VERINT

GLOBAL DATA PROCESSING ADDENDUM ("DPA") - VERINT AS CUSTOMER'S DATA PROCESSOR/SERVICE PROVIDER

This DPA forms part of the applicable agreement for the procurement of Verint offerings ("**Agreement**") by and between the applicable Verint entity and your company ("**Customer**").

1 Definitions

The terms used in this DPA shall have the meanings set forth in this DPA provided that capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. References in this DPA to: **(i)** Verint include to Verint Affiliates where such Verint Affiliates are Subprocessors, and **(ii)** Customer shall mean Customer Affiliates where such Affiliates are Data Controllers. Except as modified below, the terms of the Agreement shall remain unchanged and in full force and effect. In this DPA, the following terms shall have the meanings set out below, the word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly:

1.1 Adequacy Decision.

For a jurisdiction with Privacy Laws that impose restrictions on certain cross border transfers of Personal Data for subsequent processing, a decision of a Supervisory Authority, legislative or executive body in such jurisdiction which recognises that the destination jurisdiction in respect of a cross border transfer either by application of its own Privacy Laws or by other legal measures, provides an adequate level of protection in respect of the Processing of Personal Data in that destination jurisdiction.

1.2 Affiliate.

Any entity which now or in the future controls, is controlled by, or is under common control with the signatory to this DPA, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise.

1.3 Data Controller.

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, and in the context of this DPA shall mean the Customer.

1.4 Data Privacy Framework.

The EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

1.5 Data Privacy Framework Principles.

The Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded or replaced.

1.6 Data Processing Instructions.

The Processing instructions set out at https://www.verint.com/our-company/legal-documents/dpa/data-processing-schedule/, as may be updated by Verint from time to time, with Customer having the option to register with Verint's notification service provided to enable Customer to receive notifications from Verint concerning such updates.

1.7 Data Processor or Service Provider.

A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller, and in the context of this DPA shall mean Verint.

1.8 Data Subject.

An identified or identifiable natural or legal person.

1.9 Information Security Schedule.

The information security, technical and organisational measures specified in the Information Security Schedule, as may be updated from time to time, set out at https://www.verint.com/wp-content/uploads/Verint-Information-Security-Schedule.pdf.

1.10 Permitted Transfer.

As defined in Section 11.

1.11 Personal Data.

The meaning set out in, and will be interpreted in accordance with Privacy Laws, and in the context of this DPA, shall mean the personal data related to a Data Subject used for Processing which is provided by Customer to Verint or directly or indirectly received or obtained by Verint in connection with the provision of the Services at the request of Customer.

1.12 Personal Data Breach.

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.13 Privacy Laws.

National, federal, union, state and other laws, as applicable to the Processing of Personal Data.

1.14 Process, or Processing or Processed.

Any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, as described in the Agreement and Data Processing Instructions.

1.15 Restricted Transfer.

Means:

- a transfer of Personal Data from Customer to Verint for Processing; or
- an onward transfer of Personal Data from Verint to a Subprocessor for Processing,

in each case, where such transfer outside of the jurisdiction where the Personal Data originates would be prohibited by relevant and applicable Privacy Laws in the absence of an approved method of lawful transfer, including through (a) an Adequacy Decision, (b) Standard Contractual Clauses, or (c) by the terms of other recognised forms of data transfer agreements or other lawful processes approved by a Supervisory Authority.

1.16 Standard Contractual Clauses.

The contractual clauses approved by a decision of Supervisory Authority, legislative or executive body pursuant to Privacy Laws which provides for transfer of Personal Data from the jurisdiction from which the Personal Data originates to another jurisdiction where such transfer would otherwise be a Restricted Transfer, including those set out in the Appendices to this DPA.

1.17 Subprocessor.

Any third party (including any third party and any Verint Affiliate) appointed by or on behalf of Verint to undertake Processing in connection with the services.

1.18 Supervisory Authority.

An independent competent public authority or other legal body which is established in a jurisdiction under Privacy Laws and responsible for monitoring or enforcement applicable Privacy Laws.

1.19 Supplementary Measures.

Those measures that are considered necessary under certain Privacy Laws to apply additional protections to Personal Data transferred under a Permitted Transfer (defined in Section 11) as such measures are set out at https://www.verint.com/our-company/legal-documents/dpa/supplementary-measures/.

2 Appointment of Verint

2.1 Customer appoints Verint as its Data Processor (Service Provider) and agrees that all Personal Data provided to Verint pursuant to the Agreement and this DPA complies with the collection, transmission and lawful processing requirements under relevant Privacy Laws to enable the Processing.

2.2 Verint agrees to treat Personal Data as Customer Confidential Information.

2.3 Verint will not:

- process Personal Data other than as set out in this DPA and in the Agreement unless upon Customer's further written instructions or as required by a Supervisory Authority;
- sell Personal Data; or
- share, use or disclose the Personal Data unless it is authorized in accordance with the Agreement, this DPA, any Order, upon Customer's further written instructions or as required by a Supervisory Authority.

2.4 Customer on behalf of itself and each Customer Affiliate which is the Data Controller of the Personal Data instructs Verint to undertake Processing in accordance with this DPA and the Agreement.

2.5 With respect to SaaS Services, such SaaS Service shall only store and/or Process Personal Data in the Verint region specified in the Data Processing Instructions, as may be further specified in an applicable Order, and as may otherwise be requested by Customer in Customer's further instructions.

3 Verint Personnel

Verint shall ensure that persons authorised to undertake Processing of the Personal Data have:

- committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of the Personal Data; and
- undertaken appropriate training in relation to protection and security of Personal Data.

4 Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, including the risk of a Personal Data Breach. Verint shall implement appropriate technical and organisational measures designed to provide a level of security appropriate to the risk in Processing. For the purposes of this DPA Verint's technical and organisational measures are set out in the Information Security Schedule.

5 Subprocessing

5.1 Verint shall only appoint Subprocessors which enable Verint to comply with this DPA. Customer authorises Verint to appoint Subprocessors in accordance with this Section 5 subject to any restrictions or conditions expressly set out in the Agreement or applicable Order. Subprocessors appointed as at the effective date of this DPA are listed in the Data Processing Instructions and/or as specified in an Order. Verint shall remain liable to Customer for the performance of that Subprocessor's obligations.

5.2 Notwithstanding any notice requirements in the Agreement, before Verint engages any new Subprocessor not authorized in accordance with Section 5.1, Verint shall give Customer notice of such appointment, including details of the Processing to be undertaken by the proposed Subprocessor and for this purpose, Verint may provide such notice by updating the list of Subprocessors in the Data Processing Instructions. Customer may notify Verint of any objections (on reasonable grounds related to Privacy Laws) at globalprivacy@verint.com to the proposed Subprocessor or Data Processing Instructions ("**Objection**"). Upon receipt of the Objection, Verint and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Subprocessor or operation of the services to address the Objection. Where such further measures cannot be agreed between the parties within forty-five (45) days from Verint's receipt of the Objection (or such greater period agreed by Customer in writing), Customer may by written notice to Verint with immediate effect terminate that part of the services which require the use of the proposed Subprocessor.

5.3 With respect to each Subprocessor which is the subject of Section 5.2 above, Verint or the relevant Verint Affiliate shall:

- carry out adequate due diligence before the Subprocessor first Processes Personal Data to ensure that the Subprocessor is capable of providing the level of protection for Personal Data required by the Agreement;
- ensure that the Subprocessor is subject to a written agreement with Verint that includes appropriate data protection provisions; and
- if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses or other appropriate method of transfer are at all relevant times incorporated into the agreement executed between Verint and the Subprocessor.

6 Complying With Individual Rights of Data Subjects

6.1 Verint shall:

- upon becoming aware, promptly notify Customer if Verint receives a request from a Data Subject (or persons appointed to act on their behalf) relating to an actionable right of the Data Subject under any Privacy Law in respect of Personal Data in Verint's possession for Processing (each being an **"Individual Rights Request"**); and
- not respond to any Individual Rights Request except on the written instructions of Customer, (which Customer shall promptly provide to Verint if it requires Verint to respond), or otherwise as required by a Supervisory Authority.

6.2 Customer may where required by Privacy Laws and where directly relevant to the services, request in writing that Verint reasonably assist Customer in dealing with a Data Subject rights request validly made under Privacy Law directly to the Customer or connected with an Individual Rights Request to the extent Customer cannot fulfil this request without Verint's assistance. Verint may fulfil this request by making available functionality that enables Customer to address such Data Subject rights request without additional Processing by Verint. If Customer declines to use such functionality or to the extent such functionality is not available, Verint may provide such assistance in accordance with a mutually agreed Order.

7 Personal Data Breach

7.1 Verint shall notify Customer within forty-eight (48) hours upon Verint or any Subprocessor becoming aware of a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet its obligations under Privacy Law to report to or inform Data Subjects and/or a Supervisory Authority of the Personal Data Breach. Subject to Section 7.3 below, such notification shall at a minimum:

- describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
- communicate the name and contact details of Verint's data protection officer or other relevant contact from whom more information about the Personal Data Breach may be obtained; and
- describe the measures taken or proposed to be taken to address the Personal Data Breach.

7.2 Verint shall co-operate with Customer and take such reasonable commercial steps as are necessary to assist in the investigation, mitigation and remediation of any Personal Data Breach.

7.3 Where and in so far as it is not possible to provide the information referred to in Section 7.1 at the same time as notification of the Personal Data Breach, the information may be provided in phases without undue further delay. Verint's obligation to report or respond to a Personal Data Breach under this Section 7 is not and will not be construed as an acknowledgement by Verint of any fault or liability of Verint (or its Affiliates) with respect to a Personal Data Breach.

8 Data Protection Impact Assessment and Prior Consultation

Where directly connected to Processing, Verint shall provide reasonable assistance to Customer with any data protection impact assessments (or similar assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities), which Customer reasonably considers to be required by Privacy Laws. To the extent that such impact assessment and/or prior consultation requires assistance beyond Verint providing the applicable Verint maintained records of Processing, security of Personal Data and/or associated Documentation, Verint may provide such assistance in accordance with a mutually agreed Order.

9 Deletion or return of Personal Data

9.1 Unless otherwise provided for in the Agreement, Verint will within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), and subject to Section 9.2 below, at Customer's request, delete or return available Personal Data. At the expiry of the Return Period, if Customer has not elected either of the foregoing Verint may delete and destroy all Personal Data without liability to Customer. Where Customer requests Verint to return available Personal Data, Verint may fulfil this request by making available functionality that enables Customer to retrieve the Personal Data without additional Processing by Verint. If Customer declines to use this functionality, Customer may, within the Return Period, request that Verint return the available Personal Data under an Order for the applicable professional services. In the event the Agreement is terminated for Customer's breach, Verint shall have the right to require that Customer prepay for such professional services. Verint shall provide written confirmation to Customer that it has fully complied with this Section 9 within thirty (30) days of Customer's request for such confirmation.

9.2 Verint may retain Personal Data to the extent required by Privacy Laws or any other statutory requirement to which Verint is subject, but in such instance only to the extent and for such period as required of Verint by Privacy Laws or any other statutory requirement provided always that (a) during such retention period the provisions of this DPA will continue to apply, and (b) Verint shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws or any other statutory requirement applicable to Verint requiring its storage or any other statutory requirement to which Verint is subject and for no other purpose.

10 Review, Audit and Inspection rights

10.1 Upon Customer's reasonable request, Verint shall provide all relevant and necessary material, documentation and evidence that it complies with Section 4 of this DPA.

10.2 If, following the completion of the steps set out in Section 10.1 Customer reasonably believes that Verint is non-compliant with Privacy Laws, Customer shall provide sufficient written details thereof and allow Verint a reasonable opportunity to respond after which Customer may request that Verint make available, either by webinar or in a face-to-face review with appropriate Verint Personnel, extracts of all relevant information necessary to further demonstrate Verint's compliance with Privacy Laws and this DPA. Customer shall provide reasonable notice of a review to be conducted under this Section 10.2, by contacting Verint's Global Privacy Officer using Verint's Privacy Portal.

10.3 In the event that Customer reasonably believes that its findings following the steps set out in Section 10.2 do not enable Customer to comply materially with Customer's obligations mandated under the Privacy Laws in relation to its appointment of Verint as Data Processor, then Customer may give Verint not less than thirty (30) days prior written notice by contacting Verint's Global Privacy Officer using Verint's Privacy Portal of its intention to undertake an audit which may include inspections of Verint to be conducted by Customer or a third party auditor mandated by Customer (such third party not being a competitor of Verint). Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between Customer (or its mandated third party auditor) and Verint, (ii) be undertaken solely to the extent mandated by, and may not be further restricted under applicable Privacy Laws, (iii) not require Verint to compromise the confidentiality of security aspects of its systems and/or data processing facilities (including that of its Subprocessors), and (iv) not be undertaken in such manner so as to place Verint in breach of Verint's

confidentiality obligations to other Verint customers vendors and/or partners or otherwise cause Verint to breach laws applicable to Verint. Customer (or third party auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to Verint's premises, equipment, systems and/or personnel and shall minimize the impact of such audit or inspection to the extent reasonably possible. To the extent that such audit performed in accordance with this Section 10.3 exceeds one (1) business day, Verint shall reserve the right to charge Customer for each additional day at its then current daily rates.

10.4 If Customer has reasonable grounds following an audit or inspection undertaken pursuant to Section 10.3 to determine that Verint is non-compliant with Privacy Laws or this DPA, then Customer will provide details thereof to Verint upon receipt of which Verint shall provide its written response and to the extent required, a draft remediation plan for the mutual agreement of the parties (such agreement not to be unreasonably withheld or delayed) where the mutually agreed plan shall be termed the "Remediation Plan". Where the parties are unable to reach agreement on the Remediation Plan, or in the event of agreement, Verint materially fails to implement the Remediation Plan by the agreed dates which in either case is not cured within forty-five (45) days following Customer's notice or another period as mutually agreed between the Parties, Customer may terminate the Order for Services in part or in whole falling under the Remediation Plan provided that any other Services not subject to the Remediation Plan shall continue unaffected by such termination.

10.5 The rights of Customer under this Section 10 shall only be exercised once per calendar year unless Customer reasonably believes Verint to be in material breach of its obligations under either this DPA or Privacy Laws.

11 Restricted Transfers

11.1 Whenever a Restricted Transfer occurs, each party will ensure that such transfer is made in compliance with the relevant provisions of Privacy Law.

11.2 Certain of Verint's Affiliates have certified compliance with the Data Privacy Framework as set out in Verint's privacy notice. To the extent that a Restricted Transfer involves transferring Personal Data to the United States, and provided always that the transfer falls under the scope of Verint's self-certification to the Data Privacy Framework, then:

- Verint will rely on the Data Privacy Framework to establish that the Restricted Transfer is compliant with the relevant provisions of Privacy Law, unless the Data Privacy Framework shall become invalid, be amended or withdrawn or otherwise Verint no longer maintains certification under the Data Privacy Framework, in which case the provisions of Section 11.3 shall apply; and
- Verint will ensure that it provides at least the same level of protection to such Personal Data as is required by the Data Privacy Framework Principles and will inform Customer if it is unable to comply with this requirement.

11.3 Subject to the provisions of Section 11.2, the Standard Contractual Clauses are hereby incorporated into this DPA and shall apply to any Restricted Transfer.

11.4 Where there is any conflict between the terms of this DPA and either the Data Privacy Framework or the Standard Contractual Clauses (as the case may be) then either the Data Privacy Framework or the Standard Contractual Clauses shall prevail.

11.5 Upon request, Verint shall where required by Privacy Law, provide Customer with evidence that it has undertaken an appropriate transfer risk assessment in relation to the relevant Restricted Transfer or otherwise shall undertake such transfer risk assessment.

11.6 A Restricted Transfer which subsequently satisfies the relevant Privacy Law following an Adequacy Decision, adoption of Standard Contractual Clauses or another transfer tool permitted under applicable Privacy Law shall be termed a "**Permitted Transfer**" under this DPA.

12 Other Privacy Laws

12.1 To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements in addition to those in this DPA, including Standard Contractual Clauses, the parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws as an Appendix to this DPA or in a duly executed written addendum or amendment to this DPA or in an Order.

12.2 If any variation is required to this DPA as a result of a change in Privacy Laws then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this DPA, including incorporation of the Standard Contractual Clauses, to address such changes.

13 Supplementary Measures/Additional Safeguards

13.1 Verint shall comply with the Supplementary Measures.

13.2 As of the Effective Date of the Agreement, Verint has no reason to believe that the laws and practices in a destination country which is the transfer destination of Personal Data for further Processing following a Permitted Transfer ("**the Destination Country**"), including any requirements to disclose Personal Data or measures authorising access by public authorities, prevents Verint from fulfilling its obligations under this DPA.

13.3 Verint agrees to promptly notify Customer if at any time it makes a determination that it can no longer comply with its performance obligations under this DPA or Privacy Laws as they apply to Verint or if it has reason to believe that it is or has become subject to laws or practices which would prevent Verint from being able to comply with Section 13.2, including following a change in the laws of the Destination Country or a measure (such as a disclosure request) indicating an application of such laws in practice would prevent Verint from being able to comply with Section 13.2.

13.4 Following a notification pursuant to Section 13.3, Verint shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to address the situation. Any Permitted Transfer shall be suspended if Verint or Customer (on notice to Verint) reasonably considers that no appropriate safeguards for such transfer can be ensured, or if instructed by a Supervisory Authority to do so. If the suspension cannot be lifted within a reasonable period, Customer shall be entitled to terminate the affected Order (or affected component of an Order) in accordance with Section 13 of Schedule B provided that any remaining services shall otherwise continue unaffected by such termination.

13.5 Verint shall, unless legally prohibited from doing so:

- promptly notify the Customer in the event if it receives a legally binding request from a public authority, including judicial authorities, under the laws of a Destination Country for the disclosure of Personal Data including information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
- promptly notify the Customer in the event it becomes aware of any direct access by public authorities exercising a right under the laws of the Destination Country in relation to the Personal Data transferred to the Destination Country for Processing; and
- in respect of such a request or direct access as aforesaid take such steps as are necessary to keep disclosure and access to the minimum and provide Customer with as much information as legally permissible.

14 General Terms

14.1 Except for the governing law and jurisdiction provisions of the Standard Contractual Clauses, the parties to this DPA hereby submit to the applicable choice of governing law and jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

14.2 The UN Convention on Contracts for the International Sale of Goods shall not apply in any respect to this DPA or the Agreement (and any associated Orders) or the parties, regardless of the applicable governing law and jurisdiction.

14.3 The parties agree that any electronic link included in this DPA and the content thereof form integral part of this DPA.

14.4 In the event of inconsistencies between the provisions of this DPA and any part of any other agreements between the parties, including the Agreement, the provisions of this DPA shall prevail.

14.5 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary in writing by the parties to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

14.6 This DPA constitutes the entire agreement and understanding of the parties relating to Processing, superseding all prior or contemporaneous agreements, representations, promises and understandings, whether written, electronic, oral or otherwise.

VERINT

APPENDIX 1

EUROPEAN, SWISS AND UNITED KINGDOM TERRITORY SPECIFIC TERMS

1. As used herein, "EU GDPR" shall mean General Data Protection Regulation ((EU) 2016/679) and "UK GDPR" shall mean the UK General Data Protection Regulation (as defined by section 3(10) (as supplemented by section 205(4)) of the UK Data Protection Act 2018), each as may be amended. In respect of EU GDPR and UK GDPR, the Standard Contractual Clauses for the purposes of this Appendix shall mean the EU Standard Contractual Clauses where the "**EU Standard Contractual Clauses**" shall mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as set out in the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, replaced or superseded by the European Commission from time to time as the modules Annexes and adapted by this Appendix 1. To the extent of any conflict between the body of this DPA and this Appendix 1, this Appendix 1 shall prevail over any conflicting term in the body of this DPA and as required by clause 5 of the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail over any other term of this DPA and the Agreement.
2. In respect of any Restricted Transfers from the European Economic Area, the parties agree to the following:
   - 2.1. The EU Standard Contractual Clauses will be incorporated into this DPA;
   - 2.2. The modules and Annexes of the EU Standard Contractual Clauses are set out at https://www.verint.com/wp-content/uploads/Modules-to-SCC-pursuant-to-Regulation-EU-2016-679.pdf; and
   - 2.3. The parties agree that execution of this DPA or the agreement into which it is incorporated constitutes signature and acceptance of Annex 1.A to Appendix 1 of this DPA and acceptance and incorporation of the EU Standard Contractual Clauses.
3. In respect of any Restricted Transfers from the United Kingdom, the parties agree to the following:
   - 3.1. The Standard Contractual Clauses shall mean the UK Addendum where "UK Addendum" means the International Data Transfer Addendum to EU Transfer Contract Clauses in force 21st March 2022, as may be amended, replaced or superseded by the ICO from time to time (including when formally issued by the ICO under section 119A(1) of the UK Data Protection Act 2018);
   - 3.2. The UK Addendum will be incorporated into this DPA;
   - 3.3. The parties agree that execution of this DPA or the agreement into which it is incorporated constitutes signature and acceptance of Annex 1.A to Appendix 1 of this DPA and acceptance and incorporation of the UK Addendum; and
   - 3.4. Tables 1 to 4 (inclusive) to the UK Addendum shall be deemed completed with the information set out in at https://www.verint.com/wp-content/uploads/Modules-to-SCC-pursuant-to-Regulation-EU-2016-679.pdf;
4. In respect of any Restricted Transfers from Switzerland, the parties agree to the following:
   - 4.1. The EU Standard Contractual Clauses shall have the same meaning as described in paragraph 1 and as approved by the Swiss Data Protection and Information Commissioner, including the necessary adaptations to ensure compliance with Swiss data protection law as set out at https://www.verint.com/wp-content/uploads/Modules-to-SCC-pursuant-to-Regulation-EU-2016-679.pdf;
   - 4.2. The EU Standard Contractual Clauses will be incorporated into this DPA;
   - 4.3. The parties agree that execution of this DPA or the agreement into which it is incorporated constitutes incorporated constitutes signature and acceptance of Annex 1.A to Appendix 1 of this DPA and acceptance and incorporation of the EU Standard Contractual Clauses.

ANNEX 1.A

COMMISSION IMPLEMENTING DECISION (EU) 2021/914 OF 4 JUNE 2021 ON STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES PURSUANT TO REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

(…)

APPENDIX

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s):

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: The contracting party specified as Customer in this DPA or the relevant Customer Affiliate acting as Data exporter

Address: The principal address which appears in the Agreement or otherwise the address of the Customer which Verint has on file

Contact person's name, position and contact details: The primary contact details which Verint holds on file for the Customer

Data Protection officer's (if any) name, position, and contact details: The primary contact details which Verint holds on file for the Customer

EU representative's (if any) name, position, and contact details:

Activities relevant to the data transferred under these Clauses: As specified in the Data Processing Instructions

Signature and date: as evidenced by signature of the DPA or the Agreement into which the DPA is incorporated

Role (controller/processor): … Controller

2. Data importer(s):

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: The contracting party specified as Verint in this DPA

Address: The Verint address specified in the Agreement

Contact person's name, position and contact details: Verint's Global Privacy Officer contacted by submitting a request via Verint's Privacy Portal

Activities relevant to the data transferred under these Clauses: As specified in the Data Processing Instructions

Signature and date: as evidenced by signature of the DPA or the Agreement into which the DPA is incorporated

Role (controller/processor): … processor

…

B. DESCRIPTION OF TRANSFER

CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED
As specified in the Data Processing Instructions

CATEGORIES OF PERSONAL DATA TRANSFERRED
As specified in the Data Processing Instructions

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.
As specified in the Data Processing Instructions

THE FREQUENCY OF THE TRANSFER (E.G. WHETHER THE DATA IS TRANSFERRED ON A ONE-OFF OR CONTINUOUS BASIS).
Subject to Customer's, its Affiliates, and Customer's customers use of the service, Personal Data will be transferred on a continuous basis during the term of the Agreement

NATURE OF THE PROCESSING
As specified in the Data Processing Instructions

PURPOSE(S) OF THE DATA TRANSFER AND FURTHER PROCESSING
As specified in the Data Processing Instructions

THE PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED, OR, IF THAT IS NOT POSSIBLE, THE CRITERIA USED TO DETERMINE THAT PERIOD
During the provision of the services and following termination of the services, in accordance with the data erasure provisions of the Agreement.

FOR TRANSFERS TO (SUB-) PROCESSORS, ALSO SPECIFY SUBJECT MATTER, NATURE AND DURATION OF THE PROCESSING
As specified in the Data Processing Instructions during the provision of the services

C. COMPETENT SUPERVISORY AUTHORITY
See section Annex 1.c https://www.verint.com/wp-content/uploads/Modules-to-SCC-pursuant-to-Regulation-EU-2016-679.pdf

VERINT

APPENDIX 2
U.S. PRIVACY LAWS SPECIFIC PROVISIONS

"U.S. Privacy Laws" means all applicable United States federal, state, and local laws, rules, and regulations currently in effect, or as they become effective, relating in any way to the Processing, privacy, confidentiality, or security of Personal Data.

For purposes of the U.S Privacy Law, the Personal Data will be deemed as collected within a state if the Data Subject was within the state at the time the data was collected and/or the Data Subject is a known resident of that state.

For purposes of U.S. Privacy Laws, the definition of "Controller" is the same as the term "Business" or "Controller" under U.S. Privacy Laws and in the context of this DPA shall mean Customer. The definition of "Processor" is the same as the term "Processor" or "Service Provider" under U.S. Privacy Laws and in the context of this DPA shall mean Verint. Where the Personal Data is subject to requirements regarding Processing under the U.S. Privacy Law in effect as at the Effective Date of this DPA, the following provisions shall apply:

Requirement in U.S. Privacy Laws	Provisions in Schedule E applicable to U.S. Privacy Laws
Prohibition on Selling or Sharing Personal Data	See Sections 2.3.2 and 2.3.3. For this Appendix 2, "sell" and "share," as used in the DPA, shall take the meanings assigned to those terms in applicable U.S. Privacy Laws. .
Business Purpose of Processing and Use Limitation	Provision of SaaS Services, Professional Services and/or Support in accordance with the Agreement and DPA. More specific information available at Section1.1.4. Processor shall Process the Personal Data only to achieve the Business Purpose of Processing as set forth in the Agreement and the DPA (and may otherwise use personal information solely as permitted under the applicable U.S. Privacy Laws).
Use Limitation	Processor shall Process the Personal Data only to achieve the Business Purpose of Processing as set forth in the Agreement and the DPA (and may otherwise use personal information solely as permitted under the applicable U.S. Privacy Law).
Compliance with U.S. Privacy Law	See Schedule E in its entirety. Moreover, each party shall comply with applicable obligations under applicable U.S. Privacy Laws and is responsible for notifying the other party if they can no longer comply with U.S. Privacy Laws (See Section 13.3).
Non-combining of Personal Data as Service Provider	Processor agrees that it shall not combine Personal Data with other data it receives from other sources about the same Data Subject except where Processor is entitled to do so under Privacy Law, or pursuant to the Agreement or this DPA or the business purpose
Written agreement with each Subprocessor	See Section 5.3.2
Maintain technical and organizational measures to protect Personal Data	See Section 4.1
Certification Verint understands the restrictions	Each party certifies that it understands the restrictions set forth herein and under the applicable U.S. Privacy Laws and will comply with them.
Reasonable Support to Respond and Notice of any Requests	See Sections 6.1.1 and 6.2
Reasonable and Appropriate Steps to Ensure Compliance	See Section 10
Retention, Use or Disclosure of Personal Data	Processor will not retain, use, or disclose the Personal Data outside of the direct business relationship and for any purpose other than providing the Services as specified in the Agreement and associated Orders, for a Business Purpose, or as expressly permitted by the applicable U.S. Privacy Laws.
Right to Opt-out	Processor shall assist Controller in providing the right to opt out of the processing of Personal Data for purposes of (i) target advertising, (ii) the sale of Personal Data, or (iii) profiling for decisions that significantly affect the Controller, as required by applicable U.S. Privacy Laws.
Right to Limit Use of Sensitive Personal Data	Where required by applicable U.S. Privacy Laws, Processor shall assist Controller in providing the right to limit the use and disclosure of sensitive personal information.
Right to Stop Unauthorized Use	See Section 13.4
Duty of Confidentiality	See Section 3.1. Each person involved in processing Personal Data must be subject to a duty of confidentiality with respect to the Personal Data.
Data Deletion or Return	See Section 9.2
Audit and Review Obligations	See Section 10
Right to Access	See Section 13.5.3
Right to Correct	Processor shall assist Controller in providing the right to correct inaccuracies in Personal Data, as required by applicable U.S. Privacy Laws.
Right to Data Portability	Processor shall assist Controller in providing the right to obtain the Personal Data in a portable and, to the extent technically feasible, readily usable format that allows the Controller to transmit the data to another entity without hindrance, as required by applicable U.S. Privacy Laws.

VERINT

APPENDIX 3
BRAZILIAN GENERAL DATA PROTECTION LAW ("LGPD") TERRITORY SPECIFIC PROVISIONS

LGPD applies regardless of where the data Processing agent is located, to the extent that: (i) the data Processing activities take place in Brazil, (ii) the data Processing occurs for the offering of goods and services in Brazil, or for the Processing of Personal Data from Data Subjects located in Brazil; or (iii) the processed Personal Data is collected in Brazil. For purposes of the LGPD, the Personal Data will be deemed as collected in Brazil if the Data Subject was in Brazil at the time the data was collected.

For purposes of the LGPD, the definition of "Data Controller" is the same of the Portuguese term "Controlador" and in the context of this DPA shall mean Customer. The definition of "Data Processor" (or "Service Provider) is the same of the Portuguese term "Operador" and in the context of this DPA shall mean Verint. The definition of "Data Protection Officer (DPO)" is the same of the Portuguese term "Encarregado de Dados".
Where the Personal Data is subject to requirements regarding Processing under the Brazilian General Data Protection Law (Law No. 13,709 of 2018; hereby named as "**LGPD**") in effect as at the Effective Date of this DPA, the following provisions shall apply:

1. The Standard Contractual Clauses for the purposes of this Appendix shall mean the EU Standard Contractual Clauses where the "EU Standard Contractual Clauses" shall mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as set out in the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, replaced or superseded by the European Commission from time to time as the modules Annexes and adapted by this Appendix 3. To the extent of any conflict between the body of this DPA and this Appendix 3 as it relates to Processing falling under this Appendix 3, this Appendix 3 shall prevail of any conflicting term in the body of this DPA. Notwithstanding the foregoing, as required by clause 5 of the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail over any other term of this DPA and the Agreement.
2. In respect of any Restricted Transfers from Brazil, the parties agree to the following:
   2.1. The EU Standard Contractual Clauses will be incorporated into this DPA. The EU Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Brazil to other jurisdictions, subject to amendments for adequacy with certain obligations specifically set forth in the Brazilian General Data Protection Law, and to the extent that Brazilian Supervisory Authority ("ANPD") does not set forth its specific Standard Contractual Clauses for Restricted Transfers.
   2.2. The modules and Annexes of the EU Standard Contractual Clauses are set out at https://www.verint.com/wp-content/uploads/Modules-to-SCC-pursuant-to-Regulation-EU-2016-679.pdf; and
   2.3. The parties agree that execution of this DPA or the agreement into which it is incorporated constitutes signature and acceptance of Annex 1.A to this Appendix 3 of this DPA and acceptance and incorporation of the EU Standard Contractual Clauses.