customer's rights under the Agreement or specific Services to (a) one or more of the Customer's Affiliates, including any other Beneficiary Affiliate, or (b) a third-party that purchases or otherwise succeeds to any or all of the business or assets or equity of Customer ((a) and (b) shall be jointly referred to as "**Transferee**"). In each case, the Transferee shall have access to the Customer's transferred Services through Aptum's standard processes and tools and such Services shall be subject to terms of the Agreement.

(c) To the extent of an occurrence of a Distress Event, Aptum shall neither terminate the Agreement nor suspend or delay the performance of its obligations under the Agreement, provided that the Transferee (and/or Customer) paying all Fees accrued prior to the Distress Event and all Fees that accrue after the Distress Event in accordance with the terms of the Agreement.

8.2 Within thirty (30) days after Aptum's written notification to the Customer of its intention to terminate the Agreement for any reason other than for non-payment of Fees or Aptum's inability to reasonably procure key components necessary for the Services, the Customer (or Transferee as the case may be) may elect to extend the Services on a month-to-month basis for up to twelve (12) months, or longer if expressly required and notified by a Regulator in writing to Aptum that Aptum continue provisioning the Services ("**Extension Notice**"), provided however, Aptum may reasonably increase the Fees during the period covered by the Extension Notice. Parties acknowledge that Aptum does not control, have access to or possess any knowledge regarding the Customer's data stored on and/or transmitted through any part of the Services. It shall be the Customer's or the Transferee's responsibility to migrate or retrieve such data from the Services prior to the termination or expiration of the Agreement using Aptum's standard processes and tools; and Aptum may but does not have any obligation to preserve any part of the Services on which the Customer's data is stored after the termination or expiration of the Agreement. To the extent that the Customer (or Transferee) requires Aptum's assistance with such migration, retrieval and/or storage, such assistance shall be at the Customer's cost at Aptum's Support Rate.

8.3 Aptum has and shall maintain for the duration of the Agreement adequate business continuity and disaster recovery plans intended to restore the Services to normal operations in the event of an emergency and in accordance with applicable laws and regulations. The controls supporting such plans are validated through international-recognized standards and audit reports, such as ISO 27001 and SOC 2 Type II audits, which are initiated at least annually and are performed by qualified, independent, third-party auditors. Upon request, Aptum shall make available to Customer information regarding Aptum's business continuity and disaster recovery plan.