VERINT

This Master SaaS Agreement ("**Agreement**") is entered into as of the date of last signature below ("**Effective Date**") between Verint Systems UK Limited ("**Verint**"), a company registered in England with company registration number 02602824, whose registered address and principal place of business is 2nd Floor, The Forge, 43 Church Street, Woking, GU21 6HT, and its Affiliates, and [redacted] ("**Customer**"), whose registered address and principal place of business is [redacted].

For and in consideration of the representations and promises of the parties set forth herein, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

Agreement. This Agreement consists of this Signature Page, the following Schedules, and any Orders executed during the term of this Agreement:

- ☒ Schedule A Definitions
- ☒ Schedule B General Terms and Conditions
- ☒ Schedule C Service Levels
- ☒ Schedule D Information Security Schedule
- ☒ Schedule E Data Processing Schedule
- ☒ Schedule F Professional Services Rate Card

In addition to the terms defined elsewhere in this Agreement, capitalised terms shall have the meaning set forth in Schedule A entitled "Definitions". This Agreement constitutes the entire agreement and understanding of the parties relating to the subject matter hereof, superseding all prior or contemporaneous agreements, representations, promises and understandings, whether written, electronic, oral or otherwise. Each party acknowledges and agrees that by executing the terms and conditions specified in this Agreement, **(i)** it is not relying upon any other statements, representations, warranties, promises, assurances, or the like, **(ii)** no remedies are or will be available to a party with respect to the foregoing, and **(iii)** such remedies are unconditionally and irrevocably waived; provided, the foregoing shall not apply to any acts of fraud by a party. For the avoidance of doubt, in the event of any prior agreement(s) between the parties or its predecessor(s), where such agreement(s) covered the same subject matter as this Agreement, those prior agreements are hereby terminated, and any products licenced thereunder or services yet to be performed shall now be subject to the terms and conditions of this Agreement. By placing an Order with Verint, Customer agrees that the terms and conditions of this Agreement shall apply to and govern that Order. Except with respect to the identification of the specific products, services and pricing applicable to an Order, additional or conflicting terms in any Order shall have no force or effect on either party, unless that Order is signed by an authorised representative of each party or the Verint provided quote, order form or schedule is exchanged between the parties and attached to, or specifically referenced in, Customer's purchase order, and then those terms exchanged between the parties shall apply to the parties solely for that Order. Except as otherwise specified herein, any additional or conflicting terms contained in any other document (including, without limitation, any preprinted, additional or conflicting terms on any Customer purchase order, or acknowledgement from either party) shall be null, void and of no effect on either party. Notwithstanding the foregoing, this Agreement may be amended by an authorised representative of each party in a duly executed written amendment referencing this Agreement and expressing the intent of each party to amend these terms and conditions.

THIS AGREEMENT SHALL NOT BE EFFECTIVE UNTIL EXECUTED BY AN AUTHORISED REPRESENTATIVE OF EACH PARTY.

IN WITNESS WHEREOF, Verint and Customer have caused this Agreement to be executed by their duly authorised representatives as of the Effective Date.

VERINT SYSTEMS UK LIMITED	[redacted] **CUSTOMER**
NAME SIGNED	NAME SIGNED
NAME	NAME
TITLE	TITLE
DATE	DATE

SCHEDULE A
DEFINITIONS

This Schedule A is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule A is attached. All capitalised terms shall have the meaning ascribed to them, including the following:

1 **Access Term.** The term, as further described in Section 2 of Schedule B, for which Verint has contractually agreed to provide Customer with access to the SaaS Services in accordance with an Order.

2 **Affiliate.** Any entity which now or in the future controls, is controlled by, or is under common control with the signatory to this Agreement, 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. With respect to **(i)** Customer, an Affiliate may not be a competitor of Verint, and **(ii)** Verint, an Affiliate is limited solely to those Verint entities indicating assent to the terms and conditions of this Agreement by accepting an Order from Customer hereunder or as otherwise expressly provided for in this Agreement. For each Order signed by or on behalf of an Affiliate, "Customer", "Verint" and "party" (each as applicable) as used herein shall mean for all purposes the Affiliate identified therein.

3 **Billing Period.** The billing period for which the SaaS Access Fees shall be calculated and invoiced to Customer in advance on a pro rata basis as follows: **(i)** annual billing period(s) for an Access Term for a SaaS Service, and **(ii)** for any add-on Order(s) for that SaaS Service, a proportionate period for the initial billing cycle to enable annual co-billing thereafter.

4 **Confidential Information.** Any non-public information, technical data, or know-how, including, without limitation, that which relates to: **(i)** research, product plans, products, pricing, services, customers, personnel, markets, software, software code, software documentation, developments, inventions, lists, trade secrets, data compilations, processes, designs, drawings, engineering, hardware configuration information, marketing or finances, which is designated in writing to be confidential or proprietary at the time of disclosure if provided in tangible form, or if provided in non-tangible form, shall be identified by the disclosing party at the time of disclosure as confidential or proprietary, **(ii)** with respect to Verint, information concerning the SaaS Services, Hosted Environment, Documentation and any Software provided hereunder and/or materials resulting from Professional Services, any derivatives thereto, the terms and conditions of this Agreement, and **(iii)** with respect to Customer, any Customer Data. Notwithstanding the foregoing, Confidential Information does not include information, technical data or know-how that is: **(a)** in the public domain or becomes available to the public and not as a result of the act or omission of the receiving party; **(b)** without restriction on disclosure, rightfully obtained by the receiving party from a third party or lawfully in the possession of the receiving party at the time of disclosure; or **(c)** approved for release by written authorisation of the disclosing party.

5 **Customer Data.** All content and data, including but not limited to Personal Data, either provided by Customer or entered on its behalf, in either case, through use of the SaaS Services, or collected or generated by the SaaS Services on behalf of Customer, and which remains in Verint's possession and control for further processing.

6 **Customer Environment.** The computing environment separately procured, prepared and maintained by Customer for the access and use of the SaaS Services, as further specified in Section 4.2 of Schedule B.

7 **Designated Employees.** A reasonable number of Customer Personnel (including Customer's system administrator), who have received training from Verint. Designated Employees may be changed by notice to Verint.

8 **Documentation.** Verint's documentation describing the specifications and use of the SaaS Services and any Software provided as updated from time to time.

9 **Error.** A failure of the SaaS Services to substantially conform to the Documentation, that Verint can replicate or Customer can duplicate.

10 **Error Correction.** Revisions, modifications, alterations, and additions to the SaaS Services, installed by Verint in the Hosted Environment as bug fixes or workarounds to resolve Errors.

11 **Fees.** The Professional Service Fees, SaaS Access Fees and/or other fees as specified in this Agreement or in an Order.

12 **Hosted Environment.** Verint or its third party's technical environment required to operate and provide access to the relevant SaaS Services, as further specified in Section 4.2 of Schedule B.

13 **Intellectual Property Rights.** Any and all tangible and intangible rights, title and interest in and to: **(i)** works of authorship, including but not limited to copyrights, neighbouring rights, moral rights, and mask works, and all derivative works thereof, **(ii)** trademarks and trade names, **(iii)** Confidential Information, trade secrets and know-how, **(iv)** patents, designs, algorithms and other industrial property, **(v)** all other intellectual and industrial property rights whether arising by operation of law, contract, licence, or otherwise, and **(vi)** all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force.

14 **Order.** The details of a Customer order **(i)** on an order form or schedule provided by Verint and signed by Customer **(ii)** on Customer's purchase order provided to and accepted by Verint, or **(iii)** placed on Customer's behalf by an authorised Verint reseller on and accepted by Verint. For the purposes of (iii), all terms and conditions of this Agreement shall apply as between Customer and Verint, except with respect to invoicing and payment terms.

15 **Overage.** Measured on a monthly basis, any actual usage of the SaaS Service which exceeds the SaaS Access Rights subscribed to by Customer under an Order or Orders applicable to the SaaS Service.

16 **Personal Data.** Any information relating to an identified or identifiable natural person (each a "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person which shall include information collected by the use of web-site cookies and IP addresses, and in the context of Verint's obligations under this Agreement, shall mean the Personal Data that remains in Verint's possession and control for further Processing in accordance with, and as further described in, this Agreement.

17 **Personnel.** With respect to Customer, **(i)** each of Customer's and/or Customer's Affiliate's employees and independent contractors (in each case, not a competitor of Verint) under obligations **(a)** of confidentiality and nondisclosure, and **(b)** to protect Verint Intellectual Property, and **(ii)** any other individuals with access to components of the SaaS Service designated for external use, which Customer authorises to use the SaaS Services purchased and/or the SaaS Access Rights procured hereunder; with respect to Verint, each Verint employee or subcontractor under obligations of confidentiality and nondisclosure which performs on behalf of Verint hereunder. For the avoidance of doubt, each party shall be responsible for its Personnel's compliance with this Agreement.

18 **Privacy Laws.** 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. For the avoidance of doubt this includes, in the context of this Agreement, (i) regulation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable law about the processing of personal data and privacy; and (iv) (to the extent that it applies) the EU GDPR.

19 **Process(ing)(ed).** 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, as described in this Agreement.

20 **Professional Services.** Configuration, consulting, training and/or other professional services specified on an Order.

21 **Professional Service Fees.** In Pounds Sterling, the fees identified on each Order on a fixed fee or time and material basis for Professional Services to be performed.

22 **SaaS Access Fees.** In Pounds Sterling, the fees due to Verint, as further specified in the Order, for use of the SaaS Services to the extent of the SaaS Access Rights, plus fees for any Overage.

23 **SaaS Access Rights.** The type and quantity of SaaS access rights granted to Customer on an Order(s) for use during the applicable Access Term.

24 **SaaS Services.** The online services offered by Verint as more fully described in the Documentation, and all SaaS Access Rights, each as specified on an Order.

25 **Service Levels.** The service level commitments from Verint with respect to the maintenance and support of the Hosted Environment and SaaS Services.

25.1 **Scheduled Downtime.** Any downtime scheduled to perform system maintenance, backup and upgrade functions for the Hosted Environment, and any other downtime incurred as a result of a Customer request.

25.2 **Total Time.** The total number of minutes in the applicable month.

25.3 **Unscheduled Downtime.** Any time outside of the Scheduled Downtime when the Hosted Environment is not available to perform operations. Unscheduled Downtime is measured in minutes.

25.4 **Uptime Percentage.** Total Time minus Unscheduled Downtime, divided by Total Time.

26 **Signature Page.** The cover page of this Agreement specifying the Schedules expressly incorporated into the Agreement, the general terms of the Agreement, and containing the signature of each party's authorised representative manifesting assent to the terms and conditions of this Agreement.

27 **Software.** Computer application programs (including, if applicable, any Updates and other developments provided to Customer hereunder) in object code form developed and owned by Verint or its licensor(s) and licenced for use hereunder.

28 **Updates.** Periodic improvements or additions to the SaaS Services, including Error Corrections and other changes to the SaaS Services, that may be provided hereunder, but excluding any new feature or substantial additional functionality available for the SaaS Service.

29 **Verint Intellectual Property.** All Intellectual Property Rights in the SaaS Services, Software, Documentation, Hosted Environment and all other Confidential Information provided by Verint hereunder.

SCHEDULE B
GENERAL TERMS AND CONDITIONS

This Schedule B is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule B is attached. The following general terms and conditions shall apply to this Agreement:

1 ACCESS RIGHTS.

1.1 Access Use Rights. During the Access Term, and solely for Customer's and its Affiliates' internal business use (which may include external use of designated components by Customer's Personnel), Verint grants to Customer a non-exclusive, non-transferable, non-assignable, personal right to use the SaaS Services specified in an Order through Internet access, up to the extent of the SaaS Access Rights specified in that Order, plus any Overage. With respect to the Documentation applicable to the SaaS Services, Customer may make a reasonable number of copies of the Documentation solely as needed for Customer's and its Affiliates' internal business purposes. With regards to the on-premise components and related Documentation, Verint grants to Customer, and Customer accepts, a nonexclusive, nonassignable, and nontransferable limited licence during the Access Term, to use the applicable on-premise components and related Documentation solely in conjunction with the SaaS Services for Customer's and its Affiliates' internal business purposes, and subject to the terms and conditions of this Agreement.

1.2 Restrictions. Customer acknowledges and agrees that the use rights provided hereunder do not grant any rights not explicitly expressed. All other such rights and interests in Verint Intellectual Property (including any derivatives thereto) are expressly reserved, owned by and remain vested in Verint and its third party vendor(s), and except for the limited use rights granted hereunder, Customer shall not assert any right, title, or interest in or to any Verint Intellectual Property, or portion thereof. Without limiting the foregoing, Customer acknowledges and agrees that no rights or any other interests are provided to Customer with respect to: **(i)** rights in or to the Hosted Environment, or SaaS Services, beyond those rights specified herein, **(ii)** rights to provide access or use of the Hosted Environment, SaaS Services and on-premise components to any other party, including, without limitation, any uses in the nature of a service bureau or application services provider, **(iii)** rights to obtain possession of copies of any component of the Hosted Environment or any software used to provide or perform the SaaS Service except with respect to on-premise component(s), and then only as expressly provided for in Section 1.1, or **(iv)** representations, warranties or other third party beneficiary rights from any Verint vendor.

2 AGREEMENT TERM; ACCESS TERM. This Agreement shall commence on the Effective Date and shall continue unless earlier terminated as provided in Section 13. Unless otherwise specified on the Order, an Access Term shall commence upon the effective date of the applicable Order and shall continue for twelve (12) months thereafter. In the event Customer places additional Orders for the same SaaS Service, Verint may adjust the duration of the additional Access Terms to co-terminate with the Access Terms for that SaaS Service. Each Access Term is non-cancelable, and upon expiration shall automatically renew for additional annual terms at Verint's then current rates, unless either party provides the other with no less than sixty (60) days prior written notice of its intent to not renew.

3 ORDERS.

3.1 Order Submittal. Customer and its Affiliate(s) may submit Orders to Verint, which may be sent via mail, telefax, email attachment, electronic procurement systems, and other means as the parties may decide from time to time. Each Order provided by Customer to Verint must reference the name and Effective Date of this Agreement, and contain information required by Verint, including, without limitation, as applicable: **(i)** the Verint quote number, **(ii)** the SaaS Services and quantity and types of SaaS Access Rights, **(iii)** any Professional Services to be provided, **(iv)** the billing address, **(v)** Customer contact names and phone numbers, and **(vi)** all applicable Fees. Customer and an Affiliate who submits an Order shall both be bound by this Agreement in relation to that Order and shall be jointly and severally liable to Verint for any breach of this Agreement by an Affiliate. Customer shall provide any Affiliate who submits an Order hereunder with a copy of this Agreement (although failure to provide such copy shall not limit or in any way affect Customer's or its Affiliate's obligations or liability hereunder).

3.2 Order Acceptance. All Orders are subject to Verint's acceptance, and to the terms and conditions of this Agreement. For each Order in accordance with this Section, Verint shall acknowledge acceptance of the Order by issuing an invoice in accordance with Section 8.

4 VERINT RESPONSIBILITIES.

4.1 Procedures and Technical Protocols. Verint will specify to Customer procedures according to which Customer may establish and obtain access to and use the features and functions of the SaaS Services, including, without limitation, provision of any access codes, passwords, technical specifications, connectivity standards or protocols, or any other relevant procedures.

4.2 SaaS Services. Verint will bear responsibility, at its own cost and expense, for the procurement, preparation, hosting, operation and maintenance of the Hosted Environment, including all facilities, hardware, software, telecommunication services, and all other technical requirements necessary to provide access to and use of the SaaS Services; provided Customer will be responsible for procuring and/or operating the Customer Environment, including computer systems, software and telecommunications services meeting such minimum technical requirements and, unless otherwise specified on an Order, for the installation and configuration of the on-premise components in that Customer Environment, each as Verint may specify in the Documentation.

4.3 Support.

4.3.1 Support and Updates. As part of the SaaS Services, Verint shall provide support for the Hosted Environment and SaaS Services. In addition to establishing and maintaining the Hosted Environment, Verint shall maintain the components of the Hosted Environment with all current Updates that Verint deems necessary for the SaaS Services. Verint shall use commercially reasonable efforts to implement any required Error Corrections. Access to the SaaS Services and maintenance of the Hosted Environment shall be in accordance with the Service Levels specified in Schedule C, and Customer shall, in accordance with the terms of Schedule C, have access to support through Verint's standard telephone, email and web support services.

4.3.2 Backup and Recovery of Data. As a part of the SaaS Services, Verint shall maintain a backup of all Customer Data that Verint is required to retain as a part of the SaaS Services stored in the Hosted Environment. In the event the Customer Data becomes destroyed, or corrupt, Verint shall use commercially reasonable efforts to restore all available data from backup, and remediate and recover such corrupt data.

4.4 Security. Verint shall implement and maintain the information security and data protection requirements described in Schedule D, to protect Customer Data that is retained within the Hosted Environment. Verint shall review its security precautions on a regular basis and may modify them as required by legal, regulatory, and other requirements, provided such modification shall not reduce the level of protection of Customer Data as specified in Schedule D.

5 CUSTOMER DATA.

5.1 Ownership, Use and Disclosure. Verint acknowledges it receives no ownership or, except to the extent specified herein, other rights in any Customer Data, and all rights, title and interest in such Customer Data remain with Customer. Verint shall not, and shall not permit its Personnel to use or disclose Customer Data, unless authorised by the terms and conditions of this Agreement, by the Customer in writing, or if Verint is required to do so by law or court order. Customer agrees that Verint may: **(a)** use and disclose in aggregate, anonymous and de-identified form, information derived from Customer Data where the resulting information does not in any way identify or allow the identification of Customer or any Personal Data, and/or **(b)** access, use in accordance with the terms and conditions of this Agreement, but not otherwise use or disclose Customer Data for Verint's internal business purposes, including for purposes of planning, support, administration and invoicing related to Customer's use of the SaaS Services, and improving or creating enhancements to or new offerings related to the SaaS Services. For the avoidance of doubt, nothing in this clause 5.1 shall operate to permit Verint to use, disclose or transfer data for any purpose that is not necessary for the use of Verint's cloud-based services.

5.2 Privacy Laws. In addition to all other obligations in this Agreement with respect to Customer Data, each party agrees to comply with its obligations under Privacy Laws, and in the context of any Processing of Personal Data through the provision of the SaaS Services, support and/or Professional Services, the parties shall comply with Schedule E. Customer hereby consents to Verint, its Affiliates, and Personnel of each, Processing Personal Data in

relation to Customer's Personnel and contacting the same for legitimate purposes, including without limitation, the administrative functions connected with Orders and invoices, its contractual rights and obligations under this Agreement, the provision of the SaaS Services, support and/or Professional Services. Customer understands and acknowledges that in connection with the Processing of Personal Data pursuant to this Agreement, Verint may share Personal Data with its Affiliates, and its Personnel, and Verint and/or its Affiliates may Process such Personal Data in any jurisdiction in which Verint or its Affiliates or subcontractors maintain facilities.

6 CUSTOMER RESPONSIBILITIES.

6.1 Passwords. All access codes and passwords are personal to the individual to which it is issued. Customer and its Personnel are responsible for maintaining the confidentiality and security of all access codes and passwords issued, and ensuring that each access code and password is only used by the individual authorised. To the extent Verint assigned Customer with administrative rights to create access codes and passwords for its Personnel, Customer shall be responsible for issuing such passwords.

6.2 Customer Data and Use of SaaS Services.

6.2.1 Customer Data. Customer agrees that Customer is solely responsible for: **(i)** obtaining any Customer Data and other information Customer provides while using the SaaS Services, **(ii)** obtaining all rights and consents necessary to collect, retain, use and/or disclose the Customer Data, **(iii)** ensuring the Processing, collection, retention and other processing of Personal Data in connection with the use and delivery of the SaaS Services does not violate the rights of Data Subjects or the Privacy Laws, and **(iv)** the accuracy, completeness, quality, integrity, legality, reliability, appropriateness and copyright of all Customer Data. By providing any Customer Data or other information, Customer acknowledges and agrees that such information does not **(x)** violate any Intellectual Property Rights, publicity rights, or any other legal rights; **(y)** violate any law, rule, order, judgment or regulation to which Customer or the Customer Data may be subject; and **(z)** violate Section 6.2.2 below. Customer acknowledges and agrees that Verint is not responsible or liable for any unlawful, harassing, defamatory, privacy invasive, abusive, threatening, offensive, harmful, vulgar, obscene, tortuous, hateful, racially, ethnically or otherwise objectionable information, or content, or information or content that infringes or may infringe any copyright, patent, moral right, trade secret, confidential information, trademark right or any other right of a third party.

6.2.2 Use of SaaS Services. Customer shall be solely responsible for the **(a)** actions of its Personnel while using the SaaS Services and **(b)** uploading, entry or processing of Customer Data and transmissions to or through the SaaS Services, and any resulting Fees. Customer agrees to: **(i)** abide by all local, state, national, and international laws and regulations applicable to Customer's use of the SaaS Services, including without limitation all applicable laws and administrative regulations relating to the control of exports of commodities and technical information and/or Personal Data and shall not allow any of its Personnel to access or use the SaaS Service in violation of any export embargo, sanction, prohibition or restriction, including but not limited to any party on a U.S. or any other applicable government restricted party list; **(ii)** provide any required notifications to Data Subjects, and obtain all rights and requisite consents from Data Subjects in accordance with all applicable Privacy Laws and other relevant laws in relation to the collection, use, disclosure, creation and processing of Personal Data in connection with this Agreement and the use of the SaaS Services; **(iii)** not use the SaaS Services for illegal purposes; **(iv)** not knowingly upload or distribute in any way files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of the Hosted Environment or SaaS Services; **(v)** not knowingly interfere with another customer's use and enjoyment of the Hosted Environment, SaaS Services or another entity's use and enjoyment of similar services; **(vi)** not knowingly engage in or post or transmit "junk mail," "spam," "chain letters" or unsolicited mass distribution of email through or in any way using the SaaS Services; **(vii)** not interfere or disrupt networks connected to the Hosted Environment or SaaS Services; **(viii)** not, without lawful justification, post, promote or transmit through the SaaS Services any harassing, defamatory, privacy invasive, abusive, threatening, offensive, harmful, vulgar, obscene, tortuous, hateful, racially, ethnically or otherwise objectionable information or content of any kind or nature; and **(ix)** not transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability.

6.3 SaaS Services Restrictions. Except as otherwise specified in this Agreement, expressly permitted in writing by Verint, or otherwise cannot be precluded under mandatory applicable law, Customer shall not, and shall not permit any other party to:

a. Disassemble, decompile, decrypt, or reverse engineer, or in any way attempt to discover or reproduce source code for, any part of the SaaS Services or on-premise components; adapt, modify, or prepare derivative works based on any of the Verint Intellectual Property; or use any of the Verint Intellectual Property to create any computer program or other material that performs, replicates, or utilises the same or substantially similar functions as the SaaS Service;

b. Alter, remove, or suppress any copyright, confidentiality, or other proprietary notices, marks or any legends placed on, embedded or otherwise appearing in or on any Verint Intellectual Property; or fail to ensure that all such notices and legends appear on all full or partial copies of Verint Intellectual Property or any related material;

c. Sell, sublicence, lease, assign, delegate, transfer, distribute, encumber or otherwise transform any Verint Intellectual Property or any of the rights or obligations granted to or imposed on Customer hereunder.

7 PROFESSIONAL SERVICES.

7.1 Professional Services. Any Professional Services provided hereunder are subject to Customer's performance of its obligations herein, and in accordance with a mutually agreeable implementation plan. Customer shall provide all necessary information, access, workspace, computing resources, and other services and support materials as reasonably required by Verint to perform its duties in a timely manner, including, without limitation, establishing the Customer Environment. Any development (other than Updates) will only be by written agreement. Verint shall at all times own all Intellectual Property Rights in and to any such development, and such development shall become part of the SaaS Services for the purposes of this Agreement. All Professional Services provided on a time and material basis are per person unless otherwise specified, and charged hourly or daily as indicated for each person. Professional Services shall be priced using the Rate Card in Schedule F which may be updated upon notice from Verint.

7.2 Scheduling Professional Services. Customer shall request scheduling for Professional Services ordered hereunder with reasonable notice. Verint shall use reasonable efforts to meet the requested time schedule; provided, all scheduling is dependent upon the allocation and availability of resources. In the event Customer reschedules or cancels scheduled Professional Services, Verint may, to the extent Verint cannot reschedule its applicable resources, charge to Customer a rescheduling or cancellation fee.

8 FEES AND PAYMENTS.

8.1 Fees and Expenses. Upon Verint's receipt and acceptance of an Order, Verint shall invoice Customer one hundred percent (100%) of the Fees for the initial Billing Period, and any fixed fee Professional Service Fees applicable to such Order. Fees for Overage shall be calculated monthly pro rata based on Verint's then current list price; unless, within thirty (30) days of Verint reporting such Overage to Customer, Customer places an add-on Order for additional SaaS Access Rights equal to at least the Overage quantity reported, with the Access Term starting the first day of the prior month and continuing for the remainder of the current Access Term. In such instance, the SaaS Access Fees for such Overage shall instead be calculated based on the Fees in most recent Order for the SaaS Service in relation to which the Overage applies. Verint may invoice Customer in advance for each subsequent Billing Period, including with respect to any renewal Access Terms, Overages in arrears on a quarterly basis, and for all other fees, assessments and expenses provided for under this Agreement as performed and/or incurred. Unless otherwise agreed, Verint will submit invoices electronically to [redacted] Customer shall pay all Fees and other amounts due to Verint hereunder within thirty (30) days after the date of Verint's invoice and without deductions, except with respect to any amount disputed in good faith where prior notice is provided to Verint detailing the amount and reason for the dispute. The parties will immediately negotiate in good faith to resolve any dispute.

8.2 Late Payment; Non-Payment; Collections. Time is of the essence in all payment terms. Any undisputed amounts not paid to Verint when due shall bear interest at the rate from day to day equal to three (3) percentage points above the base rate of National Westminster Bank PLC, before and after judgement. Customer shall reimburse Verint for all costs of collection, including reasonable attorneys' fees. This Section is without prejudice to any other rights and remedies available to Verint under this Agreement or at law.

8.3 **Taxes, Assessments and Other Charges.** All amounts due to Verint hereunder are net amounts, exclusive of, and Customer is responsible for paying, all duties, sales, use or value added taxes, customs duties, GST, tariffs, or other similar taxes, assessments, or excises, however designated or levied, (except for taxes on Verint's net income), whether payable directly by or indirectly through Verint in compliance with applicable law, and except as specified in Section 8.1, no reduction, deduction or off-set may be made by Customer for any reason whatsoever.

9 WARRANTIES; DISCLAIMER.

9.1 **Limited Performance Warranty.** Verint warrants to Customer that during any Access Term, the SaaS Services will perform substantially in accordance with the Documentation. Customer's exclusive remedy under this Section shall be for Verint to use commercially reasonable efforts to correct any Errors; provided, in the event Verint is unable to correct that nonconformity, Customer shall have the right to terminate the remaining Access Term and receive a pro rata refund of any remaining prepaid SaaS Access Fees applicable to those SaaS Services.

9.2 **Disclaimer of Warranties.** THE LIMITED WARRANTY AND EXCLUSIVE REMEDY SET FORTH IN SECTION 9.1 ARE MADE FOR THE BENEFIT OF CUSTOMER ONLY, AND ARE EXPRESSLY SUBJECT TO CUSTOMER'S PAYMENT OBLIGATIONS TO VERINT AND CUSTOMER'S OBLIGATIONS TO MAINTAIN ITS CUSTOMER ENVIRONMENT. VERINT MAKES NO AND EXCLUDES ALL OTHER WARRANTIES, REPRESENTATIONS, CONDITIONS AND OTHER TERMS, WRITTEN OR ORAL, OR EXPRESS, IMPLIED, STATUTORY, COLLATERAL OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, INTEROPERABILITY, DATA ACCURACY, OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO ANY PRODUCT, SERVICES, SUPPORT, OR ANY COMPONENTS THEREOF. WITHOUT LIMITING THE FOREGOING, VERINT DOES NOT WARRANT THAT ALL ERRORS CAN BE CORRECTED, OR THAT OPERATION OF THE SAAS SERVICE SHALL BE UNINTERRUPTED OR ERROR-FREE.

10 LIMITATION OF LIABILITY.

10.1 **Cap on Liability; Exclusions.** EACH PARTY'S MAXIMUM LIABILITY ARISING OUT OF OR IN ANY WAY CONNECTED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STATUTORY OR OTHERWISE, SHALL BE EXPRESSLY LIMITED AS FOLLOWS:

A. IN NO EVENT SHALL EITHER PARTY OR ANY OF THEIR EMPLOYEES OR AGENTS HAVE ANY LIABILITY FOR ANY OF THE FOLLOWING LOSSES OR DAMAGE (WHETHER SUCH LOSSES OR DAMAGE WERE FORESEEN, FORESEEABLE, KNOWN OR OTHERWISE):

(I) LOSS OF REVENUE;
(II) LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING FOR LOSS OF PROFITS ON CONTRACTS);
(III) LOSS OF THE USE OF MONEY;
(IV) LOSS OF ANTICIPATED SAVINGS;
(V) LOSS OF BUSINESS;
(VI) LOSS OF OPPORTUNITY;
(VII) LOSS OF GOODWILL;
(VIII) LOSS OF REPUTATION;
(IX) EXCEPT AS PROVIDED IN SECTION 4.3.2, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA;
(X) WASTED EXPENDITURE;
(XI) EXCEPT AS PROVIDED IN SECTION 10.1C., COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES;
(XII) ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE HOWSOEVER CAUSED (INCLUDING, FOR THE AVOIDANCE OF DOUBT, WHERE SUCH LOSS OR DAMAGE IS OF THE TYPE SPECIFIED IN (I) - (XI) ABOVE);

B. EXCEPT AS EXPRESSLY SET OUT AT SECTION 4.3.2, VERINT SHALL NOT BE RESPONSIBLE OR LIABLE FOR RECOVERY OF ANY DATA, AND CUSTOMER ACKNOWLEDGES THAT CUSTOMER IS RESPONSIBLE FOR ANY AND ALL DATA, DATA BACKUP, AND DATA RECOVERY;

C. WHERE THIS AGREEMENT IS TERMINATED BY CUSTOMER AS PROVIDED FOR UNDER SECTION 9.1 OR VERINT AS PROVIDED FOR UNDER SECTION 12.1, THEN SUBJECT TO THE LIABILITY PROVISION ABOVE AND SECTION 10.1D BELOW AND WITHOUT PREJUDICE TO CUSTOMER'S OTHER RIGHTS IN CONTRACT OR LAW, VERINT SHALL BE LIABLE TO THE CUSTOMER FOR THE DIRECT ADMINISTRATIVE COSTS OF PROCURING A COMPARABLE REPLACEMENT SOLUTION TO THE SAAS SERVICES TERMINATED . THE COSTS OF THE OPERATION OF ANY SUCH REPLACEMENT SOLUTION SHALL NOT BE MET BY VERINT. WHERE THIS CLAUSE 10.1C APPLIES, VERINT SHALL, AT ITS OWN EXPENSE, UNDERTAKE THE ACTIONS AGREED UNDER CLAUSE 13.3D (EXIT PLAN AND HANDOVER), OR SUCH OTHER ACTIONS AGREED BETWEEN THE PARTIES, ACTING REASONABLY, TO FACILITATE HANDOVER AND CONTINUITY OF SERVICE.

D. SUBJECT TO CLAUSE 10.1E, NEITHER PARTY SHALL BE LIABLE FOR ANY OTHER LOSSES IN AN AMOUNT EXCEEDING THE GREATER OF (I) **£225,000** OR (II) **125%** OF THE FEES PAID AND/OR PAYABLE HEREUNDER DURING THE TWELVE (12) MONTHS PRECEDING THE DATE UPON WHICH THE LIABILITY AROSE;

E. SUBJECT TO THE EXCLUSIONS OF LIABILITY SET OUT IN SECTION 10.1(A), THE AGGREGATE LIABILITY OF VERINT UNDER THIS AGREEMENT FOR ALL LOSSES INCURRED BY CUSTOMER AS A RESULT OF VERINT BREACHING ITS OBLIGATIONS UNDER SCHEDULE D (INFORMATION SECURITY SCHEDULE) OR SCHEDULE E (DATA PROCESSING SCHEDULE) DIRECTLY CAUSING A PERSONAL DATA BREACH SHALL BE LIMITED TO THE GREATER OF (I) 300% OF THE FEES PAID HEREUNDER FOR THE RELEVANT SAAS SERVICES DURING THE TWELVE (12) MONTHS PRECEDING THE DATE UPON WHICH THE DAMAGES CLAIM OR SERIES OF CLAIMS AROSE OR (II) TWO MILLION POUNDS (£2,000,000).

D. VERINT SHALL NOT BE LIABLE TO ANY PERSON NOT A PARTY TO THIS AGREEMENT, WHETHER STATUTORY (INCLUDING, WITHOUT LIMITATION, ANY ACTS, DIRECTIVES, RULES OR REGULATIONS RELATING TO THE PROTECTION OF PERSONAL DATA), COMMON LAW, OR OTHERWISE. SUBJECT TO THE LIMITATIONS AND EXCLUSIONS OF LIABILITY HEREUNDER, LOSSES OF AFFILIATES OF CUSTOMER SHALL BE DEEMED TO BE LOSSES OF THE CUSTOMER AND AS SUCH MAY BE CLAIMED BY CUSTOMER, AND AFFILIATES SHALL NOT BE ENTITLED TO SEPARATELY BRING A CLAIM AGAINST VERINT.

IN NO EVENT SHALL ANY PARENT, SUBSIDIARY, AFFILIATE OR LICENSOR OF VERINT, OR ANY OF THEIR OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, OR REPRESENTATIVES THERETO (COLLECTIVELY "OTHER PARTIES"), BE LIABLE TO CUSTOMER OR ANY OTHER PERSON FOR DAMAGES OF ANY KIND OR NATURE OR IN ANY MANNER WHATSOEVER; PROVIDED IF SUCH LIABILITY ARISES AND IS NON-EXCLUDABLE AS A MATTER OF LAW, SUCH OTHER PARTIES SHALL HAVE THE BENEFIT OF THE OTHER LIMITATIONS ON LIABILITY SPECIFIED IN THIS SECTION 10. THIS SECTION 10 SHALL SURVIVE AND CONTINUE IN FULL FORCE AND EFFECT DESPITE ANY FAILURE OF ESSENTIAL PURPOSE, CONSIDERATION, OR OF AN EXCLUSIVE REMEDY.

BOTH PARTIER SHALL BE UNDER AN OBLIGATION TO MITIGATE THEIR LOSSES.

10.2 **Non-Excluded Liability.** NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT LIABILITY FOR: (I) A PARTY'S INDEMNIFICATION OBLIGATION IN SECTION 12, (II) PERSONAL INJURY OR DEATH CAUSED BY NEGLIGENCE OR WILFUL MISCONDUCT, (III) FRAUD, OR (IV) A BREACH OF OBLIGATIONS WITH RESPECT TO VERINT INTELLECTUAL PROPERTY .

11 CONFIDENTIALITY.

The unauthorised disclosure or use of Confidential Information of a disclosing party or of a disclosing party's third party licensors, and all information and services related thereto, would cause great injury and harm to the owner thereof. Therefore, each party agrees to take all appropriate action to ensure the confidentiality and security of the other party's Confidential Information, but in any event no less than the same standard of care it uses to protect its own Confidential Information of like kind and value. Without limiting the generality of the foregoing, Customer and Verint each agree that it: **(i)** shall maintain the other's Confidential Information in the strictest confidence, including compliance with reasonable remote access security requirements; **(ii)** shall not disclose, display, publish, transmit, or otherwise make available such Confidential Information or take the benefit thereof, in whole or in part, except in confidence to its own Personnel on a need-to-know basis; and **(iii)** except as expressly permitted hereunder, shall not copy, duplicate, replicate, transform, or reproduce such Confidential Information. Notwithstanding anything to the contrary in this Section, neither party shall be liable to the other for damages resulting from disclosure of any Confidential Information required by law, regulation or valid court order; provided, to the extent legally permitted, prior written notice is provided to the other party sufficiently in advance of such required disclosure to allow the other party to respond and take reasonable and lawful action to avoid and/or minimise the degree of such disclosure or seek appropriate protective orders.

12 INDEMNIFICATION.

12.1 **Verint Indemnity.** Verint, at its sole expense, shall defend, indemnify and hold harmless Customer from any action based upon a claim that the SaaS Service used as permitted infringes any valid and enforceable third-party patent, copyright, trade secret, or other proprietary right, and shall reimburse Customer for all damages, costs, and expenses (including reasonable attorneys' fees) awarded against Customer pursuant to any such actions. If the SaaS Service becomes, or in Verint's opinion is likely to become, subject of such a claim of infringement, Verint shall be entitled, at Verint's sole option, to either procure the right for Customer to continue to use the SaaS Service, or replace or modify it so that it becomes non-infringing. If neither of the foregoing is commercially and reasonably available to Verint, Verint may terminate the SaaS Service and refund to Customer a pro rata refund of any remaining prepaid SaaS Access Fees applicable to those SaaS

Services. Verint shall have no obligation or liability hereunder for any claim resulting from: **(i)** modification of the SaaS Service **(a)** by any party other than Verint, or **(b)** by Verint in accordance with Customer's designs, specifications, or instructions; **(ii)** use of the SaaS Service other than as granted in this Agreement; or **(iii)** use of the SaaS Service in conjunction with other products or services not provided by Verint or necessary for the operation of the SaaS Service, where such infringement would not have occurred but for such use; or **(iv)** use of a version of the SaaS Service other than the then-current version where Customer has requested the prior version remain in use.

12.2 Customer Indemnity. Customer, at its sole expense, shall defend, indemnify and hold harmless Verint from any action based upon a claim resulting from breach of Section 6.2 by Customer, its Affiliates or Personnel of either, and shall reimburse Verint for all damages, costs, and expenses (including reasonable attorneys' fees) awarded against Verint pursuant to any such actions.

12.3 Conditions. Each party's indemnification obligations hereunder are contingent upon the indemnified party providing the indemnifying party with **(i)** prompt written notice of the claim; **(ii)** an opportunity for complete control of the defence of and the right to settle such claim; and **(iii)** all available information, assistance, authority, and cooperation to enable the defence or settlement of such claim. This Section sets forth the exclusive remedy of the indemnified party against the indemnifying party, and the complete liability of indemnifying party with respect to any action or claim indemnified hereunder.

13 TERMINATION.

13.1 Service Suspension. In the event Customer **(i)** fails to pay Verint any undisputed amounts past due where Verint has given Customer written notice of breach of Section 8.1 and Customer has failed to cure such breach within 5 working days, or **(ii)** is in breach of Section 6.2, Verint shall have the right to immediately suspend without notice the SaaS Services and any Professional Services provided to Customer hereunder until remediation.

13.2 Agreement Termination. This Agreement may be terminated as follows:

a. By Verint immediately if Customer breaches Sections 6.2, 6.3 or 11; or

b. By either party for material breach hereof which has not been cured within thirty (30) days after written notice of such breach; or

c. By either party at any time if the other party makes an assignment for the benefit of creditors, or commences or has commenced against it any proceeding in bankruptcy or insolvency.

13.3 Effects of Termination.

a. Termination of Agreement. Upon termination of this Agreement, and except to the extent specified herein, **(i)** all fees due to Verint for the current Access Term and any other amounts due Verint shall be immediately paid, and **(ii)** all Customer rights to access and use any of the SaaS Services and to have any on-premise components installed shall immediately terminate without right of refund and Customer shall delete, or if requested by Verint, return all Verint Intellectual Property in its possession.

b. Customer Data. Within thirty (30) days of termination of this Agreement or non-renewal of the relevant SaaS Service (the "**Return Period**") and subject to Customer's compliance with Section 13.3(a)(i), Customer may request in writing that Verint either delete or return available Customer Data with respect to the terminated SaaS Service(s). At the expiry of the Return Period, if Customer has not elected either of the foregoing Verint may delete and destroy all such Customer Data without notice or liability to Customer. Where Customer requests Verint return available Customer Data, Verint may fulfil this request by making available functionality that enables Customer to retrieve the Customer 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 Customer Data under an Order for the applicable Professional Services. Verint agrees to provide such Professional Services at its then current rates, provided that in the event this 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 13.3(b) within thirty (30) days of Customer's request for such confirmation.

c. Survival. Provisions herein which by their context and content are intended to survive termination or expiration hereof shall so survive, including the Signature Page, Schedule A, Sections 1.2, 5, 6, 8, 9.2, 10, 11, 12, 13.3, 14, and 15 of Schedule B, Schedule D, and Schedule E.

d. **Exit Plan and Handover.** Verint shall at the request of the Customer provide an exit plan in relation to the SaaS Services. The exit plan must be reviewed and, if necessary, updated by Verint on each the anniversary of the Agreement and/or where there are any material changes to the SaaS Services provided by Verint. Customer may request changes to the exit plan. The Parties will mutually agree any changes to the Exit Plan, acting reasonably. Verint shall, at the request of the Customer assist the Customer with the migration of the services in line with exit plan subject to any additional Fees agreed between the Parties. The exit plan must include full details of: (i) the process for exportation or transferring the Customer's data from Verint's systems to any replacement supplier;; and (ii) any other activities reasonably required to ensure continuity of service, including details of the timescale, actions, and responsible personnel to the extent within the knowledge and control of Verint. For the avoidance of doubt, the production of an Exit Plan shall be at no charge to the Customer.

14 GOVERNING LAW.

14.1 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of England and Wales, and shall be subject to the jurisdiction of the English courts. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply in any respect to this Agreement or the parties.

14.2 Remedies. Customer acknowledges that each provision providing for ownership and/or protection of Verint Intellectual Property is material to this Agreement, and that any threatened or actual breach thereof shall constitute immediate, irreparable harm to Verint. If Customer breaches or threatens to breach any such provision, in addition to any other remedies Verint may have, Verint shall be entitled to seek injunctive, equitable, or other equivalent relief against such breach directly from any court of competent jurisdiction, without the requirement to post bond or other security. Customer agrees to cooperate with Verint, and to obtain all required consents, in the event a third party seeks to compel Verint to disclose Customer Data through any legal process. To the extent legally permitted, Verint shall provide Customer with advance notice to allow Customer to take reasonable and lawful action to minimise the degree of such disclosure or to seek appropriate protective orders. Verint shall be entitled to charge Customer for all costs and expenses (including reasonable attorney fees) incurred complying with or defending against such legal process, and on a time and material basis for any work performed to produce such Customer Data. Verint may also, to the extent legally compelled, remove any violating content posted on the SaaS Services or transmitted through the SaaS Services. Notwithstanding any other terms in this Agreement, Verint shall not be liable to any person for any damages or losses resulting from any disclosure of Customer Data under such legal process.

15 GENERAL PROVISIONS.

15.1 Consent. Wherever in this Agreement consensus, approval, acceptance, or other consent is required, such consent shall not be unreasonably withheld, conditioned, or delayed; however, it shall not be considered unreasonable for Verint to withhold its consent if such consent could jeopardise the confidentiality of or Verint's property interests in and to Verint Intellectual Property or other business interests of Verint.

15.2 Assignment. Neither this Agreement nor any rights granted hereunder may be sold, leased, assigned, or otherwise transferred, in whole or in part, by Customer, and any such attempted assignment shall be void and of no effect without the advance written consent of Verint. Notwithstanding the foregoing, **(a)** such consent shall not be required if Customer assigns this Agreement to an Affiliate or in connection with a merger, or sale of all its stock or all or substantially all of its assets; provided, **(i)** the Affiliate or surviving entity is not a direct competitor of Verint, **(ii)** any such assignee has the financial and other abilities required to perform Customer's obligations and agrees to be bound in writing to Customer's obligations under this Agreement, and **(iii)** at the time of assignment, Customer is not in breach of this Agreement, and **(b)** Verint may assign this Agreement or any Order issued hereunder to any Verint Affiliate. In no event shall this Agreement, or any rights or privileges hereunder, be an asset of Customer under any bankruptcy, insolvency, or reorganisation proceedings, or in any other manner whatsoever; however, this Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, and permitted transferees, successors, and assigns.

15.3 Counterparts, Fax Signatures. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall be deemed for all purposes to constitute one and the same instrument. The parties hereby agree that hardcopy signatures transmitted and received via facsimile or other electronic means shall be treated as original signatures for all purposes of this Agreement.

Notwithstanding the foregoing, electronic mail without attachment evidencing the sending party's authorised signature shall not constitute a writing for the purpose of binding that party or amending this Agreement.

15.4 **Force Majeure.** Except for obligations of confidentiality, payment, and compliance with laws, neither party shall be liable for any delay or failure in performing hereunder if caused by any factor beyond the reasonable control of the party, including force of nature, war, riot, civil action, terrorism, labor dispute, malicious acts or denial of service by a third party, or failure of telecommunication systems or utilities ("Force Majeure Event"). A Force Majeure Event will not include: (i) industrial action/dispute about either Party, its staff or within either Party's supply chain; or (ii) an event that (a) was foreseeable on it at commencement of this Agreement by the Party seeking to rely on it, (b) is attributable to failure to comply with disaster recovery or business continuity arrangement of the Party wishing to rely on it, (c) is attributable to the negligence or failure of to take reasonable precautions of the Party wishing to rely on it.. Performance shall be deferred until such cause of delay is removed, provided that the delayed party promptly notified the other party after having actual knowledge of any such occurrence.

Notwithstanding the above, a Party my terminate this Agreement by notice if the other Party is affected by a Force Majeure Event that lasts for more than 60 consecutive days.

15.5 **Notices.** All notices or other communications required hereunder shall be made in writing and shall be deemed to be effectively given: **(i)** if made available to Customer's Personnel by Verint posting such notice to the SaaS Service and if emailed, the first business day after sending the notice (provided email shall not be sufficient for notices of termination, alleged breach or an indemnifiable claim); or **(ii)** if hand delivered, when received and if mailed for overnight delivery, when delivery by the overnight carrier is made, in each instance at the applicable address set forth on the Signature Page. Such addresses may be updated by a party from time to time by providing notice to the other party in accordance with the terms of this Section. Each party may change its notices address by giving notice in the manner set forth herein.

15.6 **Severability; Waiver.** If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the parties agree to negotiate in good faith an amendment to replace such invalid or unenforceable provision to cause them to be valid and enforceable; provided, if the parties are unable to agree on such amending terms, a court of competent jurisdiction or arbitrator (as applicable) shall so amend and restate such provision in light of the parties' apparent original intent. The invalidity or unenforceability of any provision shall not constitute a failure of consideration hereunder. Any failure or delay in exercising any right or remedy by either party shall not be deemed a waiver of any further, prior, or future right or remedy hereunder.

15.7 **Anti-corruption.** During the term of this Agreement, both parties are obligated to comply with the Bribery Act 2010 and desist from all practices which may lead to penal liability due to fraud or embezzlement, insolvency crimes, crimes in violation of competition, guaranteeing advantages, bribery, acceptance of bribes or other corruption crimes on the part of persons employed by the other party or other third parties. In the event of violation of the foregoing provisions, either party has the right to immediately withdraw from or terminate all legal transactions existing with the other party including this Agreement.

15.8 **Miscellaneous.** The official language of this Agreement is, and all attachments or amendments to this Agreement, contract interpretations, notices and dispute resolutions shall be in English. Translations of this Agreement shall not be construed as official or original versions. Headings are for convenience only and do not define, interpret or limit the scope of any provision hereof. In all cases, the use of "includes/ing" shall mean "includes/ing without limitation". References to a particular section within a schedule or other document expressly attached to the Signature Page shall serve to reference the applicable section within that schedule or document, unless otherwise specified therein. Nothing in this Agreement shall make either party the agent of the other for any purposes whatsoever. No exclusive rights are granted by Verint under this Agreement. All rights or licences not expressly granted to Customer herein are reserved to Verint, including the right to licence the use of the SaaS Services and any Software to other parties. The parties acknowledge that the SaaS Services may be subject to U.S. and other applicable foreign export controls. Any reference to a law or statute in this Agreement shall be deemed to include any amendment, replacement, re-enactment thereof for the time being in force and to include any by-laws, statutory instruments, rules, regulations, orders, notices, directions, consents, or permissions (together with any conditions attaching to any of the foregoing) made in respect thereof.

15.9 **Insurance**. Verint shall maintain: (i) professional indemnity insurance cover held by Verint, and any agent, subcontractor or consultant involved in the provision of the Software and all and any related services shall be covered under Verint's policy with a minimum limit of indemnity of £1,000,000 for each individual claim (or any other limit required by law or reasonably requested by the Customer); and (ii) employers' liability insurance with a limit of £5,000,000 (or such other limit required by law).

15.10 **Intellectual Property Rights**. Unless otherwise specified in this Agreement, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights of the other Party or its licensors.

15.11 **Information Sharing and Transparency**. Verint must tell the Customer within 48 hours of becoming aware if it receives a Request For Information in relation to the Customer.

In accordance with a reasonable timetable and in any event within 5 working days of a request from the Customer, Verint will provide reasonable assistance to give the Customer co-operating and providing relevant and necessary information, which the Customer cannot obtain without Verint's involvement, needed so the Customer can:

a) comply with any valid Freedom of Information Access request;

b) comply with any Environmental Information Regulations ("EIR") request in relation to the Services;

c) if the Agreement has a value over the relevant threshold in Part 2 of the Public Contracts Regulations 2015 (and/or the Public Contracts (Scotland) Regulations 2015, if the context requires)) as amended from time to time Regulations, comply with any of its obligations in relation to publishing Transparency Information.

For the purpose of this Section 19.11, "Transparency Information" includes the content of the Agreement, including any changes to this Agreement agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Agreement required to be published by the Customer to comply with its transparency obligations, including those set out in Public Procurement Policy Note 09/21 (update to legal and policy requirements to publish procurement information on Contracts Finder) and Public Procurement Policy Note 01/17 (update to transparency principles) where applicable except for: (i) any information which is exempt from disclosure in accordance with the provisions of the Freedom of Information Act, which shall be determined by the Customer; and (ii) Confidential Information. To the extent that it is allowed and practical to do so, the Customer will use reasonable endeavours to notify the Customer of any request in relation to this Section 15.11 and will consult with Verint to help it decide whether to publish information under Section 19.11.

15.12 **Business Continuity & Disaster Recovery**

a) Verint shall maintain a Business Continuity and Disaster Recovery Plan throughout the duration of the Access Term, a review of which can be provided to the Customer upon request. Verint shall implement the actions and the processes set out in its Business Continuity and Disaster Recovery Plan in the event of one or more relevant events which separately or cumulatively means that the SaaS Services, or a material part thereof becomes unavailable (or could reasonably be anticipated to be unavailable).

b) The Disaster Recovery and Business Continuity Plan shall be reviewed by Verint at least once per year.

c) Verint shall test the Disaster Recovery and Business Continuity Plan ("BCP") on a regular basis (and in any event, not less than once in every twelve (12) month period) unless the BCP is invoked in which case the 12 month schedule continues after normal operations are resumed.

15.13 **Modern Slavery.** Verint shall comply with all applicable anti-slavery and human trafficking laws, statutes, regulations from time to time in force including but not limited to the Modern Slavery Act 2015 and have and maintain throughout the term of this Agreement its own policies and procedures to ensure its compliance.

15.14 **Audit.** Customer and/or its authorized representative (who is not a competitor of Verint's) is entitled to assess or audit (either by webinar or face-to-face), directly or by a third party designated by the auditing party (who is not a competitor of Verint's), once per year, in order to verify the accuracy of the charges and any other amounts payable by the Customer under the Agreement by giving Verint not less than thirty (30) days prior written notice of its intention. The means of intervention and scope applicable to the above operations shall be defined jointly by Customer and Verint acting reasonably.

Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between the auditing party (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 a party in breach of its confidentiality obligations to other customers vendors and/or partners generally or otherwise cause it to breach laws applicable. Customer (or auditor mandated) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to the others premises, equipment, personnel and business in the course of such a review.

To the extent that such audit lasts longer than one business day Verint shall reserve the right to charge Customer such engagement at Verint's then current daily rates.

This does not prevent the National Audit Office carrying out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Customer has used its resources.

SCHEDULE C
SERVICE LEVELS

This Schedule C is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule C is attached. The calculation of Uptime and any Service Level Credits shall be calculated independently for each SaaS Service subscribed to by Customer. **THIS SCHEDULE C SHALL NOT APPLY TO ANY BETA, PILOT OR OTHER TRIAL SUBSCRIPTIONS, OR TO ANY NON-PRODUCTION ENVIRONMENTS, EACH OF WHICH ARE PROVIDED 'AS IS' AND WITHOUT WARRANTY OF ANY KIND.**

1 SERVICE AVAILABILITY.

1.1 Uptime. Verint will use commercially reasonable efforts to ensure that the Hosted Environment will be available 24 hours per day, 7 days per week, excluding any Scheduled Downtime. In addition to any other notification requirements, Verint will provide Customer with a minimum of seven (7) days advance notice of Scheduled Downtime, and Verint may post a notice on the application log-in screen to notify Customer administrator of any Scheduled Downtime that will exceed two (2) hours. The duration of any downtime is measured, in minutes, as the amount of elapsed time from when the Hosted Environment is not accessible or does not permit Customer to log on, to when the SaaS Services permits Customer to log on and access the Hosted Environment.

1.2 Service Level Credits. If Verint does not meet the Uptime Percentage levels specified below, Customer will be entitled, upon written request, to a service level credit ("**Service Level Credit**") to be calculated, with respect to the applicable Hosted Environment, as follows:

- If Uptime Percentage is at least 99.99% of the month's minutes, no Service Level Credits are provided; or

[redacted]

Customer shall only be eligible to request Service Level Credits if it notifies Verint in writing within thirty (30) days from the end of the month for which Service Level Credits are due. All claims will be verified against Verint's system records. In the event after such notification Verint determines that Service Level Credits are not due, or that different Service Level Credits are due, Verint shall notify Customer in writing on that finding. With respect to any Services Level credits due under Orders placed directly by Customer on Verint, Service Level Credits will be applied to the next invoice following Customer's request and Verint's confirmation of available credits; with respect to any Service Level Credits due for SaaS Services under Orders placed on Verint by a Verint authorised reseller on Customer's behalf, Service Level Credits will be issued by such reseller following Customer's request and Verint's confirmation of available credits and such Services Level Credits may only be used by Customer with respect to subsequent purchases of Verint offerings through that reseller. Service Level Credits shall be Customer's sole and exclusive remedy in the event of any failure to meet the Service Levels. Verint will only provide records of system availability in response to good faith Customer claims.

1.3 Exceptions. Customer's right to receive Service Level Credits, and the inclusion of any minutes in the calculation of Unscheduled Downtime are conditioned on: **(i)** prompt payment by Customer of all Fees, **(ii)** Customer performing all Customer obligations (including, without limitation, establishing and maintaining the Customer Environment), **(iii)** Customer's compliance with Section 6.2 of Schedule B, **(iv)** Customer agreeing to use of the most current version of the SaaS Service, and **(v)** the Unscheduled Downtime not being caused by the failure of any non-Verint third party vendors, the Internet in general, any emergency or force majeure event, or issues caused by the Customer Environment or Customer specific configurations not expressly contemplated in the Documentation.

2 SUPPORT.

2.1 Generally for SaaS Services. During any Access Term, Customer Designated Employees shall have access to Verint technical support Personnel through Verint's standard telephone, and/or web support services during the support hours applicable to the specific SaaS Services subscribed to by Customer. The contact information for Verint technical support Personnel, support hours applicable to the SaaS Services, and Error type classifications and response times can be found at [redacted]

2.2 On-Premise Components. With respect to any on-premise components, except as specified in an Order, Customer shall be responsible for the installation and configuration of the on-premise components in the Customer Environment. Verint shall provide technical support for such on-premise components through Verint's standard telephone, email and/or web support services during the support hours specified in the Maintenance and Support Plan under the Premium Plan found at [redacted]

2.3 Support Hours. "Standard Support Hours" are 8.00 am to 6pm (UK time) Monday to Friday excluding UK public holidays.

During any applicable holiday, the Customer may log an incident by telephone and Verint shall continue to investigate a Severity 1 or 2 incident during a holiday.

Extended Support Hours will be 24 hours a day, 365 days per calendar year and include Standard Support Hours. Extended Support Hours are available for Severity 1 and Severity 2 Errors only when Errors are logged by telephone only. Verint Support are able to provide cover for Severity 3 issues between 08:00-18:00 Monday to Friday (excl Verint holidays). All incidents should be logged via the Phone or Online Portal.

The geographic number for UK support is [redacted]

2.4 Progress Review Meetings. Verint shall attend service review and progress meetings with the Customer throughout the term of the Contract. The frequency of the service progress review meetings shall be mutually agreed between the Parties but in the ordinary course of business shall be no more frequent than monthly. Service review and progress meetings may be attended by the Parties virtually.

SCHEDULE D
INFORMATION SECURITY SCHEDULE

This Schedule D is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule D is attached.

1 DEFINITIONS. In addition to the capitalised terms in Schedule A, all capitalised terms shall have the meaning ascribed to them herein this Schedule, and for the purposes of this Schedule, shall govern and control in the event of any conflict, including the following:

1.1 Encryption Standards. Encryption algorithms that are publicly or commercially available, with key lengths sufficient to prevent commercially reasonable attempts to decrypt through brute force the encrypted information.

1.2 Hosted Services. Any SaaS Services or hosting services subscribed to by Customer from Verint.

1.3 Industry Standard(s). Generally accepted standards applicable to the performance obligations of a party with respect to a product or service. Industry Standards can include in part or in whole frameworks published by the National Institutes for Standards and Technology (NIST), International Organisation for Standardisation, ISACA, Payment Card Industry Security Standards Council and other internationally recognised standards organisations.

1.4 Verint Personnel. Each Verint employee or subcontractor under obligations of confidentiality and nondisclosure which performs on behalf of Verint hereunder.

2 GENERAL SECURITY TERMS. Verint is committed to helping protect the security of Customer Data, and has implemented, and will maintain and follow appropriate technical and organisational measures that conform to Industry Standards intended to protect Customer Data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. Verint may modify any of its policies, process or procedures at any time and without obligation to notify or update this Schedule, provided such modifications provide substantially similar or greater protections than those provided for herein. Except as otherwise specified in Section 3, the following terms and conditions in this Section 2 apply to all performance obligations under the Agreement.

2.1 Access Controls. Verint implements Industry Standard access control methodologies, which rely on policy, process, and logical controls to help prevent unauthorised access to systems and data under Verint's control. These access controls include no less than the following:

- Verint uses the "Principle of Least Privilege" model for restricting access to systems and data, and regularly reviews access rights granted to Verint Personnel.
- Verint Personnel each have a unique user ID and personal secret password for accessing internal networks, equipment and data. Verint shall maintain policies concerning the maintenance of password secrecy. Verint Personnel access rights must be suspended within twenty-four (24) hours of employment termination, and modified within forty-eight (48) hours when Verint Personnel roles and/or responsibilities are changed.
- Verint maintains a password policy which, at a minimum, complies with the following standards: **(i)** passwords must not employ any structure or characteristic that results in a password that is predictable or easily guessed; **(ii)** passwords must include at least three (3) of the following character sets, in accordance with password policy settings: **(a)** an English uppercase character (A – Z); **(b)** an English lowercase character (a – z); **(c)** a westernised Arabic numeral; and **(d)** a non-alphanumeric special character from the following character set: !, $, #, %; **(iii)** passwords must be changed at least every one hundred and eighty (180) days; and **(iv)** account lockout must occur after a maximum of five (5) failed password entry attempts. Re-enabling of locked accounts must require extended time based delay, or interaction with a security administrator or help desk function. All password changes must be accomplished through secure procedures.
- Multi-factor authentication processes must be utilised for any access to systems containing Customer Data. All passwords must be stored and transmitted using Encryption Standards.
- User sessions must expire and require the re-entry of a password if idle by more than **(i)** twenty (20) minutes for administrator consoles, and **(ii)** sixty (60) minutes for all other systems and session types.
- For any facilities hosting Customer Data, such facilities shall have implemented electronic access controls to enter such facilities, and further access controls for entering specific areas where such Customer Data is physically resident. Verint shall maintain processes to validate the identity of individuals prior to issuing identification and access badges, and shall maintain processes for issuing visitor badges, logging such issuance, and escort requirements for such visitors. Such logs shall be maintained by Verint for no less than six (6) months from issuance.

2.2 Data Controls. In its performance obligations, Verint does not require access to Customer systems or data, and Customer shall take commercially reasonable efforts to prevent Verint from accessing Customer systems and data. Where Customer provides Customer Data to Verint for Professional Services or Support purposes, Customer shall take commercially reasonable efforts to redact or remove Personal Data prior to providing that Customer Data to Verint. Where possible, such services shall be delivered via screen share or telephone with no data transferred to Verint. If it is necessary to transfer Customer Data to Verint, the following shall apply:

- Customer shall only use Verint approved communication channels for providing Customer Data to Verint. With respect to the storage of such Customer Data by Verint and any further transmission of that Customer Data by Verint, Verint shall ensure such Customer Data is protected using Encryption Standards.
- In the event Verint makes backups of such Customer Data, all backups of Customer Data shall be encrypted on backup media using Encryption Standards.
- Customer Data may only be stored on portable media, including laptops, DVD, CD, magnetic tape media, removable hard drives, USB drives or similar portable storage, if Encryption Standards are used on that portable media.

2.3 Operational Controls. Verint shall maintain operational controls sufficient to enable Verint's satisfaction of its performance obligations in this Section 2, including, without limitation, the following:

- Maintain a dedicated information security function to design, maintain and operate security in line with Industry Standards. This function shall focus on system integrity, risk acceptance, risk analysis and assessment, risk evaluation, and risk management.
- Maintain a written information security policy that is approved by the Verint management team and published and communicated to all Verint Personnel and relevant third parties.
- Provide security awareness training at least annually to its employees, and maintain records of training attendance for no less than one (1) year.
- Conduct vulnerability assessments and/or penetration tests of networks, systems, applications and databases where Customer Data is located at rest, in transit and in use. Verint shall triage identified vulnerabilities and remediate or mitigate vulnerabilities in accordance with Industry Standards.
- Maintain appropriate authentication system(s) to authenticate and restrict access to Verint systems and networks to valid users.
- Install and maintain antivirus software on all servers and computing devices involved with Processing activities and use other malware detection techniques where reasonably required. Such antivirus software shall be updated on a daily basis, or as otherwise provided by the antivirus software manufacturer.
- Maintain physical security measures with respect to Verint facilities to help prevent and detect physical compromise, including, without limitation, use of identification badges, smart card or other electronic or physical identity verification systems, alarms on external doors, and CCTV on all entrances / exits to such facilities. Verint shall periodically review access records and CCTV video to ensure access controls are

being enforced effectively, with any discrepancies or unauthorised access investigated immediately.

- With respect to Verint internal networks, ensure perimeter networks are physically or logically separated from internal networks containing Customer Data, establish and configure firewalls in accordance with Industry Standards, use network intrusion detection systems as a part of network security, and restrict and control remote network access.
- Complete diligent review of any Verint subcontractors that will have access to Customer Data, and require such subcontractors contractually commit to substantially similar terms and conditions as those specified in this Schedule, or terms and conditions that Verint reasonably determines as providing substantially similar protection. With respect to any performance subcontracted by Verint, Verint remains responsible for its subcontractors' compliance with Verint's performance obligations in the Agreement.

2.4 Availability Controls. Verint will maintain contingency planning policies and procedures defining roles and responsibilities on proper handling of contingency events. This shall include a business continuity and disaster recovery plan intended to facilitate the restoration of critical operations and processes which would allow for Verint's continued performance of its obligations hereunder. Such plan shall be periodically reviewed, updated and tested by Verint.

2.5 Application Controls. Verint shall implement and conform its software development practices to applicable Industry Standards relative to the functionality to be performed by the specific Verint product offering. Verint shall maintain software development practices which satisfy the following:

- Use commercially reasonable measures to detect product vulnerabilities prior to release. These measures may include manual test scripts, test automation, dynamic code analysis, static code analysis, penetration testing, or other measures chosen by Verint. Verint shall update procedures and processes from time to time to improve detection of vulnerabilities within its products.
- Verint's developers shall not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any systems or network.
- Verint's developers shall receive regular training on coding and design with respect to application security.

3 SAAS AND HOSTING SECURITY TERMS. In addition to the terms and conditions in Section 2, the following terms and conditions shall apply to Verint's performance obligations with respect to any Hosted Services procured by Customer under this Agreement. To the extent of any conflict between the terms and conditions in this Section 3 and in Section 2, the terms and conditions in this Section 3 shall control solely with respect to Hosted Services.

3.1 Access Controls. Customer shall have access to Customer Data maintained within their applicable production instance. Customer shall be responsible for maintaining user access and security controls for users accessing the Hosted Services. Verint shall be responsible for restricting all other access to Customer Data residing within the production instance. For the avoidance of doubt, Verint has no obligation to verify that any user using Customer's account and password has Customer's authorisation. Verint shall provide access on a need to know basis and shall review access rights of Verint Personnel at least annually. Verint's access controls shall include no less than the following:

- Verint shall enforce complex passwords using built in system settings of at least 8 characters. Verint shall require password changes at least every ninety (90) days. Verint administrators shall use multi-factor authentication for access to the production environment(s).
- Access to Verint's production environment(s) is controlled at four distinct hierarchical levels: the hosting partner level, the Hosted Services operations team level, the Verint network security level, and the application level. Access control is required for each of these levels to provide the optimal level of security for the solution.
- Any Customer Data accessed by authorized Verint Personnel is subject to the aforementioned access controls and is encrypted at rest and in transit.
- A Verint hosting partner's role is to design, deploy, secure, make available, and support the infrastructure upon which Hosted Services operate. For the avoidance of doubt, "hosting partner" shall mean the Sub-processors providing Hosted Services infrastructure specified in an Order or the Data Processing Instructions. The hosting partners have primary control over the infrastructure upon which Hosted Services operate but such control does not extend to access to Customer Data or Verint solutions processing Customer Data. The hosting partner provides Verint's operations teams with the initial credentials required to access the infrastructure and associated support portals to enable Verint to operate and manage the Hosted Services.

3.2 Data Controls. In its performance obligations with respect to Hosted Services, Verint does require access to Customer Data, and the following additional terms and conditions shall apply:

- Verint's security procedures shall require that any Customer Data stored by Verint only be stored using secure data encryption algorithms and key strengths of 128-bit symmetric and 1024-bit asymmetric or greater. Verint shall monitor Industry Standards and implement an action plan if key lengths in use can be compromised through commercially reasonable means.
- Verint will maintain a key management process that includes appropriate controls to limit access to private keys and a key revocation process. Private keys, and passwords shall not be stored on the same media as the data they protect.
- Verint will prohibit Verint Personnel from the download, extraction, storage or transmission of Customer Data through personally owned computers, laptops, tablet computers, cell phones, or similar personal electronic devices except where enrolled in Verint's Mobile Device Management (MDM), Information Rights Management (IRM), or other security programs. If personal computers or mobile devices are used to perform any part of the Hosted Services, Verint will encrypt all Customer Data on such mobile devices.
- Verint agrees that any and all electronic transmission or exchange of Customer Data shall be protected by a secure and encrypted means (e.g. HTTPS, PGP, S/MIME, SSH, SMTP encryption using TLS on gateway while sending emails).
- Customer Data stored as a part of the Hosted Services shall reside only on Verint production systems housed in Verint hosting partner data centers, unless noted in an Order or statement of work or required with respect to professional service engagements or performance of support services. Any storage of Customer Data on Verint premises is temporary and is used strictly for support and services engagements. Once Customer Data on Verint premise has served its purpose, it shall be promptly destroyed in accordance with Verint's confidential data destruction procedures.

3.3 Operational Controls. In its performance of Hosted Services, Verint shall maintain operational controls sufficient to enable Verint's satisfaction of its performance obligations in this Section 3, including, without limitation, the following:

- Verint will utilise up-to-date and comprehensive virus and malware protection capabilities, and commercially reasonable practices, including detection, scanning and removal of known viruses, worms and other malware on the Verint's hosting systems. These virus protection capabilities will be in force on all computers and/or devices utilised in connection with the technology services, as well as on all data files or other transfers that have access or are connected to Verint's hosting system.
- If a virus, worm or other malware causes a loss of operational efficiency or loss of data, Verint will mitigate losses and restore data from the last virus free backup to the extent practicable.
- Verint shall obligate its hosting partners to provide a multiple layered security approach. This shall include perimeter firewalls, DMZ, one or more internal network segments, and network intrusion detection monitors for attempted intrusion to the production environment. Network vulnerability scans shall be conducted regularly, and issues addressed according to Industry Standard change control processes.
- Verint shall mitigate security vulnerabilities through the use of perimeter and host countermeasures such as intrusion prevention, web application firewall, IP address shunning, and other measures designed to prevent successful exploitation of vulnerabilities.

- Verint and its hosting partners shall proactively address security risks by applying released security patches, including, as example, Windows security patching and updates to patch known vulnerabilities in an applicable operating system. Patches shall be deployed to production via Verint's change management process. Verint shall test all patches in its test environment prior to release to production. If a patch degrades or disables the production environment, Verint shall continue to mitigate vulnerabilities until a patch is provided by the software or operating system manufacturer that does not degrade or disable production. Such mitigation efforts may include intrusion prevention, web application firewall, and other measures chosen by Verint to reduce likelihood or prevent successful access to Customer Data by an unauthorised party.
- Each month, Verint and its hosting partners shall schedule maintenance windows to perform data center, system, and application maintenance activities. Verint shall notify Customer in advance of any scheduled maintenance activity that is expected to disrupt the Hosted Services functionality.
- Verint shall retain security logs for a minimum of thirty (30) days online and ninety (90) days archived. Verint may retain logs for a longer period at its sole discretion.

3.4 **Availability Controls.** With respect to Hosted Services:

- Verint shall maintain business continuity and disaster recovery plans specific to its Hosted Services and shall include data center failover configurations.
- Verint shall maintain a backup of all Customer Data that Verint is required to retain as a part of the Hosted Services. In the event the Customer Data becomes destroyed or corrupt, Verint shall use commercially reasonable efforts to restore all available data from backup, and remediate and recover such corrupt data.

4 **ATTESTATIONS OF COMPLIANCE.** Upon Customer's reasonable request, **(i)** Verint shall provide an attestation of compliance to the terms in this Schedule, and/or **(ii)** Verint shall provide its Industry Standard security assessment questionnaire responses applicable to the services provided to Customer. Requests shall be made in writing through the Account Executive assigned to Customer unless otherwise specified by Verint.

SCHEDULE E
DATA PROCESSING SCHEDULE

This Schedule E is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule E is attached.

1. Definitions

1.1 In addition to the capitalised terms in Schedule A, all capitalised terms shall have the meaning ascribed to them herein this Schedule, and for the purposes of this Schedule, shall govern and control in the event of any conflict, including the following:

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 jurisdiction;

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 Schedule E, 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 Schedule E shall mean the Customer;

1.1.4 "**Data Processing Instructions**" means the Processing instructions set out at [redacted]

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 Schedule E shall mean Verint;

1.1.6 "**Data Subject**" means an identified or identifiable natural or legal 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 [redacted]

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 Schedule E, shall mean the data provided by Customer to Verint for Processing;

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 the Processing of Personal Data;

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 this Agreement and Data Processing Instructions;

1.1.12 **"Restricted Transfer"** means:

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

1.1.12.2 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;

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

1.1.14 **"Standard Contractual Clauses"** means the contractual clauses approved by the EU Commission or a Supervisory Authority 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 the specific references to standard contractual clauses in Section 11 of this Schedule E;

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 or other legal body which is established in a jurisdiction under Privacy Laws and responsible for monitoring applicable Privacy Laws.

1.2 References in this Schedule E to Verint include to Verint Affiliates where such Verint Affiliates are Subprocessors.

2. Processing of Personal Data

2.1 Customer agrees to appoint Verint as its Data Processor and that providing Personal Data to Verint pursuant to this Agreement complies with the relevant Privacy Laws.

2.2 Verint will not:

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

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

2.3 Customer on behalf of itself and each Customer Affiliate:

2.3.1 instructs Verint:

2.3.1.1 to Process Personal Data; and

2.3.1.2 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 Schedule E.

2.4 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 Data Subjects, 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 Schedule E 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 this Schedule E. Customer authorises Verint to appoint Subprocessors in

accordance with this Section 5 subject to any restrictions or conditions expressly set out in this Agreement. Subprocessors appointed as at the effective date of this Schedule E 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 this 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 this 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 Schedule E as they apply to Processing of Personal Data carried out by that Subprocessor, as if such Subprocessor were party to this Schedule E 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 to, or inform, a Supervisory Authority and 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. 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

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 Verint shall comply with its obligations in Section 13.3(b) of Schedule B regarding the return of Personal Data.

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 Schedule E will continue to apply, (b) 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 of any review to be conducted under this Section 10.3, by contacting Verint's Global Privacy Officer by submitting a request via [redacted]

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 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 Schedule E or Privacy Laws.

11. Restricted Transfers

11.1 Customer, as ("data exporter") and Verint (its Affiliates or authorised Sub-processors), as appropriate, (as "data importer") hereby agree that the Standard Contractual Clauses shall apply in respect of any Restricted Transfer, where applicable and required by Privacy Laws. Each Party agrees to execute the Standard Contractual Clauses upon request of the other Party, to the extent required by Privacy Laws.

11.2 In respect of any Restricted Transfers from the European Economic Area, the parties agree to the following:

11.2.1 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;

11.2.2 The EU Standard Contractual Clauses will be incorporated into this Schedule E by reference and shall apply to the extent required under Privacy Laws;

11.2.3 The modules and Annexes of the EU Standard Contractual Clauses are set out at [redacted]

11.2.4 The parties agree that execution of this Agreement constitutes signature and acceptance of Schedule 1 to this Schedule E and acceptance and incorporation of the EU Standard Contractual Clauses.

11.3 In respect of any Restricted Transfers from the United Kingdom, the parties agree to the following:

11.3.1 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);

11.3.2 The UK Addendum will be incorporated into this Schedule E by reference and shall apply to the extent required under Privacy Laws;

11.3.3 The parties agree that execution of this Agreement constitutes signature and acceptance of Schedule 1 to this Schedule E and acceptance and incorporation of the UK Addendum;

11.3.4 Tables 1 to 4 (inclusive) to the UK Addendum shall be deemed completed with the information set out in at [redacted]

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

11.4.1 The Standard Contractual Clauses shall have the same meaning as described in Section 11.2.1 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 [redacted]

11.4.2 The Standard Contractual Clauses for the purpose of Restricted Transfers from Switzerland will be incorporated into this Schedule E by reference and shall apply to the extent required under Privacy Laws;

11.4.3 The parties agree that execution of this Agreement constitutes signature and acceptance of Schedule 1 to this Schedule E and acceptance and incorporation of the Standard Contractual Clauses for the purpose of Restricted Transfers from Switzerland.

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 Schedule E, 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 Schedule E or in an Order.

12.2 If any variation is required to this Schedule E 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 Schedule E, 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 to a third country.

13.2 The parties agree that any electronic link included in this Schedule E and the content thereof form integral part of this Schedule E.

13.3 Nothing in this Schedule E reduces Verint's or any Verint Affiliate's obligations under this Agreement in relation to the protection of Personal Data or permits Verint or any Verint Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by this Agreement. In the event of inconsistencies between the provisions of this Schedule E and any part of any other agreements between the parties, including this Agreement, the provisions of this Schedule E shall prevail. 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 Schedule E and this Agreement.

ANNEX 1 TO SCHEDULE E

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) [Customer]:

1. Name: … as specified in the signature block of the Signature Page

   Address: … as specified on the Signature Page

   Contact person's name, position and contact details: …as specified in the signature block of the Signature Page

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

   Signature and date: … as evidenced by the execution of the Agreement on the Signature Page

   Role (controller/processor): …controller.

…

2.

Data importer(s) [Verint]:

1. Name: … as specified in the signature block of the Signature Page

   Address: … as specified on the Signature Page

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

   Activities relevant to the data transferred under these Clauses: …as specified in this Agreement and the Data Processing Instructions

   Signature and date: … as evidenced by the execution of the Agreement on the Signature Page

   Role (controller/processor): … processor

…

2.

SCHEDULE F
PROFESSIONAL SERVICES RATE CARD

This Schedule F is made a part of the Agreement signed by the parties on the Signature Page to which this Schedule F is attached.

Overview

The Rate Card which is applicable to professional services which may be provided by Verint, during the term of the Agreement, is set out below.

Role	Day Rate
Systems Engineer	[redacted]
Systems Integrator	[redacted]
Application Consultant	[redacted]
Business Consultant	[redacted]
Project Manager	[redacted]
AdviceLine*	[redacted]

*** AdviceLine is a flexible consulting service; a minimum of 1 day can be ordered, the consulting services are typically scheduled by mutual agreement, in hourly increments, for 1:1 or small group engagements.**

The roles and rates described are those that we would expect to relate to professional services engagements which are typically associated with the SaaS Services. Other roles/rates may be applicable, by exception.

Services are typically set out in a Statement of Work and associated Quote/Order Form, which will be agreed by the parties prior to the Customer raising an Order.

Supplementary Notes

Except where defined differently in a Statement of Work, the following terms will typically apply to the scoping of services engagements.

- Working day: 8 hours exclusive of travel and lunch
- Working week: Monday to Friday excluding UK Public Holidays
- Normal Working Hours: between 08.00 and 18.00, Monday to Friday, or as otherwise defined in a Statement of Work.
- Normal Services methodology is 'remote working', or as otherwise defined in a Statement of Work.
- Travel, mileage and subsistence: when appropriate, normal and reasonable travel, in the United Kingdom only, is included in the day rate. Any exceptional travel, mileage and subsistence requirements will be negotiated and defined in a Statement of Work.