



DORA ADDENDUM

This **DORA Addendum** (the “**Addendum**”) forms part of the Agreement identified below between the party identified in the Agreement or the applicable RSA quotation (“**Customer**”) and the relevant RSA sales entity, and applies to the provision of certain ICT services, comprising the Services, by RSA to Customer, where Customer is a financial sector entity subject to certain regulatory requirements which obligate Customer to have certain contractual provisions on digital operational resilience in its agreements with its suppliers.

IT IS HEREBY AGREED as follows:

1. DEFINITIONS

1.1 Capitalized words will have the meanings set out in the Agreement, unless they are defined in this Addendum, or the context requires otherwise. In this Addendum the following words and expressions shall have the following meanings, unless the context otherwise requires:

- a) “**Affiliate**” means, any entity that directly or indirectly controls, is controlled by, or is under common control with another entity. For the purpose of this definition, “control” means direct or indirect ownership or control of more than 50% of the voting interests of the entity;
- b) “**Agreement**” means the written or electronic agreement identified and located at <https://www.rsa.com/standard-form-agreements/>, or any agreement executed between the parties that governs the provision of Services by RSA and the use of the Services by the Customer;
- c) “**Applicable Laws**” means any laws and regulations issued by a Regulatory Body, which applies to the performance of the Agreement or the Services.
- d) “**Customer Data**” means any data or information relating to Customer or their customers, service providers or any personnel of Customer that are supplied to RSA by Customer, or which RSA processes, stores or transmits in connection with the Services performed under the Agreement;
- e) “**DORA**” means EU Regulation 2022/2554 on digital operational resilience for the financial sector.
- f) “**Regulatory Bodies**” means those resolution authorities, government departments and regulatory, statutory and other bodies, entities and committees which, whether under statute, rule, regulation, code of practice or otherwise, are responsible to regulate Customer and its Affiliates (and “**Regulatory Body**” shall be interpreted accordingly);
- g) “**Resolution Event**” means
 - the exercise by a Regulatory Body, in relation to Customer, of any supervisory action pursuant to a Resolution Power;
 - any other action taken by a Regulatory Body based on, or taken in connection with, Resolution Powers in relation to Customer, including, without limitation, any request by the Regulatory Body to Customer to take any action, where such requested action directly adversely affect Customer's ability to meet its contractual obligations;
 - the exercise of stabilization powers by a Regulatory Body pursuant to a Resolution Power, each pursuant to legislation, regulation, or pursuant to powers of a Regulatory Body to establish a framework for the recovery and/or resolution of Customer including (where any of the following directly adversely affect Customer's ability to meet its contractual obligations):
 - (i) a transfer of the shares of a financial institution to a third party;
 - (ii) a transfer of all or part of the business, assets or liabilities of a financial institution by way of asset transfer;
 - (iii) the making of a bank insolvency order or bank administration order; or
 - (iv) a bail-in or other compromise of the claims of the creditors of a financial institution.
- g) “**Resolution Power**” means the legislative powers of the applicable Regulatory Body in connection with such Regulatory Body’s authority pursuant to Articles 68 and 71 of Directive 2014/59/EU (or howsoever these Articles are implemented into national law), where such

powers relate to RSA's performance under the Agreement or Customer's ability to meet its contractual obligations;

- h) **"Resolution Unit"** means Customer or Customer Affiliate which is subject to a Resolution Event, which Resolution Event directly affects the Agreement.
- i) **"Services"** 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, including but not limited to the provision of RSA products, RSA cloud-based license or service or customer support service provided by RSA.

1.2 Words referring to the singular only, also include the plural and vice versa, where the context requires.

2. SERVICES AND SERVICE LEVELS

2.1 RSA will provide Customer with the Services as described in the Agreement. The service levels applicable to the Services, related service credits (if any), and any updates and revisions thereof, are provided in the Agreement.

3. PERMITTED LOCATIONS

3.1 The location where the Services will be provided and where Customer Data will be kept and processed, is available at <https://community.rsa.com/s/article/RSA-Subprocessor-Information>.

3.2 RSA will provide the Services from and will store and process Customer Data from (the locations set out in <https://community.rsa.com/s/article/RSA-Subprocessor-Information> (the "**Permitted Locations**"). If RSA wishes to provide all or any part of the Services from outside of the Permitted Locations and/or store and/or process Customer Data from outside of the Permitted Locations or RSA wishes to change the Permitted Locations, then upon Customer's subscription at <https://community.rsa.com/s/article/RSA-Subprocessor-Information>, RSA will provide 30 days' prior notice of such change. If Customer has a reasonable basis to object to RSA's change of Permitted Location, Customer shall notify RSA of such objection. Customer's consent shall be deemed given if Customer does not object in writing within thirty (30) days after receipt of the prior notice. If Customer objects to the change in Permitted Location on reasonable grounds, then either RSA will not change the Permitted Location or Customer may elect to immediately suspend or terminate the Service under the Agreement affected by such change of Permitted Location. Such termination shall not entitle Customer to any refund on a committed license term and Customer shall remain liable for all fees otherwise due. For the avoidance of doubt, Customer shall be liable to pay any outstanding fees on a committed order.

4. SUB-CONTRACTING

4.1 RSA may subcontract any part of the Agreement or permit any subcontractor to process or store Customer Data, provided that RSA remains responsible for the performance of the Services and is liable for the acts and omissions of the subcontractors. RSA shall maintain an up-to-date list of its current subcontractors at the following hyperlink: <https://community.rsa.com/s/article/RSA-Subprocessor-Information>. Provided that Customer has subscribed to receive notification at the aforesaid hyperlink, RSA will provide at least thirty (30) days' prior notice to Customer in the event of any change of the subcontractors. If such change in subcontractors in Customer's reasonable opinion poses a material risk to Customer, Customer shall notify RSA of its objection. Customer's consent shall be deemed given if Customer does not object in writing within thirty (30) days after receipt of the prior notice. If Customer objects to the change of subcontractors due to material risk posed to Customer, then either RSA will not change the subcontractor or Customer may elect to immediately suspend or terminate the Service under the Agreement affected by such change. Such termination shall not entitle Customer to any refund on a committed license term and Customer shall remain liable for all fees otherwise due. For the avoidance of doubt, Customer shall be liable to pay any outstanding fees on a committed order.

4.2 RSA shall maintain oversight and control of its subcontractors in accordance with the requirements of the Agreement and to ensure that the obligations of the Agreement are met.

5. TERMINATION

5.1 Customer may terminate the Agreement with written notice:

- a) where RSA is in significant breach of Applicable Law;
- b) where RSA commits a material breach of the Agreement which is incapable of remedy or, if capable of remedy, is not remedied within thirty (30) calendar days after written notice to Customer of the occurrence of such event;
- c) where Customer identifies circumstances or events which Customer reasonably considers have resulted in, or will result in, the Services not being provided substantially in accordance with the Agreement (including material changes adversely affecting the provision of the Services under this Agreement or the situation of RSA);
- d) where there is evidence of weaknesses in RSA's ICT risk management, and in particular in the way RSA ensures the availability, authenticity, integrity and confidentiality of Customer Data, which is not remedied within thirty (30) calendar days after Customer provides written notice informing of such evidence of weakness; and
- e) where the Regulatory Body can no longer effectively supervise Customer as a result of the conditions of, or circumstances related to, the Agreement.

6. CONSEQUENCES OF TERMINATION

6.1 If the Agreement is terminated or expires, or in the case of the insolvency, resolution or discontinuation of business operations of RSA and/or its agents and/or its sub-contractors, Customer is responsible for ensuring that Customer has necessary copies of all Customer Data which has been uploaded into RSA's cloud service for processing, storage or hosting (if applicable).

6.2 RSA shall comply with any data deletion requests received from Customer. Following termination of the Agreement, RSA shall delete all Customer Data from RSA's systems, and any other place where Customer Data is held or accessible from.

7. INFORMATION SECURITY

7.1 RSA shall comply with up to date industry standard IT security practices that are appropriate for providing the Services and comparable with the ISO/IEC 27000 series or any equivalent and ensure that its information security measures that it uses to provide the Services, are appropriate in order to ensure the security, availability, confidentiality, and accuracy of Customer Data.

8. DATA PROTECTION

8.1 RSA shall comply with the data protection provisions set out in the Agreement.

9. SECURITY INCIDENT MANAGEMENT

9.1 If RSA confirm the existence of, a single event or series of linked events that compromises the security of RSA's network and information systems, and has an adverse impact on the availability, authenticity, integrity or confidentiality of Customer Data held or controlled by RSA, or the provision of the Services to Customer (an "**ICT Incident**"), RSA shall:

- a) notify Customer of that fact without undue delay, together with reasonable details of the ICT Incident and any steps required to be taken or that it is taking to mitigate the effects of the ICT Incident, including if relevant any steps necessary to reduce the risk of any future breach of security of that same nature;
- b) provide reasonable assistance required by Customer to support Customer to recover from the ICT Incident and to comply with its obligations under applicable law including with regard

to notifications to the Regulatory Body, at no additional cost to Customer if such ICT Incident is proven to be caused by RSA's negligence or default; and at Customer's cost based on RSA's then current rates, if such ICT Incident is not due to RSA's negligence or default; and

- c) promptly address and remediate the ICT Incident and mitigate its effects.

10. AWARENESS TRAINING

10.1 RSA is committed to conducting an annual security awareness program for its personnel, which shall include at least:

- a) Information and training on security policies, procedures, and protocols;
- b) Awareness of the reporting channels put in place by RSA for the detection of anomalous behavior; and
- c) Returning all ICT assets and tangible information in RSA personnel's possession, that belong to RSA or a Customer, upon termination of employment.

10.2 If RSA's security program is found to be lacking in any requirements under applicable laws or regulations, Customer may request that RSA's relevant personnel, at Customer's expense, be included in Customer's training programs.

11. COOPERATION WITH REGULATORY BODY

11.1 RSA shall fully cooperate with the Regulatory Body (including persons appointed by them) in connection with this Agreement and the Services provided under this Agreement and shall reasonably cooperate with Customer to provide such information as may be reasonably required by Customer to meet a request from a Regulatory Body.

12. RESOLUTION

12.1 Pursuant to the Resolution Powers, where a Resolution Event occurs to a Resolution Unit by, or instigated by, a Regulatory Body then the benefit of the Agreement will, at Customer's discretion, continue to apply to the Resolution Unit to the extent required by a Regulatory Body. Any provisions in the Agreement giving rise to termination or suspension rights at law in favor of RSA will not apply to the extent that the rights arise solely out of, or solely in connection with, a Resolution Event, provided that once the Resolution Event ceases to be in effect, all rights in this respect shall be available. Nothing in the foregoing will affect or remove RSA's right to claim for fees, charges or costs that are payable by Customer under the Agreement, and Customer remains obligated to pay for all fees, charges or costs payable under the Agreement.

13. GENERAL

13.1 In the event of any conflict between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum shall prevail. Except as set out above, the Agreement shall continue in full force and effect.