VERINT

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

This DPA forms part of the applicable agreement in which this DPA is incorporated between the applicable Verint entity and the Customer ("**Agreement**").

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 have data transfer restrictions, a country that the Supervisory Authority or other body in such jurisdiction recognises as providing an adequate level of data protection as required by such jurisdiction's Privacy Laws such that transfer to that country shall be permitted without additional requirements;

1.1.2 "**Affiliate**" means 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;

1.1.3 "**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 the context of this DPA shall mean the Customer;

1.1.4 "**Data Processing Instructions**" means the Processing instructions set out at https://www.verint.com/our-company/legal-documents/dpa/data-processing-schedule/;

1.1.5 "**Data Processor**" means 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;

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

1.1.7 "**Information Security Schedule**" means 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/our-company/legal-documents/dpa/security-schedule;

1.1.8 "**Personal Data**" shall have 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 in Customer Data, Processed by Verint in accordance with the Services as outlined in the Data Processing Instructions, which relates to a Data Subject;

1.1.9 "**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;

1.1.10 "**Privacy Laws**" means national, federal, union, state and other laws, as applicable to Personal Data in the context and jurisdiction of the Processing, concerning the regulation of the collection, retention, processing, data security, disclosure, trans-border data flows, use of web-site cookies, email communications, use of IP addresses and meta-data collection;

1.1.11 "**Process**" or "**Processing**" means 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 Data Processing Instructions;

1.1.12 "**Restricted Transfer**" means:

1.1.12.1 a transfer of Personal Data from Customer to Verint; or

1.1.12.2 an onward transfer of Personal Data from Verint to a Subprocessor,

in each case, where such transfer outside of jurisdiction of Customer would be prohibited by Privacy Laws in the absence of an approved method of 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 processes;

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

1.1.14 "**Standard Contractual Clauses**" means the contractual clauses approved by a Supervisory Authority pursuant to Privacy Laws which provides for multi-jurisdictional transfer of Personal Data from one jurisdiction to another where such transfer would otherwise be a Restricted Transfer;

1.1.15 "**Subprocessor**" means 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; and

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

1.2 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 Verint include to Verint Affiliates where such Verint Affiliates are Subprocessors.

1.4 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. Except as modified below, the terms of the Agreement shall remain unchanged and in full force and effect.

2. Processing of Personal Data

2.1 Verint will not:

2.1.1 Process Personal Data other than on Customer's documented instructions (set out in this DPA and in the Agreement) unless Processing is required by a Supervisory Authority; or

2.1.2 sell Personal Data received from Customer or obtained in connection with the provision of the Services to Customer.

2.2 Customer on behalf of itself and each Customer Affiliate:

2.2.1 instructs Verint:

2.2.1.1 to Process Personal Data; and

2.2.1.2 in particular, transfer Personal Data to any country or territory;

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

2.3 The Data Processing Instructions sets out the subject matter and other details regarding the Processing of the Personal Data contemplated as part of the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing.

3. Verint Personnel

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

3.1 committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of the Personal Data; and

3.2 undertaken appropriate training in relation to protection of Personal Data.

4. Security

4.1 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, Verint shall in relation to the Personal Data implement appropriate technical and organisational measures designed to provide a level of security appropriate to that risk in the provision of the Services and for the purposes of this DPA Verint's technical and organisational measures are set out in the Information Security Schedule.

4.2 In assessing the appropriate level of security, Verint shall take account in particular of the risks that are presented by Processing.

5. Subprocessing

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

5.2 Notwithstanding any notice requirements in the Agreement, before Verint engages any new Subprocessor, Verint shall give Customer notice of such appointment, including details of the Processing to be undertaken by the proposed Subprocessor. In addition to any other notifications, 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) to the proposed Subprocessor or Data Processing Instructions ("**Objection**"), then 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 Customer's 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:

5.3.1 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;

5.3.2 ensure that the Subprocessor is subject to a written agreement with Verint that includes appropriate data protection provisions; and

5.3.3 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.

5.4 Verint shall ensure that each Subprocessor performs the obligations under this DPA as they apply to Processing of Personal Data carried out by that Subprocessor, as if such Subprocessor were party to this DPA in place of Verint.

6. Data Subject Rights

6.1 Verint shall:

6.1.1 upon becoming aware, promptly notify Customer if Verint receives a request from a Data Subject relating to an actionable Data Subject right under any Privacy Law in respect of Personal Data;

6.1.2 not respond to that request except on the documented instructions of Customer or as required by a Supervisory Authority; and

6.1.3 upon request from Customer where required by Privacy Laws and in the context of the Services, reasonably assist Customer in dealing with an actionable Data Subject 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. To the extent such functionality is not available, in order for Verint to provide such reasonable assistance, Customer must communicate such request in writing to Verint providing sufficient information to enable Verint to pinpoint and subsequently amend, export or delete the applicable record.

7. Personal Data Breach

7.1 Verint shall notify Customer without undue delay upon Verint or any Subprocessor becoming aware of a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Privacy Laws. Subject to Section 7.3 below, such notification shall as a minimum:

7.1.1 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;

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

7.1.3 describe the likely consequences of the Personal Data Breach in so far as Verint is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

7.1.4 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 each such 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, the information may be provided in phases without undue further delay.

8. Data Protection Impact Assessment and Prior Consultation

8.1 To the extent necessary, Verint shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Privacy Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Verint. To the extent that such impact assessment and/or prior consultation requires assistance beyond Verint providing the applicable Verint processing record(s) and Documentation, Verint shall reserve the right to charge Customer such engagement at Verint's then current daily rates.

9. Deletion or return of Personal Data

9.1 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, Verint will either 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 notice or liability to Customer. Where Customer requests Verint 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 and only to the extent and for such period as required by Privacy Laws or any other statutory requirement to which Verint is subject and always provided that (a) during such retention period the provisions of this DPA will continue to apply, (b) that Verint shall ensure the confidentiality of all such Personal Data, and (c) Verint shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws 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 information in relation to Verint's technical and organisational security measures used to protect the Personal Data in relation to the Services provided in order to demonstrate compliance with Privacy Laws.

10.2 Verint shall ensure a security audit of its technical and organisational security measures is carried out at least annually in compliance with Privacy Laws. Such security audit will be performed according to ISO 27001 standards by an internal qualified auditor within Verint. The results of such security audit will be documented in a summary report. Verint shall promptly provide Customer upon request with (i) a confidential summary of such report; and (ii) evidences of appropriate remediation of any critical issues within four (4) weeks from date of issuance of the audit report.

10.3 If, following the completion of the steps set out in Sections 10.1 and 10.2 Customer reasonably believes that Verint is non-compliant with Privacy Laws, Customer may request that Verint make available, either by webinar or in a face-to-face review, extracts of all relevant information necessary to further demonstrate compliance with Privacy Laws. Customer undertaking such review shall give Verint reasonable notice, by contacting Verint's Information Security Director (in the Americas and APAC regions to privacy@verint.com or in EMEA to EMEA.Privacy@Verint.com), of any review to be conducted under this Section 10.3.

10.4 In the event that Customer reasonably believes that its findings following the steps set out in Section 10.3 do not enable Customer to comply materially with Customer's obligations mandated under the Privacy Laws in relation to its appointment of Verint, then Customer may give Verint not less than thirty (30) days prior written notice of its intention, undertake an audit which may include inspections of Verint to be conducted by Customer or an auditor mandated by Customer (not being a competitor of Verint). Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between Customer (or its mandated 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 where it would place Verint in breach of Verint's confidentiality obligations to other Verint customers vendors and/or partners generally or otherwise cause Verint to breach laws applicable to Verint. Customer (or auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to Verint's premises, equipment, personnel and business in the course of such a review. To the extent that such audit performed in accordance with this Section 10.4 exceeds one (1) business day, Verint shall reserve the right to charge Customer for each additional day at its then current daily rates.

10.5 If following such an audit or inspection under Section 10.4, Customer, acting reasonably, determines that Verint is non-compliant with Privacy Laws then Customer will provide details thereof to Verint upon receipt of which Verint shall provide its 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; the mutually agreed plan being 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 Services in part or in whole which relates to the non-compliant Processing and the remaining Services shall otherwise continue unaffected by such termination.

10.6 The rights of Customer under 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 Customer (as "data exporter") and Verint, as appropriate, (as "data importer") hereby agree that the Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Customer to Verint. Each Party agrees to execute the Standard Contractual Clauses upon request of the other Party and further agrees that absent of execution the terms and conditions of the Standard Contractual Clauses shall in any event apply to any Restricted Transfer. Where such Standard Contractual Clauses must be fully executed to take effect and Customer has not executed such Standard Contractual Clauses as set out in this Section 11, Customer authorises Verint to enter into the Standard Contractual Clauses for and on behalf of Customer as data exporter with each applicable data importer.

11.2 For the purposes of Appendix 1 or other relevant part of the Standard Contractual Clauses, the Data Processing Instructions to this DPA sets out the Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing (processing operations).

11.3 For the purposes of Appendix 2 or other relevant part of the Standard Contractual Clauses, the Information Security Schedule sets out the description of the technical and organisational security measures implemented by Verint (the data importer) in accordance with clauses 4(d) and 5(c) of the Standard Contractual Clauses.

VERINT

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, both Parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws and any such additional measures agreed to by the Parties will be documented 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, 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.

13. General Terms

13.1 The applicable law provisions of this Agreement are without prejudice to clauses 7 (Mediation and Jurisdiction) and 10 (Governing Law) of the Standard Contractual Clauses where applicable to Restricted Transfers of Personal Data from the European Union (including the United Kingdom) to a third country.