DATA PROCESSING ADDENDUM
FOR SECURID CLOUD SERVICE OFFERINGS

This Data Processing Addendum ("DPA") forms part of the Agreement (defined below) between the party identified in the Agreement or the applicable RSA quotation ("Customer") and RSA Security LLC, its direct and indirect subsidiaries and Affiliates ("RSA") and applies to the extent that (i) RSA Processes Personal Data on behalf of Customer in providing Services, and (ii) the Agreement expressly incorporates this DPA by reference. This DPA does not apply where RSA is the Controller. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

1. **Definitions**.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity. For purposes of this definition, "control" means direct or indirect ownership or control of more than 50% of the voting interests of the entity.

"Agreement" means the written or electronic agreement identified and located at https://www.rsa.com/en-us/company/standard-form-agreements between Customer and RSA pursuant to which RSA provides Services to Customer.

"Data Breach" means a breach by RSA of the security obligations under this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data Processed.

" Controller" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of the Personal Data.

" Processor" means an entity that Processes Personal Data on behalf of a Controller.

"Data Protection Laws" means any data protection and/or privacy related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party to this DPA is subject and which are applicable to the Services provided under the Agreement.

"GDPR" means General Data Protection Regulation 2016/679 on the protection of natural persons in the Processing of Personal Data and on the free movement of such data, as may be amended or superseded from time to time.

"Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject") which is Processed by RSA, acting as a Processor on behalf of the Customer, in connection with the provision of and subject to the limitations of the Services (as set forth in the Agreement), and which is subject to Data Protection Laws. For the avoidance of doubt, in cases where data is anonymized or pseudonymized such that the Data Subject cannot be identified by RSA, such data shall not be deemed nor construed as 'Personal Data'.

"Processing", "Processed", or "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,

restriction, erasure or destruction, subject to the parameters and limitations as set forth in the Agreement between RSA and Customer.

"Services" means any RSA cloud-based license or service, or customer support service provided by RSA to Customer pursuant to the Agreement.

“Standard Contractual Clauses” are the clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and located at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

"Subprocessor" means a third party engaged by RSA that Processes Personal Data pursuant to the Agreement.

2. **Processing**.

2.1 As between RSA and Customer, RSA will Process Personal Data under the Agreement as a Processor acting on behalf of the Customer. Customer agrees that it will not require RSA to undertake or engage in any activity that would require, or result in, RSA acting in the capacity of a Controller.

2.2 Customer authorizes RSA to Process the Personal Data to provide the Services in accordance with RSA’s rights and obligations under the Agreement and in any subsequent statements of work or service orders, and RSA may use performance data derived from the provision of the Services and the Processing of the Personal Data to enhance and/or improve RSA’s products and services.

2.3 This DPA, the Agreement, and any subsequent statements of work or service orders, and any configurations by Customer or its authorized users, comprise Customer’s complete instructions to RSA regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed upon by the parties in writing, including the costs (if any) associated with complying with such instructions.

2.4 RSA is not responsible for determining if Customer’s instructions are compliant with applicable law. However, if RSA is of the opinion that a Customer instruction infringes applicable Data Protection Laws, RSA shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

2.5 Customer will, in its use of the Services, comply with its obligations under Data Protection Laws when Processing Personal Data and when issuing Processing instructions to RSA. Customer represents that it has all rights and authorizations necessary for RSA to lawfully process Personal Data pursuant to the Agreement, as described in applicable Data Protection Laws.

2.6 RSA may only disclose Personal Data to its Subprocessors, Affiliates, and subsidiaries for the purpose of: (a) complying with Customer’s reasonable and lawful instructions; (b) as required in connection with the Services and as permitted by this DPA; and/or (c) as required to comply with Data Protection Laws, or an order of any court, tribunal, regulator, or government agency with competent jurisdiction to which RSA is subject. With regard to (c) above, RSA will (to the extent permitted by law) inform the Customer in advance of making any disclosure of Personal Data and will reasonably cooperate with Customer to limit the scope, proportionality, and duration of such requested disclosure to what is strictly necessary or legally required.

2.7 RSA shall maintain the confidentiality of Personal Data in accordance with Data Protection Laws applicable to Processors and shall ensure those authorized to Process the Personal Data (including its Subprocessors) are committed to obligations of confidentiality.

3. **Subprocessing**.

3.1 Customer agrees that RSA may appoint and use Subprocessors to Process Personal Data in connection with the Services PROVIDED that: (a) RSA puts in place a written contract with each Subprocessor that imposes obligations that are (i) relevant to the Services to be provided by the Subprocessors, and (ii) materially similar to the rights and/or obligations granted or imposed on RSA under this DPA; and (b) where a Subprocessor fails to fulfill its data protection obligations as specified above, RSA shall be liable to the Customer for the performance of the Subprocessor's obligations.

4. **Security Measures**.

4.1 Taking into account industry standards, the costs of implementation, the nature, scope, context, and purposes of the Processing, and any other relevant circumstances relating to the Processing of the Personal Data on RSA systems, RSA shall implement appropriate technical and organisational measures to ensure security, confidentiality, integrity, availability, and resilience of processing systems and services involved in the Processing of the Personal Data are commensurate with the risk in respect of such Personal Data. RSA will periodically (i) test and monitor the effectiveness of its safeguards, controls, systems, and procedures, and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the Personal Data, and ensure these risks are addressed. RSA shall implement and document appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services (including restoring access to the Personal Data where applicable) in a timely manner after a disruptive event.

4.2 Customer is responsible for using and configuring the Services in a manner that enables Customer to comply with Data Protection Laws, including implementing appropriate security, technical, and organizational measures. Such measures shall provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause.

4.3 RSA restricts its personnel from Processing Personal Data without authorization (unless required by applicable law) and will ensure that any personnel authorized by RSA to process Personal Data is subject to an obligation of confidentiality.

5. **Data Breach.**

5.1 Where a Data Breach is caused by RSA's failure to comply with its obligations under this DPA, RSA shall, where required by applicable Data Protection Laws, notify Customer without undue delay after establishing the occurrence of the Data Breach and shall:

(a) to the extent such information is known or available to RSA at the time, provide Customer with details of the Data Breach, a point of contact, and the measures taken or to be taken to address the Data Breach; and

(b) reasonably cooperate and assist Customer with any investigation into, and/or remediation of, the Data Breach (including, without limitation and where required by Data Protection Laws, the provision of notices to regulators and affected individuals); and

(c) not inform any unaffiliated third party (other than another customer affected by the same Data Breach, a Subprocessor potentially possessing relevant information, or experts or consultants utilized by RSA) of any Data Breach relating to the Personal Data without first obtaining Customer's prior written consent, except as otherwise required by applicable law.

5.2 in the event Customer intends to issue a notification regarding the Data Breach to a data protection supervisory authority, other regulator, or law enforcement agency, Customer shall (unless prohibited by law) allow RSA to review the notification and Customer shall consider any reasonable comments or amendments proposed by RSA.

6. **Demonstrate Compliance.**

RSA shall, upon reasonable prior written request from Customer (not to be made more than once in any twelve-month period), provide Customer such information as may be reasonably necessary under applicable law and in accordance with RSA's security practices, to demonstrate RSA's compliance with its obligations under this DPA.

7. **International Data Transfers.**

5.1 RSA may, in connection with the provision of the Services, or in the normal course of business, make international transfers of Personal Data to its Affiliates, subsidiaries, and/or Subprocessors. When making such transfers, RSA shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this DPA.

5.2 Where the provision of Services involves the transfer of Personal Data from the EEA to countries outside the EEA (which are not subject to an adequacy decision under Data Protection Laws) such transfer shall be subject to the following requirements: (a) RSA has in place intra-group agreements that incorporate Standard Contractual Clauses with any Affiliates or subsidiaries which may have access to the Personal Data; and (b) RSA has in place agreements with its Subprocessors that incorporate the Standard Contractual Clauses, as appropriate.

5.3 RSA and Customer agree that:

a) When Customer acts as the Controller and RSA as a Processor, then Module Two applies.
    i. The appropriate designation is set forth in Annex I attached hereto.

ii. Option 2 for Clause 9(a) applies. RSA shall inform the Customer of any intended changes to sub-processors at least 30 days in advance.

iii. Option 2 for Clause 17 applies. As described in Clause 17, Parties agree that the law of the relevant Member State shall be the governing law.

iv. For Clause 18, disputes shall be resolved in the courts of Data Exporter Member State.

v. Annex II and III are set below.

8. **Deletion of Data.**

Upon termination of the Services (for any reason) and if requested by Customer in writing, RSA shall, as soon as reasonably practicable and in accordance with applicable law, delete the Personal Data on RSA systems, PROVIDED that RSA may: (a) retain one copy of the Personal Data as necessary to comply with any legal, regulatory, judicial, audit, or internal compliance requirements; and (b) defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof cannot reasonably and practically be expunged from RSA's systems. The parties hereby expressly acknowledge that Customer instructs RSA to maintain back-up files of all Customer data (which may include Personal Data), for the duration established in the Agreement. For such retention or deferral periods as set forth above, the provisions of this DPA shall continue to apply to such Personal Data. RSA reserves the right to charge Customer for any reasonable costs and expenses incurred by RSA in deleting the Personal Data pursuant to this clause. A certificate of destruction will be provided upon request.

9. **Cooperation.**

9.1 If RSA receives any request from Data Subjects, or applicable data protection authorities relating to the Processing of Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Data Protection Laws, RSA will promptly redirect the request to the Customer. RSA will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If RSA is required to respond to such a request, RSA will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.

9.2 RSA shall provide reasonable cooperation and assistance to Customer, to the extent applicable in relation to RSA's processing of the Personal Data and within the scope of the agreed Services, in connection with any data protection impact assessment(s) which the Customer may carry out in relation to the processing of Personal Data to be undertaken by RSA, including any required prior consultation(s) with supervisory authorities. RSA reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

9.3 To the extent required by Data Protection Laws, RSA will, upon reasonable notice and at Customer's expense, provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments ("DPIAs") and/or prior consultations with data protection authorities.

9.4 Neither RSA nor any Subprocessor shall be liable for any claim brought by Customer or any third party arising from any action or omission by RSA and/or Subprocessors to the extent such action or omission resulted from compliance with Customer's instructions, security practices, policies, and/or procedures.

10. **General.**

10.1 Any claims brought under this DPA will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

10.2 In the event of any conflict between this DPA and the Agreement, the terms of this DPA will prevail.

10.3 RSA may modify the terms of this DPA as provided in the Agreement (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary, to comply with Data Protection Laws, or (iii) to implement or adhere to Standard Contractual Clauses, approved codes of conduct or certifications, binding corporate rules, or other compliance mechanisms, which may be permitted under Data Protection Laws. Supplemental terms may be added as an Annex or Appendix to this DPA where such terms only apply to the Processing of Personal Data under the Data Protection Laws of specific countries or jurisdictions. RSA will provide notice of such changes to Customer, and the modified DPA will become effective, in accordance with the terms of the Agreement or as otherwise provided on RSA's website if not specified in the Agreement.

Annex I

Annex I to the Standard Contractual Clauses

A. LIST OF PARTIES

Module Selection

Select applicable Module(s)	
	Module One: Controller to Controller
X	Module Two: Controller to Processor
	Module Three: Processor to Processor
	Module Four: Processor to Controller

Data exporter(s):

Name: The entity identified as "Customer" in the Addendum.

Address: The address for Customer associated with its account or as otherwise specified in the Addendum or the Agreement.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the Addendum or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities are specified in Section 2 of the Addendum.

Signature and date: By using RSA services or products the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller.

Data importer(s):

Name: "RSA" as identified in the Addendum.

Address: The address for RSA is specified in the Agreement.

Contact person's name, position and contact details: The contact details for RSA are specified in the Addendum or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities are specified in Section 2 of the Addendum.

Signature and date: By transferring Customer Personal Data to Third Countries on Customer's instructions, the data importer will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred**:*

The data subjects are Customer's end users, employees, contractors, suppliers and other third parties relevant to the Services.

***Categories of personal data transferred**:*

- *Contact details: which may include name, address, email address, telephone, fax, other contact details, emergency contact details, associated local time zone information.*

- *Customer details: which may include Contact details, invoicing, and credit related data.*

- *IT systems and operational information: which may user ID and password details, computer name, email address, domain name, user names, passwords, IP address, permission data (according to job roles), account and delegate information for communication services, individual mailboxes and directories, chat communication data, software and hardware inventory, tracking information regarding patterns of software and internet usage (e.g. cookies), and information recorded for operational and/or training purposes.*

- *Customer support: which may include personal identifiers, voice, video and data recordings.*

- *Other: Any other Personal Data submitted by Customer, including the Personal Data identified at the following link: https://community.rsa.com/docs/DOC-75846#View*

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**:*

RSA does not intend to process any special categories of Personal Data on behalf of the Customer. Customer agrees not to provide, transfer, or disclose any special categories of Personal Data at any time to any of RSA's service offerings.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Personal data is transferred in accordance with Customer's instructions as described in Section 2.

Nature of the processing:

The nature of the processing is described in Section 2 of the Addendum.

***Purpose(s) of the data transfer and further processing**:*

To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*:*

The data exporter determines the duration of processing in accordance with the terms of the Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*:*

The subject matter, nature, and duration of the processing are described in Section 1.3 of the Addendum.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

Annex II

Annex II to the Standard Contractual Clauses. Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data.

Technical and organizational security measures in RSA's compliance programs include the following:

A. Measures to ensure security of processing

1. Entrance Control

Appropriate measures preventing unauthorized persons from gaining access to data processing systems on which personal data are processed or used:

- Visitors need to register; date and time of arrival, time of leaving the building as well as the name of the person being visited shall be recorded; visitors shall be accompanied by an authorized person at all times;
- All office units are secured by an "access control system". Access to the office units is granted with an activated entry card only;
- CCTV covers appropriate areas (e.g. entrances to data centers);
- Data centers are located in separated areas with special access requirements; Additionally, authorized persons are instructed to grant access to persons known to them only;
- Security guard service for the main, operational buildings is provided;
- Outside areas may be under video surveillance or under monitoring by a security service.

2. Admission Control

Appropriate measures preventing unauthorized persons from using data processing systems.

- Access to IT systems is granted only to a user when registered under a valid username and password;
- Internal password policy requires periodical mandatory password changes and minimum length and the use of special characters;
- Policy includes automatic computer lock after a short period, with renewed access to the PC only after new registration with a valid username and password;
- Outside network access requires a two-factor-authentication.

3. Access Control

Appropriate measures ensuring that persons entitled to use a data processing system have access only to the data to which they should have the right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage:

- Access authorization is issued in respect of the specific area of work to which the employee is assigned (work roles);
- Policy requires regular verification of access authorizations;

4. Separation Control

Appropriate measures ensuring that data collected for different purposes can be processed separately:

- Personal data of different controllers shall be processed separately;
- Functional separation between test and production systems is employed.

B. Measures to ensure integrity of processing

1. Transmission Control

Appropriate measures ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is made:

- Encrypted data transfer when handling confidential data and when accessing the company network;
- Sensitive Personal Data is saved encrypted on employees' laptops;
- Monitor for suspicious data traffic;
- Restrictive usage of Wireless LAN;
- Restrictive remote-access to the RSA network (using two-factor-authentication);
- External access to the internet from internal networks by employees or the use of Wireless LAN within the office building is provided only via internal IT systems, a User-ID, an individual password and encrypted connections;
- Data media shall be disposed of in accordance with data protection policies by use of safety container and document shredders; magnetic data storage media shall be destroyed physically, or erased using industry recognized processes; compliance with guidelines concerning erasure and/or destruction of data storage media and documents;
- In case of remote support (screen sharing), the connection will be encrypted and requires an affirmative action from the customer.

2. Input Control

Appropriate measures ensuring the possibility to check and establish whether and by whom personal data have been input into data processing systems, accessed, modified or removed:

- When using relevant applications, access is automatically recorded;
- In case of remote-support, the customer can terminate the data processing or support activity at any time.

C. Measures to ensure availability and resilience of processing

1. Job Control

No Processing according to Art. 28 GDPR shall take place without Controller's instructions, clear contract drafting, formalized assignment management, strict vetting processes and checks.

- Subcontractors are on-boarded in globally consistent processes. During the onboarding process, subcontractors are carefully vetted and must contractually commit to consistent compliance standards;
- Subcontractors are regularly reviewed for compliance with their contractual and legal obligations;
- The processor and his subcontractors shall agree on provisions substantially equivalent to the provisions agreed between the controller and the processor;

2. Availability Control

Appropriate measures ensuring that personal data are protected from accidental destruction or loss:

- Anti-virus software is installed on all applicable systems;
- Protection of the network via Firewall;
- Network segmentation;
- Use of content filter/Proxys;
- Interruption-free power supply for all critical systems;

- Regular generation of backups of relevant data;
- Fire safety system;
-
- Emergency/ Disaster recovery plans;
- Air-conditioned server rooms.

3. Resiliency

Punctual peak demands or long term high demands are reflected in the design of systems and services (memory, access and throughput capacities, etc) in order to ensure resilience and consistency of processing.

- The infrastructure is designed to function under high demand and can handle peak demands.

4. Incident Response

Appropriate processes to address cybersecurity events.

- A corporate response plan for Cybersecurity incidents is in place that outlines Purpose, Scope, Identification, Assessment, Response and Remediation of security incidents, including notifications to Regulators, controllers and/or data subjects as may be required.

D. 1. Encryption

- Identifiable sensitive personal data is encrypted in transit and at rest;
- Encryption standards are specific and clearly defined.

E. Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

e.g. back-up concepts, redundant storage locations, mirrored IT infrastructure

- Disaster Recovery plans exist for relevant data;
- Critical data is backed up or mirrored.

F. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of personal data processing

- All IT security policies are regularly checked to ensure they are effective and up-to-date;

Annual review of all corporate level security Policies, Standards and corresponding Procedures occurs with the final review/approval of the Chief Security Officer.

Annex III

Annex III to the Standard Contractual Clauses. List of Sub-Processors.

As applicable, the controller authorizes the use of the sub-processors located at https://www.rsa.com/content/dam/en/terms/rsa-subprocessors.pdf