Data Processing Terms and Conditions

This DPA is between the Parties listed on the Cover Page and each Party is acting on its own behalf and as agent for, with respect to Vendor, Vendor Affiliates, and with respect to Verint, Verint Affiliates. The terms used in this DPA shall have the meanings set forth in this DPA and the Principal Agreement. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement as amended by, and including, this DPA.

1. DEFINITIONS.

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Adequacy Decision**" means, 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;

1.1.2 "**Authorised Subprocessor**" means any company, organisation, entity or person (including any Vendor Affiliate) which is authorised by Verint in accordance with Section 6 to Process Protected Data in connection with the Principal Agreement and the terms of this DPA;

1.1.3 "**Authorised Transfer**" means a Restricted Transfer which is authorised by Verint in Section 12 of this DPA as permissible or otherwise as authorised in writing by Verint as permissible;

1.1.4 "**Cover Page**" means the document executed by Verint and Vendor which incorporates the terms of this DPA. The DPA will be considered executed once the Cover Page has been properly executed;

1.1.5 "**Customer Data**" means any data including where such data contains Personal Data, Processed pursuant to this DPA, where Verint's customer is the Data Controller, Verint is a Data Processor and the Vendor is a Verint subprocessor;

1.1.6 "**Data Controller**" means 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 respect of **(i)** Verint Data, means Verint, and **(ii)** Customer Data, means the applicable Verint customer.

1.1.7 "**Data Privacy Framework**" means 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;

1.1.8 "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded or replaced;

1.1.9 "**Data Processor**" means the Vendor;

1.1.10 "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates;

1.1.11 "**Personal Data**" shall have the meaning set out in, and will be interpreted in accordance with Privacy Laws;

1.1.12 "**Personal Data Breach**" means 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;

1.1.13 "**Principal Agreement**" means the agreement to which this DPA forms a part as incorporated by reference in the Cover Page.

1.1.14 "**Privacy Laws**" means as applicable to the Processing of Protected Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation;

1.1.15 "**Process**" or "**Processing**" or "**Processed**" means any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as access, collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and in the context of this DPA, the nature of the Vendor's Processing is set out on the Cover Page;

1.1.16 "**Protected Data**" means either:

1.1.16.1 Customer Data; or

1.1.16.2 Verint Data,

which is Processed by the Vendor pursuant to the terms of this DPA and the Principal Agreement,

1.1.17 "**Restricted Transfer**" means:

1.1.17.1 a transfer of Protected Data from Verint to Vendor or Verint to Vendor Affiliate (as the case shall be);

1.1.17.2 a transfer of Protected Data from Vendor to an Authorised Subprocessor; or

1.1.17.3 an onward transfer of Protected Data from an Authorised Subprocessor to another Authorised Subprocessor;

in each case, where the entity importing the Protected Data is based outside the jurisdiction of the exporting entity and therefore such transfer would otherwise be prohibited by Privacy Laws in the absence of appropriate safeguards, including **(a)** an Adequacy Decision, **(b)** execution of Standard Contractual Clauses, **(c)** by the terms of other forms data transfer agreements or processes that are deemed appropriate by applicable Privacy Laws;

1.1.18 "**Services**" means the services and other activities to be supplied or carried out by or on behalf of Vendor for Verint pursuant to the Principal Agreement;

1.1.19 "**Standard Contractual Clauses**" means 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;

1.1.20 "**Supervisory Authority**" means an independent public authority which is established in a jurisdiction under Privacy Laws with competence in matters pertaining to data protection;

1.1.21 "**Verint Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Verint, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.22 "**Verint Data**" means any data including where such data contains Personal Data, Processed pursuant to this DPA, where Verint is the Data Controller and the Vendor is a Data Processor;

1.1.23 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.24 "**Written Subcontract**" means a binding written agreement between the Vendor and any Authorised Subprocessor including terms which offer at least the same level of protection for Protected Data as those set out in this DPA.

1.2 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

1.3 References in this DPA to Vendor include reference to Vendor Affiliates where such Vendor Affiliates are Authorised Subprocessors.

2. AUTHORITY.

Vendor warrants and represents that, before any Authorised Subprocessor Processes any Protected Data, Vendor's entry into this DPA as agent for and on behalf of that Authorised Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Authorised Subprocessor.

3. PROCESSING OF PROTECTED DATA.

3.1 Vendor will, and will ensure that each Authorised Subprocessor will:

3.1.1 comply with Privacy Laws in relation to the Processing of Protected Data;

3.1.2 only Process Protected Data in accordance with Verint's documented instructions which will include as authorised under this DPA and the Principal Agreement where Processing is expressly required to comply with the Principal Agreement;

 REVDECEMBER2024

3.1.3 not sell Protected Data; and

3.1.4 not transfer or dispose of Protected Data unless authorised under this DPA.

3.2 Subject to the provisions of clauses 3.3-3.4, Verint hereby instructs Vendor:

3.2.1 to Process Protected Data; and

3.2.2 to conduct Authorised Transfer(s) of Protected Data;

in each case as strictly as necessary for the provision of the Services and consistent with the Principal Agreement and this DPA.

3.3 The Cover Page to this DPA sets out the subject-matter, nature and purpose, duration of the processing, the type(s) of Personal Data being Processed, and the categories of Data Subjects pertaining to the Vendor's Processing or transferring of Protected Data and shall form the instruction from Verint to Vendor. Verint may make amendments to the Cover Page by prior written notice to Vendor from time to time as Verint reasonably considers necessary to meet the requirements of Privacy Laws.

3.4 Vendor shall immediately notify Verint, if, in its opinion, any instruction given by Verint to Vendor under this DPA infringes Privacy Laws.

3.5 Vendor shall only Process Protected Data for the duration of the Principal Agreement, or other period if specified on the Cover Page or in other written instructions provided by Verint.

4. **VENDOR PERSONNEL.**

Vendor shall take all steps to ensure (a) the reliability of any employee, agent or vendor acting on its behalf who may have access to the Protected Data, (b) in each case that access is strictly limited to those individuals who need to know/access the relevant Protected Data for the purposes of the Principal Agreement, and (c) that all such individuals are subject to binding confidentiality undertakings and have undertaken appropriate training in relation to the protection of Personal Data.

5. **SECURITY.**

General Requirements

5.1 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 natural persons, Vendor shall, in relation to the Protected Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk.

5.2 In assessing the appropriate level of security, Vendor shall take account in particular of the risks that are presented by Processing and in particular the risks to Data Subjects arising from a potential Personal Data Breach.

5.3 Vendor shall implement and maintain technical and organisational measures applicable to the systems used to provide the Services at least as sophisticated as, or greater than, those technical and organisational measures set out in Verint's Vendor Information Security Schedule set out at https://www.verint.com/Assets/resources/resource-types/legal/vendor-information-security-requirements.pdf.

5.4 In addition to the foregoing, the Vendor shall implement any additional security measures required under applicable Privacy Laws for the safeguarding of Protected Data.

6. **SUBPROCESSING.**

6.1 Vendor shall only appoint subprocessors which enable Vendor to comply with Privacy Laws and this DPA, and Vendor shall obtain prior written authorisation in respect of each subprocessor and shall not use any subprocessor to undertake Processing of the Protected Data without the prior written authorisation of Verint. Prior written authorisation includes where such subprocessors are referred to in the Cover Page of this DPA or otherwise agreed in writing by Verint, and each such authorised subprocessor shall deemed to be an Authorised Subprocessor for the purposes of this DPA and the Principal Agreement.

6.2 Where Verint's written authorisation in respect of an Authorised Subprocessor is included in the Cover Page of this DPA and therefore such Authorised Subprocessor is classified as an existing appointed subprocessor of the Vendor, then Vendor shall provide written evidence upon Verint's request to enable Verint to verify the Authorised Subprocessor's activities relating to the Processing of Protected Data.

6.3 With respect to each Authorised Subprocessor, Vendor shall:

6.3.1 before the Authorised Subprocessor first Processes Protected Data (or, where relevant, in accordance with Section 6.2), carry out adequate due diligence to ensure that the Authorised Subprocessor is capable of providing the level of protection for Protected Data required by the Principal

Agreement and this DPA and upon Verint's request provide written evidence thereof;

6.3.2 ensure that each Authorised Subprocessor is subject to a Written Subcontract and ensure that each Written Subcontract contains a prohibition on further subcontracting of the Processing of Protected Data (to any other subprocessor) unless with Verint's prior written consent;

6.3.3 ensure the Written Subcontract incorporates the Standard Contractual Clauses in respect of any Processing by the Authorised Subcontractor that involves an Authorised Transfer under this DPA; and

6.3.4 provide to Verint for review a copy of the Written Subcontract as Verint may request from time to time to enable Verint to verify compliance with this Section 6 (which copy may be redacted to remove confidential commercial information not relevant to the requirements of this DPA).

6.4 Vendor shall ensure that each Authorised Subprocessor performs the obligations under Sections 3, 4, 5, 6, 7.1, 8.1, 9 and 10.1, as they apply to Processing of Protected Data carried out by that Authorised Subprocessor, as if it were party to this DPA in place of Vendor.

7. **DATA SUBJECT RIGHTS.**

7.1 Taking into account the nature of the Processing, Vendor shall assist in the fulfilment of Verint or Verint Affiliate's obligations to respond to requests to exercise data subject rights under Privacy Laws. Vendor shall action such requests to the extent instructed by Verint.

7.2 Vendor shall:

7.2.1 promptly notify Verint if Vendor receives a request from a Data Subject under Privacy Laws in respect of Protected Data; and

7.2.2 ensure that the Vendor does not respond to that request except on the documented instructions of Verint or as required by the Privacy Laws to which the Vendor is subject, in which case Vendor shall to the extent permitted by Privacy Laws inform Verint of that legal requirement before the Vendor responds to the request.

8. **PERSONAL DATA BREACH.**

8.1 Vendor shall notify Verint by contacting Verint's Global Privacy Officer by submitting its notice via Verint's Privacy Portal without undue delay upon Vendor becoming aware of a Personal Data Breach affecting Protected Data, providing Verint with sufficient information to allow Verint to meet any obligations to notify the Data Controller, a Supervisory Authority, and/or Data Subjects, as applicable, pursuant to Privacy Laws. Such notification shall as a minimum:

8.1.1 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;

8.1.2 communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 Vendor shall co-operate with Verint, and, where applicable, the Data Controller (to the extent the Personal Data Breach relates to Customer Data) and take such reasonable commercial steps as are directed by Verint, and, where applicable, the Data Controller (to the extent the Personal Data Breach relates to Customer Data), to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION.**

Vendor shall provide reasonable assistance to Verint and, where applicable, the Data Controller (to the extent the Processing relates to Customer Data) with any data protection impact assessments, and prior consultations with a Supervisory Authority, which Verint or the applicable Data Controller reasonably considers to be required in order to comply with Privacy Laws, in each case solely in relation to Processing of Protected Data by, and taking into account the nature of the Processing and information available to the Vendor.

10. **DELETION OR RETURN OF PROTECTED DATA.**

10.1 Vendor shall promptly, and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Protected Data (the "Cessation Date"), return or, solely upon Verint's written request, delete and procure the deletion of all copies of Protected Data in the custody, power or possession of the Vendor.

 REVDECEMBER2024

10.2 The Vendor may retain Protected Data only to the extent and for such period as required by Privacy Laws provided the provisions of this DPA will continue to apply and Vendor shall ensure the confidentiality of all such Protected Data and shall ensure that such Protected Data is only Processed as necessary for the purpose(s) specified in Privacy Laws requiring its storage and for no other purpose.

10.3 Vendor shall provide written certification to Verint that Vendor has fully complied with this Section 10 within thirty (30) days of such request.

11. AUDIT RIGHTS.

11.1 Subject to Section 11.2, Vendor shall make available to Verint on request (or periodically where required pursuant to applicable Privacy Laws) all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Verint or an auditor appointed by Verint in relation to the Processing of the Protected Data by the Vendor. Verint may exercise the rights set out in this Section 11 either as a Data Controller in relation to Verint Data or as a Data Processor in relation to Customer Data.

11.2 Verint shall give Vendor reasonable notice of any audit or inspection to be conducted under Section 11.1 except where **(i)** Verint reasonably considers it necessary to commence an audit or inspection immediately because of genuine concerns as to Vendor's compliance with this DPA; or **(ii)** as otherwise required by Privacy Laws or a Supervisory Authority.

12. AUTHORISED TRANSFERS.

12.1 Whenever a Restricted Transfer occurs, the entities involved in the transfer will ensure that such transfer is made in compliance with the relevant provisions of Privacy Law.

12.2 Where Vendor has certified compliance with the Data Privacy Framework, 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 Vendor's self-certification to the Data Privacy Framework, then:

12.2.1 Vendor 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 Vendor no longer maintains certification under the Data Privacy Framework, in which case the provisions of Section 12.3 shall apply; and

12.2.2 Without limiting Vendor's obligations under Section 5, Vendor 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 Verint if it is unable to comply with this requirement.

12.3 Subject to Section 12.2, where a Restricted Transfer occurs unless the Restricted Transfers is subject to a valid cross border transfer mechanism under Privacy Laws, including but not limited to an Adequacy Decision, Vendor (on behalf of itself and all Authorised Subprocessors) and Verint agree that the Standard Contractual Clauses are hereby incorporated into this Agreement.

12.4 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.

12.5 Vendor shall (or shall ensure that the Authorised Subprocessor) where required by Privacy Law, provide Verint 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 upon the request of Verint.

12.6 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.

12.7 Vendor warrants and represents that it 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 or under Privacy Laws. Where any supplementary measures are required by Privacy Law or Supervisory Authority to continue Processing in the Destination Country, Vendor shall promptly implement (or shall require that the Authorised Subprocessor implements) such supplementary measures to satisfy the Privacy Law and shall provide Verint with evidence of having done so.

13. INDEMNITY.

Vendor shall be liable for and shall indemnify (and keep indemnified) Verint against each and every action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and disbursements on a solicitor and client basis) and demand incurred by Verint which arise directly or in connection with the Vendor's Processing in breach of this DPA.

14. GENERAL TERMS.

Governing law and jurisdiction

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

14.2 Without prejudice to the provisions of the Standard Contractual Clauses which are mandatory:

14.2.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal 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; and

14.2.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

14.3 Vendor shall, unless legally prohibited from doing so:

14.3.1 promptly notify Verint 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

14.3.2 promptly notify Verint 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

14.3.3 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 Verint with as much information as legally permissible.

Order of precedence

14.4 Nothing in this DPA reduces Vendor's obligations under the Principal Agreement in relation to the protection of Protected Data or otherwise or permits Vendor to Process (or permit the Processing of) Protected Data in a manner which is prohibited by the Principal Agreement. In relation to Restricted Transfers only, in the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. In the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Changes in Privacy Laws, etc.

14.5 If any variation is required to this DPA as a result of a change in Privacy Laws, including any variation which is required to the Standard Contractual Clauses, 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 the Standard Contractual Clauses, to address such changes.

Incorporation of Hyper-links

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

Severance

14.7 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 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.

 REVDECEMBER2024

Data Processing Terms and Conditions

APPENDIX 1

EUROPEAN, SWISS AND UNITED KINGDOM TERRITORY SPECIFIC TERMS

1. "**GDPR**" shall mean Regulation (EU) 2016/679 of The European Parliament and of the Council

2. 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 available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en 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 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.

3. In respect of any Restricted Transfers where Verint is exporting personal data to a Vendor or Authorised Subprocessor based outside the European Economic Area, the parties agree to the following:

   3.1. The EU Standard Contractual Clauses will be incorporated into this DPA;

   3.2. The modules and Annexes of the EU Standard Contractual Clauses are set out at https://www.verint.com/wp-content/uploads/2025/01/eu-standards-contractual-clauses.pdf to this DPA ("**the Modules**"); and

   3.3. The parties agree that the signature(s) in any form in any form, including handwritten or electronic) given in connection with the execution of this DPA or the Principal Agreement constitutes signature and acceptance of Annex 1.A to this Appendix 1 of this DPA and acceptance and incorporation of the EU Standard Contractual Clauses, and the dates of such signature(s) shall apply (respectively)..

4. In respect of any Restricted Transfers where Verint is exporting personal data to a Vendor based outside the United Kingdom, the parties agree to the following:

   4.1. The Standard Contractual Clauses shall mean the UK Addendum where "UK Addendum" means "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 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);

   4.2. The UK Addendum will be incorporated into this DPA;

   4.3. The parties agree that the signature(s) in any form in any form, including handwritten or electronic) given in connection with the execution of this DPA or the Principal Agreement constitutes signature and acceptance of Annex 1.A to this Appendix 1 of this DPA and acceptance and incorporation of Annex 1A to this Schedule and acceptance and incorporation of the UK Addendum , and the dates of such signature(s) shall apply (respectively); and

   4.4. Tables 1 to 4 (inclusive) to the UK Addendum shall be deemed completed with the information set out in the Modules;

5. In respect of any Restricted Transfers from Switzerland, the parties agree to the following:

   5.1. 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 in the Modules;

   5.2. The EU Standard Contractual Clauses will be incorporated into this DPA;

   5.3. 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 this 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

Data exporter(s):

1.
   Name: … Verint

   Address: … The address specified for Verint in the Principal 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 Principal Agreement, associated Statements of Work and this DPA

   Signature and date: … as evidenced by signature of the DPA

   Role (controller/processor): …processor

   …

2.

Data importer(s):

Data Processing Terms and Conditions

1.
Name: … Vendor or Vendor Affiliate

Address: …The Vendor address specified in the Principal Agreement

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …as specified in the Principal Agreement, associated Statements of Work and this DPA

Signature and date: … as evidenced by signature of the DPA

Role (controller/processor): … processor

…

2.

ANNEXES IB, 1C, II and III to the EU Standard Contractual Clauses shall be completed with the details the Modules and the Cover Page

VERINT PROPRIETARY AND CONFIDENTIAL INFORMATION REVDECEMBER2024

Data Processing Terms and Conditions

APPENDIX 2
US STATES PRIVACY LAW SPECIFIC PROVISIONS

These US States Privacy Law Specific Provisions ("**US Privacy Terms**") apply to the Processing by Verint Personal Data originating from the U.S., and are supplemental to the terms of the DPA.

Capitalized terms used but not defined in these US Privacy Terms shall have the same meanings as set out elsewhere in the DPA.

1. Definitions

1.1 **"California Privacy Law"** shall together mean the California Consumer Privacy Act of 2018 and its implementing regulations, the California Privacy Rights Act of 2020 and its implementing regulations.

1.2 **"Sell"** shall have the same meaning as set forth in California Privacy Law.

1.3 **"Share"** shall have the same meaning as set forth in California Privacy Law.

1.4 **"Service Provider"** shall mean the Vendor and refer to a service provider or subcontractor, as defined by applicable US State Privacy Laws.

1.5 **US State Privacy Laws** shall mean and refer to all United States data protection and privacy laws which may be applicable to Vendor in the processing of Vendor Personal Information as part of the performance of the Services, including but not limited to the California Consumer Privacy Act of 2018 and its implementing regulations, the California Privacy Rights Act of 2020 and its implementing regulations, the Virginia Personal Information Privacy Act of 2021 and its implementing regulations, the Colorado Privacy Act of 2021 and its implementing regulations, etc.

2. Scope of US Privacy Terms

These US Privacy Terms apply to Vendor acting as Service Provider processing Personal Data under US State Privacy Laws, where such processing is described in the Agreement and this DPA.

3. Roles and Responsibilities

3.1 **Vendor Obligations.**

3.1.1 **Purpose Limitation**. Vendor shall Process the Personal Data for the purposes of the performance of the Services as described in the Agreement except where otherwise required or permitted by US State Privacy Laws.

3.1.2 **Obligations.** Vendor will:

(a) Operate exclusively as a Service Provider and comply with the applicable US State Privacy Law obligations.

(b) Provide the same level of privacy protection as required by the applicable US State Privacy Law.

(c) Notify Vendor if it can no longer meet its US State Privacy Law obligations.

(d) Not Sell or Share the Personal Data including, for the avoidance of doubt, not use the Personal Data for cross-context behavioral advertising.

(e) Not retain, use, or disclose the Personal Data for any other purpose other than as agreed upon in the Agreement, outside the direct business relationship between the Verint and Vendor, or as permitted by applicable US State Privacy Law.

(f) Not combine the Personal Data it receives from, or on behalf of Verint with Personal Data it receives from, or on behalf of, another person subject to the exceptions under applicable US State Privacy Law.

(g) Cooperate with Verint to determine reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

3.1.3 **Cooperation.** Vendor will cooperate with Verint to make available all information in its possession to demonstrate compliance with US State Privacy Laws.

3.2 **Vendor rights**. Vendor may take reasonable and appropriate steps to ensure that Verint uses Personal Data in a manner consistent with Vendor's obligations under U.S. State Privacy Laws.

4. Miscellaneous

Unless the above explicitly states otherwise, the terms and conditions of the Agreement, and of the DPA, shall, as relevant, apply to the US Privacy Terms. In case of any conflict between the terms of the Agreement, the DPA, and the terms of these US Privacy Terms, these US Privacy Terms prevail with regard to data processing activities subject to US State Privacy Laws.

Data Processing Terms and Conditions

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/2025/01/eu-standards-contractual-clauses.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.

REVDECEMBER2024