OneTrust Master Terms of Service

This software subscription agreement is made up of these Terms of Service (including Annexes and Appendices hereto, "**Terms**") together with any Order Forms (collectively, "**Agreement**") and is made between Customer ("**Customer**" or "**you**") and the OneTrust entity identified on the Order Form ("**OneTrust**") (each a "**Party**", together, the "**Parties**") and governs Customer's use of the OneTrust Software and Professional Services.

If you enter into these Terms on behalf of a company or other legal entity including any Affiliates, you represent that you have the authority to bind such entity and Affiliates. If you do not have such authority, or if you do not unconditionally agree to these Terms, you, the company, and its Affiliates have no right to use the Software. Affiliates of either Party may also execute Order Forms subject to these Terms.

1. DEFINITIONS.

"Affiliate" means, with respect to a Party, any corporation or other business entity Controlled by, Controlling or under common Control with that Party, whereby Control means (i) the direct or indirect ownership of more than 50% (fifty percent) of the equity interest in such corporation or business entity, or (ii) the ability in fact to control the management decisions of such corporation or business entity.

"API" means any application programming interface made available by OneTrust to Customer in connection with the Agreement.

"Authorized Users" means Customer, its Affiliates, and their respective employees, contractors or consultants.

"Customer Content" means any data, applications, files, information or materials input into the Software or provided to OneTrust in the course of performing Professional Services, by or on behalf of Customer or its Authorized Users.

"Documentation" means the OneTrust User Guide, written release notes, implementation guides and any other technical documentation related to the Software or Professional Services which is made available to Customer by OneTrust.

"Environment" means one software installation with a unique database in a logically separated tenant environment including unlimited users and groups within the organizational hierarchies, except where otherwise indicated on the Order Form.

"Intellectual Property Rights" means all intellectual property rights throughout the world, including: (a) patents, disclosures of inventions (whether or not patentable), patent applications, reissues, reexaminations, utility model rights and design rights (registered or otherwise), and registered or other industrial property rights, (b) trademarks, service marks, corporate names, trade names, Internet identifiers, trade dress, and other similar designations of source or origin together with the goodwill symbolized by any of the foregoing, (c) copyrights, moral rights, design rights, database rights, data collections, and other sui generis rights, (d) trade secrets or other proprietary rights in confidential information or technical, regulatory and other information, designs, results, techniques, and other know-how, and (e) applications, registrations, and renewals for, and all associated rights with respect to, any of the foregoing in any part of the world.

"OneTrust Support Portal" means my.onetrust.com (or any successor support website provided by OneTrust).

"OneTrust User Guide" means the most current user specification for the Software available in the OneTrust Support Portal.

"Order Form" means the: (i) signed order form between the Parties referencing these Terms; or (ii) the applicable online registration form or click through agreement referencing these Terms.

"Professional Services" means any services performed by OneTrust relating to the Software such as installation, activation, training, configuration, integration, assessment, and optimization.

"Software" means the software applications provided by OneTrust and set out in the Order Form or which OneTrust otherwise agrees to license to Customer, including Upgrades thereto and any related content, APIs, software delivery kits, software tools and Environments provided by OneTrust.

"SOW" means any statement of work which is: (i) signed by both Parties and incorporates these Terms, or (ii) referenced on an Order Form that incorporates these Terms.

"Support" means the technical support services at the subscription level set out in the Order Form, as described in the OneTrust support offering as amended from time to time by OneTrust and posted online (currently https://onetrust.com/support/supportoffering.pdf) (the "**Support Offering**").

2. LICENSE GRANT AND RESTRICTIONS.

2.1.   OneTrust grants to Customer and its Affiliates a non-sublicensable, non-transferable, non-exclusive right to access and use the Software and Documentation for Customer's and its Affiliates' internal business or compliance purposes during the subscription term stated in the applicable Order Form. Customer will not be provided with and shall have no right to any software code and OneTrust reserves the right to suspend access to the Software for scheduled maintenance (in accordance with the Support Offering) or emergency maintenance. Customer is responsible for Authorized Users' compliance with the Agreement.

2.2.   Unless otherwise expressly set out in the Order Form, Customer's right to use the Software shall be limited to one production Environment of the Software.

2.3.   Customer shall not: (a) provide access to the Software or Documentation to any third party (except Authorized Users) or otherwise permit a third party (except Authorized Users) to use or benefit from the Software or Documentation, (b) copy, modify, or reverse engineer the Software or otherwise attempt to discover any software code, or underlying technical information (except to the limited extent that applicable law prohibits such restrictions), (c) use or export the Software: (i) in breach of any applicable laws, regulations, embargoes, restrictive measures or the Documentation; or (ii) to any country for which the United States or any other government, at the time of export requires an export license or other governmental approval, without first obtaining such license or approval, (d) access, store, or transmit any viruses, spam, or duplicative messages, or any material that is unlawful, abusive, obscene, or harmful, (e) for data in or from the United States, input any Protected Health Information (as the term is defined in the Health Insurance Portability and Accountability Act of 1996 (as amended, superseded or replaced) in the Software, or (f) use the Software: (i) to try to gain unauthorized access to any service, device, data, account or network or (ii) in a manner that

infringes Intellectual Property Rights. OneTrust shall not be responsible for any Authorized Users' use of third-party software or systems accessed from the Software.

2.4. Except to the extent caused by a breach of the Agreement by OneTrust, Customer is responsible for (i) all activity occurring under Customer's user accounts; and (ii) Customer Content, and shall hold OneTrust and its Affiliates harmless and indemnify them for all claims, losses, damages, liabilities, costs (including legal fees) and expenses arising out of or relating to Customer Content. Customer shall maintain the copyright notices that appear on any materials relating to the Software and Documentation.

3. UPGRADES.

OneTrust may issue new releases for the Software including, upgrades, features, fixes, or patches ("**Upgrades**") which will be provided at no additional charge and will be automatically available.

4. FEES AND PAYMENT.

Fees will be invoiced according to the Order Form. All payment obligations are non-cancelable and all amounts paid are non-refundable (unless expressly stated otherwise in the Agreement). All payments shall be made in the currency indicated in the Order Form in full and cleared funds without any set-off, counterclaim, deduction or withholding (except for any deduction or withholding required by law) within thirty (30) days after the applicable invoice date, unless otherwise specified in the Order Form ("**Payment Due Date**"). All sums payable under the Agreement are exclusive of value added tax (VAT) or any other local sales taxes, for which Customer shall be responsible. If payment has not occurred by the Payment Due Date, then without limiting any other right or remedy available to OneTrust, OneTrust reserves the right to charge a late fee ("**Late Fee**") of 1.5% of the invoice amount. Prior to charging Late Fees, OneTrust will contact Customer regarding the delinquency and verify receipt of the applicable invoice. Customer agrees to provide OneTrust with complete and accurate billing and contact information.

5. LIMITATION OF COMPLIANCE, NO LEGAL ADVICE.

Each party is responsible for its own compliance with applicable laws. The Software, Professional Services, materials, or information provided by OneTrust are not intended, and should not be taken, as legal advice. Customer shall be responsible for ensuring that any information provided to OneTrust in connection with the Professional Services is accurate and complete.

6. LIMITED WARRANTY AND DISCLAIMERS.

6.1. OneTrust warrants that (i) the Software will substantially perform the functions set forth in the OneTrust User Guide (the **"Specification"**), (ii) Support shall conform to the Support Offering, and the Support Offering shall not materially degrade during the Term, (iii) it shall provide Professional Services in a workmanlike and professional manner pursuant to any applicable Statement of Work, and (iv) it shall use industry standard measures to prevent viruses from being released in the Software. If Customer notifies OneTrust in writing of any failure in the Software, Support or Professional Services to materially conform to the warranties outlined above, OneTrust shall, at its option and expense: (a) repair, (b) replace or reperform, or (c) if unable to repair, replace or reperform, terminate the Agreement or the applicable Order Form with respect to the non-conforming Software, Support or Professional Services, and issue a pro rata refund of the fees paid for the terminated Software, Support or Professional Services. This remedy is conditioned upon Customer providing information necessary to assist OneTrust in resolving the nonconformance, including a documented example of any nonconformance, or sufficient information to enable OneTrust to re-create the nonconformance. This Section 6.1 is Customer's sole and exclusive remedy under the warranties.

6.2. TO THE MAXIMUM EXTENT PERMITTED BY LAW, ONETRUST DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, CONDITIONS, REPRESENTATIONS OR OTHER TERMS RELATING TO THE SOFTWARE, SUPPORT, OR PROFESSIONAL SERVICES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OR OTHER TERMS OF SATISFACTORY QUALITY, MERCHANTABILITY AND FITNESS FOR A PURPOSE OR A PARTICULAR PURPOSE.

6.3. OneTrust is not responsible for any delays, delivery failures, or other loss or damage resulting from the transfer of data over communications networks and facilities which are not directly controlled by OneTrust. Customer acknowledges that the Software may be subject to problems inherent in the use of such communications facilities.

6.4. In the event of any loss or damage to Customer Content, Customer's sole and exclusive remedy shall be for OneTrust to use reasonable commercial endeavors to restore the lost or damaged Customer Content from the latest back-up of such Customer Content maintained by OneTrust in accordance with its archiving procedure.

7. ONETRUST INDEMNITY.

7.1. OneTrust, at its sole expense, agrees to defend Customer and its Affiliates (each, a "**Customer Indemnitee**") against any third-party claim that Customer Indemnitee's use of the Software, as made available by OneTrust to Customer and used in accordance with the Agreement, directly infringes a third party's Intellectual Property Right (an "**Infringement Claim**"), and indemnify Customer Indemnitee from the resulting costs and damages finally awarded against Customer Indemnitee to such third party by a court of competent jurisdiction or agreed to in settlement; provided that: (a) Customer Indemnitee promptly notifies OneTrust in writing of the Infringement Claim; (b) OneTrust has sole control of the defense and all related settlement negotiations; (c) Customer Indemnitee provides OneTrust with the information, assistance and authority to enable OneTrust to perform its obligations under this Section 7; and (d) Customer Indemnitee makes no admission of liability and does not compromise the ability of OneTrust to defend the claim. Customer Indemnitee may not settle or compromise any Infringement Claim without the prior written consent of OneTrust.

7.2. In any action based on an Infringement Claim, OneTrust, at its option and expense, will either: (i) procure the right for Customer to continue using the Software in accordance with the Agreement; (ii) make modifications to or replace the Software so that the infringing Software becomes non-infringing without incurring a material diminution in performance or function; or (iii) terminate the right to use the infringing Software and refund to Customer the unused remainder of any Software subscription fees prepaid by Customer and received by OneTrust for such infringing Software. OneTrust shall have no liability or obligations for an Infringement Claim pursuant to this Section 7 to the extent that it results from: (A) modifications to the Software made by a party other than OneTrust or a party under the direct control of OneTrust; (B) the combination, operation or use of the Software with non-OneTrust products, software, or materials; (C) use of the Software outside the scope of the Agreement; (D) OneTrust's use of any Customer Content, designs, instructions, specifications, or the like, provided by Customer Indemnitee, if any; or (E) use of third party software or, technology not embedded by OneTrust into the Software. This Section 7 sets out Customer Indemnitees' sole and exclusive

remedies and OneTrust's entire liability with respect to claims subject to indemnification under this Section, including claims for infringement or violation of third-party Intellectual Property Rights by the Software.

8. LIMITATION OF LIABILITY AND DAMAGES.

8.1. EACH PARTY'S TOTAL AGGREGATE LIABILITY REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING BUT NOT LIMITED TO NEGLIGENCE), BREACH OF STATUTORY DUTY, STRICT LIABILITY OR OTHER THEORY, WITH RESPECT TO ALL SUBJECT MATTER RELATING TO THE AGREEMENT SHALL NOT EXCEED THE TOTAL OF THE AMOUNTS PAID AND PAYABLE TO ONETRUST (WHETHER OR NOT INVOICED) UNDER THE AGREEMENT IN THE YEAR PRECEDING THE FIRST EVENT GIVING RISE TO A CLAIM. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS LIMIT.

8.2. NEITHER PARTY WILL BE LIABLE FOR ANY: (A) SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES; (B) LOSS OF REVENUES; (C) LOSS OF PROFITS; (D) LOSS OR INACCURACY OF DATA; OR (E) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY, ARISING IN CONNECTION WITH THE AGREEMENT, IN EACH CASE, REGARDLESS OF THE FORM OF ACTION (AND WHETHER (B) THROUGH (E) ARE DIRECT, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL), WHETHER IN CONTRACT, TORT (INCLUDING BUT NOT LIMITED TO NEGLIGENCE), BREACH OF STATUTORY DUTY, STRICT LIABILITY OR OTHER THEORY.

8.3. THE LIMITATIONS AND EXCLUSIONS CONTAINED IN SECTIONS 8.1 AND 8.2 SHALL NOT APPLY TO BREACHES OF LICENSE RESTRICTIONS SET OUT IN SECTION 2, INDEMNIFICATION OBLIGATIONS, CUSTOMER'S PAYMENT OBLIGATIONS, A BREACH OF SECTION 9 (CONFIDENTIALITY AND PROPRIETARY INFORMATION), AND WILLFUL MISCONDUCT. NOTHING IN THE AGREEMENT SHALL LIMIT OR EXCLUDE EITHER PARTY'S LIABILITY FOR ANY LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY LAW.

9. CONFIDENTIALITY AND PROPRIETARY INFORMATION.

A Party (the "**Receiving Party**") may receive Confidential Information of the other Party or its Affiliates (the "**Disclosing Party**") and the Receiving Party shall keep all such Confidential Information confidential and protect it by using the same level of care and discretion that the Receiving Party uses with respect to its own confidential information, which will be in no case less than reasonable care and discretion. The Receiving Party shall not disclose Confidential Information to any person other than such Party's Authorized Users, or OneTrust's subprocessors, who have a need to know that Confidential Information provided that the Receiving Party remains responsible for the confidentiality of the information. The Parties shall not use Confidential Information for any purpose other than as necessary to exercise rights or fulfill obligations under the Agreement. Without limiting the foregoing, either Party may disclose Confidential Information to a government authority if that disclosure is: (a) required by law or (b) necessary to exercise its rights or perform its obligations under and in accordance with the Agreement. To the extent Customer performs any benchmarking or comparative study or analysis involving the Software (or such is done on its behalf), Customer may only disclose the results to its Authorized Users. In the Agreement, "**Confidential Information**" means business information of a confidential or proprietary nature (including trade secrets and information of commercial value), including without limitation, pricing, software, software code and underlying technical or business information, which relates to the Disclosing Party that is disclosed or provided to Receiving Party by or on behalf of Disclosing Party pursuant to the Agreement (or potential future purchases subject to this Agreement); provided, however, that Confidential Information shall not include information that (i) is or becomes a part of the public domain through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure and had not been obtained by the Receiving Party either directly or indirectly from the Disclosing Party; (iii) is lawfully disclosed to the Receiving Party by a third party without restriction on disclosure; (iv) is input into the Software or (v) is independently developed by the Receiving Party. This Section shall apply during the Term of this Agreement, and for three (3) years after the Agreement's termination.

10. TERMINATION; SUSPENSION.

10.1. Without affecting any other right or remedy available to it, either Party may terminate the Agreement with immediate effect by giving written notice to the other Party if the other Party breaches a material obligation under the Agreement that has not been cured (if curable) within thirty (30) business days of the effective date of such written notice requiring the remedy of such breach or if either Party (a) announces a cessation of its entire business or becomes insolvent; (b) elects to dissolve and wind-up its business; (c) makes a general assignment for the benefit of creditors; or (d) petitions for or appoints (or a third party causes to be appointed for itself) a receiver, custodian or trustee to take possession of all or substantially all of that Party's property. The Agreement will also terminate automatically upon the termination of all Order Forms unless automatically renewed pursuant to Section 17.1.

10.2. Upon termination of the Agreement by any means, the rights granted under Section 2 will terminate and (a) Customer shall promptly destroy any and all OneTrust Confidential Information, and, upon OneTrust's request, have an officer of Customer confirm the same in writing; (b) Customer may export a copy of the Customer Content (stored in the Software at the time of termination) in a structured, commonly used and machine-readable format within sixty (60) days after such expiration or termination and OneTrust may delete all Customer Content remaining in the Software after such time has passed; (c) OneTrust shall promptly destroy any and all Customer Confidential Information and an officer of OneTrust shall confirm the same to Customer in writing on Customer's request; otherwise, the terms of the Agreement will remain in effect with respect to such Confidential Information; and (d) OneTrust will remove access to the Software.

10.3. Without limiting the foregoing, OneTrust may upon fourteen (14) days' prior written notice (except in the event of an emergency under subsection (b)) suspend or limit Customer's access to or use of the Software without liability if (a) Customer's account is past due, or (b) Customer's use of the Software breaches Section 2 or impairs performance of the Software or OneTrust systems or use of the Software by other OneTrust customers; provided that OneTrust will promptly end such suspension when Customer cures the foregoing (without prejudice to OneTrust's other remedies in respect of the applicable breach).

10.4. Termination of the Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination.

11. DATA PROTECTION.

The Parties agree to comply with Annex 1 (Data Processing Addendum) with respect to the processing of any personal data under the Agreement.

12. INTELLECTUAL PROPERTY.

12.1. OneTrust or its third-party licensors own all Intellectual Property Rights embodied in the Software, Documentation, Support and/or any Professional Services provided by OneTrust or its Affiliates under the Agreement including all modifications or derivatives thereof. No rights are

granted to Customer other than as expressly set forth in the Agreement. OneTrust does not convey any Intellectual Property Rights other than those expressly provided herein.

12.2.   OneTrust shall be the sole owner of any newly-developed Intellectual Property Rights related in any way to the Software or Software code, Documentation, Support, or the Professional Services. The Customer hereby assigns to OneTrust any of these newly-developed Intellectual Property Rights that result from Customer's requests, feedback, or ideas ("**Feedback**"), regardless of whether such newly-developed Intellectual Property Rights result from Software-related services paid for by Customer. If OneTrust creates custom templates for Customer in connection with Professional Services performed under the Agreement, Customer may retain copies of such templates after any termination of the Agreement and OneTrust shall grant Customer a non-exclusive, non-transferable, non-sublicensable, royalty-free, perpetual license to use such templates for its internal business and compliance purposes only. Nothing contained in the Agreement shall prevent OneTrust from independently developing its own content.

12.3.   Customer Content (including Customer Content contained in any output from the Software) shall remain the property of Customer. To the extent materials developed by OneTrust in connection with the Agreement contain any Customer Content, OneTrust shall not own the Customer Content therein, and OneTrust shall have no right to use any part of Customer Content (except for Feedback, pursuant to Section 12.2).

13.   THIRD PARTY MATERIALS.

The Software may contain hyperlinks to other websites and databases, the content of which have not been authored or vetted by OneTrust, and which are provided on an "as-is" and "as-available" basis.

14.   SURVEYS.

OneTrust may conduct periodic surveys on a remote basis for the sole purposes of verifying Customer's use of the Software in compliance with the Agreement.

15.   NOTICE.

Except as otherwise provided herein, all notices under the Agreement shall be deemed properly given and effective (a) when personally delivered (to the person or department if one is designated in the Order Form); (b) when deposited in the United States certified mail, registered mail, postage prepaid or return receipt requested; or (c) when deposited with an internationally recognized overnight delivery service such as Federal Express with all fees and charges prepaid, and addressed in each such case as set out in the Order Form. When any notice under the Agreement is sent to OneTrust, a copy shall be sent to legal@onetrust.com.

16.   NONASSIGNABILITY.

Except for an assignment by OneTrust to a wholly owned Affiliate, neither the rights nor the obligations arising under the Agreement are assignable or transferable by either Party without the other Party's prior written consent (which will not be unreasonably withheld), and any such attempted assignment or transfer shall be void and without effect.

17.   EFFECTIVE DATE; TERM; GOVERNING LAW AND JURISDICTION; SEVERABILITY.

17.1.   The Agreement shall become effective on the date of the last signature on the initial Order Form between the Parties which references these Terms (the "**Effective Date**") and shall continue for a period of twelve (12) months ("**Initial Term**") or such other period indicated on the Order Form. Each Order Form shall automatically renew for an additional twelve (12) month term (each, a "**Renewal Term**," together with the Initial Term, the "**Term**") on OneTrust's then-current pricing and terms unless either party provides notice of its intent not to renew at least thirty (30) days in advance of the end of the Initial Term or current Renewal Term. OneTrust will provide Customer with sixty (60) days' notice of an upcoming Renewal Term. Any notice provided under this Section may be accomplished via email or electronically submitted invoice or notice.

17.2.   The Agreement and any dispute or claim (including non-contractual disputes or claims) arising under or in connection with the Agreement, its subject matter, or formation shall be governed by and construed in accordance with the governing law identified in Section 17.5 and will be resolved in accordance with such jurisdiction. The Parties consent to the exclusive jurisdiction of such court and waive any personal jurisdiction or venue defenses otherwise available. The United Nations Convention on Contracts for the International Sale of Goods is expressly and entirely excluded and will not apply to the Agreement. In any action to enforce the Agreement, the prevailing party will be entitled to reasonable costs and attorneys' fees actually incurred. No claim or action may be brought by either Party against the other Party arising in any way out of the Agreement after one (1) year from the date on which the cause of action arose (and regardless of the nature of the claim or form of action) provided, however, the foregoing limitation shall not apply to any claim or action related to the infringement of a Party's Intellectual Property Rights.

17.3.   Each provision of the Agreement shall be considered severable such that if any provision conflicts with any existing or future law, or is held to be illegal, unenforceable or invalid by a court, the other provisions of the Agreement shall be limited or modified to the minimum extent necessary to make it valid, legal, and enforceable and so that the Agreement shall otherwise remain in effect.

17.4.   The Agreement and all related documentation is and will be in the English language and all disputes arising under the Agreement shall be resolved in the English language.

17.5.   If the OneTrust contracting party is OneTrust LLC, the governing laws are the laws of Georgia, USA under the exclusive jurisdiction of the Courts of Atlanta, Georgia, USA. If the OneTrust contracting party is OneTrust Technology Limited, the governing laws are the laws of England and Wales under the exclusive jurisdiction of the Courts of England and Wales. If the OneTrust contracting party is OneTrust B.V., the governing laws are the laws of the Netherlands, under the exclusive jurisdiction of the Netherlands Commercial Court, Amsterdam, the Netherlands. If the OneTrust contracting party is OT Australia (Pty) Limited, the governing laws are the laws of Victoria, Australia under the exclusive jurisdiction of the Courts of Victoria, Australia. If the OneTrust contracting party is OneTrust Singapore Pte. Ltd., the governing laws are the laws of Singapore under the exclusive jurisdiction of the Courts of Singapore.

18.   ENTIRE AGREEMENT; MODIFICATIONS; WAIVERS; THIRD PARTY RIGHTS.

18.1.   The Agreement constitutes the entire agreement and understanding between the Parties with respect to the subject matter of this Agreement and the Software, superseding all prior or contemporaneous proposals, communications and understandings, oral or written relating to that subject matter. Each Party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty that is not set out in the Agreement. Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the Agreement. To the extent there is any conflict or inconsistency between the Terms and any Order Form, the Order

Form shall prevail to the extent of any such conflict or inconsistency. Any additional or different terms or conditions proposed by Customer are hereby expressly excluded.

18.2.   Except as expressly provided in the Agreement, any modifications of the Agreement must be in writing and signed by both Parties (and in the case of OneTrust, signed by the Chief Executive Officer, Chief Financial Officer, Chief Operations Officer or a Director of OneTrust).

18.3.   Any waiver of any provision of the Agreement must be in writing and will not be deemed a waiver of any other provision. Waiver by a Party of a breach of any provision of the Agreement by the other Party will not operate as a waiver of any other or subsequent breach by such breaching Party.

18.4.   Subject to Section 18.5, the Agreement does not confer any right or benefit on any person who is not a Party to it and no one other than a Party to the Agreement, their successors and permitted assignees shall have any right to enforce any of the terms of the Agreement.

18.5.   If applicable law prohibits a party from being indemnified on behalf of an Affiliate, such Affiliate shall be entitled to be indemnified directly pursuant to (and subject to the terms of the Agreement). Notwithstanding the foregoing, the consent of an Affiliate shall not be required to amend or terminate the Agreement.

19. GENERAL.

19.1.   A delay by either Party in performing its obligations will not be a breach of the Agreement if caused by fire, flood or other event beyond the reasonable control of such Party. The affected Party will notify the other Party of such event and resume performance as soon as possible.

19.2.   The Agreement may be executed in any number of counterparts, each of which is an original, but all the counterparts together constitute the same document. Delivery of an executed counterpart of a signature page to the Agreement by e-mail or other electronically delivered signatures of the Parties shall be as effective as delivery of a manually executed counterpart of the Agreement.

19.3.   Nothing in the Agreement is intended to create a joint venture, partnership, agency or employment relationship between the Parties.

19.4.   Sections 1, 2.3, 2.4, 4, 6, 7, 8, 9, 10, 11, 12, 17, 18, and 19, will survive the termination of the Agreement.

20. NON-PRODUCTION ENVIRONMENTS.

With respect to Customer's use of any non-production environment such as a user acceptance testing or trial Environment of the Software, the following shall apply, notwithstanding anything to the contrary herein. These Environments: (i) are not intended to contain production-level data and OneTrust shall not be responsible for any data input into such Environments; and (ii) may contain forward-looking code that is provided only for evaluation purposes. THESE ENVIRONMENTS ARE NOT SUBJECT TO ANY WARRANTY WHATSOEVER.

21. GOVERNMENT USE.

If Customer is part of an agency, department, or other entity of the United States government ("**Government**"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Software is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Software is a "commercial item," "commercial computer software" and "commercial computer software documentation." In accordance with such provisions, any use of the Software by the Government shall be governed solely by the terms of the Agreement.

22. ON-PREMISE SOFTWARE.

The following additional terms shall apply with respect to on-premise Software and to the extent there is a conflict between this Section 22 and the general terms applicable to Customer's use of the Software, this Section 22 shall prevail:

22.1.   "Environment" means one software installation in Customer's designated facility.

22.2.   Only Software object code will be provided, and Customer shall have no right to any Software source code. For on-premise Software, "access and use the Software" in Section 2.1 above means loading the Software into temporary memory or permanent storage on the relevant computer.

22.3.   Customer shall uninstall and remove the Software within thirty (30) days of termination of the license and OneTrust reserves the right to audit to confirm such removal. Upon termination, OneTrust has no obligations to retrieve or deliver to Customer a copy of Customer Content.

22.4.   Upgrades are not immediately and automatically available as of the release date. OneTrust will arrange assistance for Customer to guide and help Customer to implement the Upgrades, provided however that the Software version installed on-premise at the time Customer requests assistance to implement the Upgrade is either (i) one of the four (4) latest major versions of the Software; or (ii) any major version released within the prior six (6) months. Assistance from the OneTrust Professional Services team during the upgrade process may require the purchase of Professional Services.

22.5.   The warranty provided in Section 6.1 shall only apply to the extent such defect or fault does not result from Customer (i) modifying the Software, (ii) using it in combination with any other software not provided by OneTrust, or (iii) failure to load the Software onto OneTrust-specified or suitably configured equipment.

22.6.   OneTrust shall have no liability or obligations for an Infringement Claim pursuant to Section 7 to the extent that it results from Customer's failure to use all available Upgrades, if the claim would not have occurred but for such failure.

22.7.   OneTrust reserves the right to authorize a representative of OneTrust to verify Customer's compliance with these Terms in the least disruptive manner reasonably possible. Upon prior written notice, Customer shall perform such actions reasonably requested by OneTrust to exercise its rights under this Section 22.7. As an alternative, at Customer's election, an officer of Customer may provide written confirmation of Customer's compliance.

Annex 1 Data Processing Addendum

1. DATA PROTECTION

1.1. _Definitions:_ In this Annex, the following terms shall have the following meanings:

"**Applicable Data Protection Law**" means applicable data protection and privacy laws including, where applicable, EU Data Protection Law, UK Data Protection Law and the CCPA.

"**Business**", "**consumer**", "**personal information**", and "**service provider**" shall have the meanings given in Applicable Data Protection Law.

"**CCPA**" means the U.S. California Consumer Privacy Act of 2018, as amended or superseded from time to time, and any implementing regulations as promulgated by the California Attorney General.

"**Controller**", "**data subject**", "**personal data**", "**processor**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law.

"**EDPB Recommendations**" means the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

"**EU Data Protection Law**" means: (i) the EU General Data Protection Regulation (Regulation 2016/679); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any and all EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

"**UK Data Protection Law**" means the data privacy legislation adopted by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 as supplemented by the terms of the Data Protection Act 2018 and the UK GDPR (Retained Regulation (EU) 2016/679 (UK GDPR) pursuant to section 3 of the European Union (Withdrawal) Act 2018).

1.2. _Relationship of the Parties:_ Customer (the controller) appoints OneTrust as a processor to process the personal data described in the Agreement (the "**Data**") for the purposes described in the Agreement (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**"). OneTrust shall not retain, use, or disclose the Data for any purpose other than for the Permitted Purpose, or as otherwise permitted by the Applicable Data Protection Law, including retaining, using, or disclosing the Data for a commercial purpose other than the Permitted Purpose. OneTrust shall not buy or sell the Data.

1.3. _International Transfers & Data Localization Laws:_ If any Data originates from the European Economic Area ("**EEA**") under the Agreement, OneTrust shall not transfer the Data outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient (a) in a country that the European Commission has decided provides adequate protection for personal data, (b) that has achieved binding corporate rules authorisation in accordance with EU Data Protection Law, (c) that has executed standard contractual clauses adopted or approved by the European Commission. Where Data is governed by EU Data Protection Law and OneTrust LLC is party to the Agreement; (i) the applicable standard contractual clauses ("**SCC's**") at https://www.onetrust.com/legal-sccs ("**SCC's Webpage**") shall automatically be deemed to be a part of the Agreement; or (ii) Customer may enter into the applicable SCC's with OneTrust LLC by executing the pre-signed version on the SCC's Webpage and emailing a copy to legal@onetrust.com. Prior to transferring Data to a country outside the EEA ("**Third Country**"), OneTrust shall review the adequacy of data protection in the Third Country and shall apply (where necessary) the appropriate measures to ensure that the transferred Data is subject to an essentially equivalent protection as that guaranteed in its original jurisdiction. The supplementary measures implemented by OneTrust pursuant to the EDPB Recommendations are described in the OneTrust Support Portal. OneTrust shall (i) notify Customer by email (including through the OneTrust Support Portal) if OneTrust is unable to comply with its legal or contractual obligations related to international transfers under EU Data Protection Law; and (ii) suspend the applicable transfers of Data until it is able to comply with such legal and contractual obligations.

If any data originates from a country (other than an EEA country) with laws imposing data transfer restrictions, then Customer shall inform OneTrust of such data transfer restrictions before such data is input into the Software, in order to enable Customer and OneTrust to ensure (where one is available) an appropriate and mutually agreed transfer mechanism is in place. Customer shall not use or access the Software in a manner that would require Customer's Environment to be hosted in a country other than the Data Center location selected on the applicable Order Form in order to comply with applicable law (including data localization laws).

For Data originating from the United Kingdom ("**UK**") references in this Section 1.3 to (i) the "EEA" shall be replaced with the "UK"; (ii) "EU Data Protection Law" shall be replaced with "UK Data Protection Law" and; (iii) the "European Commission" shall be replaced with the "Information Commissioner's Office".

1.4. _Security:_ Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, OneTrust shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (in accordance with Applicable Data Protection Law) to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Breach**"). All penetration or other testing conducted by Customer shall be done in a designated testing environment and pursuant to mutual agreement of the parties. OneTrust LLC's Information Security Management System (ISMS) is ISO/IEC 27001:2013 certified and its Privacy Information Management System (PIMS) is ISO/IEC 27701:2019 certified. OneTrust LLC has completed a SOC 2 Type 2 report providing verification of the security, confidentiality, and availability controls maintained by OneTrust LLC and OneTrust Technology Limited.

1.5. _Subprocessing:_ Customer consents to OneTrust engaging subprocessors to process the Data for the Permitted Purpose. The current list of subprocessors is maintained at https://my.onetrust.com/s/list-of-subprocessors ("**Subprocessors List**"). OneTrust shall (i) update the Subprocessor List with any change in subprocessors at least 30 days' prior to such change (except to the extent shorter notice is required due to an emergency) and Customer may sign-up to e-mail notification of any change to the Subprocessors List; (ii) impose data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and (iii) remain liable for any breach of this Data Processing Addendum that is caused by an act, error or omission of its subprocessor. Customer may object to OneTrust's appointment of a subprocessor prior to its appointment, provided such objection is based on reasonable data protection grounds.

OneTrust

In such event, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

1.6. *Cooperation and Data Subjects' Rights:* Taking into account the nature of the processing, OneTrust shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to OneTrust, OneTrust shall promptly inform Customer providing full details of the same.

1.7. *Assessment, Consultation and Assistance:* Taking into account the nature of the processing, OneTrust shall provide Customer with reasonable cooperation (at Customer's expense) to enable Customer to (i) conduct any data protection or transfer impact assessments that it is required to undertake under Applicable Data Protection Law; and (ii) consult competent supervisory authorities prior to processing where required by Applicable Data Protection Law.

1.8. *Security Breaches:* If it becomes aware of a Security Breach, OneTrust shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under Applicable Data Protection Law. OneTrust shall further take such reasonably necessary measures and actions to mitigate the effects of the Security Breach and shall keep Customer informed of all material developments in connection with the Security Breach. The Customer acknowledges that in the event of a Security Breach impacting a subprocessor of OneTrust, the Customer may receive notification directly from the subprocessor in accordance with the Standard Contractual Clauses between OneTrust and such subprocessor. In such event, the Customer agrees to provide any reasonable co-operation or assistance required by OneTrust and the subprocessor in order to facilitate such notification.

1.9. *Deletion or Return of Data:* Following termination of the Agreement, Customer shall have sixty (60) days to export its Data from the Software and after such time has passed OneTrust may destroy all Data in its possession or control. This requirement shall not apply to the extent that: (i) OneTrust is required by applicable law to retain some or all of the Data; or (ii) Data is archived on OneTrust's back-up and support systems, provided that OneTrust shall continue to protect such Data in accordance with its obligations herein.

1.10. *Review & Audit:* OneTrust shall deal promptly and adequately with any enquiries from the Customer about the processing of Data in accordance with this Data Processing Addendum and make available all information reasonably necessary to demonstrate compliance with its obligations in this Data Processing Addendum for Customer's review ("**Review**"). To the extent Customer cannot reasonably establish OneTrust's compliance pursuant to a Review, OneTrust shall, upon reasonable notice (no less than forty-five (45) days) and payment of a reasonable fee, not more than once a year (unless there is a material Security Breach, in which case a second audit is permitted), allow its procedures and documentation to be inspected or audited ("**Audit**") by Customer (or its designee, as agreed between the Parties) during business hours, and without interrupting OneTrust's business operations, in order to ascertain compliance with this Data Processing Addendum. For the avoidance of doubt, the scope of any Audit shall be limited to documents and records allowing the verification of OneTrust's compliance with this Data Processing Addendum and shall not include financial records of OneTrust or any records concerning OneTrust's other customers. Remote audits shall be utilized where possible, with on-site audits occurring only where a walkthrough of the premises is required. In deciding whether to undertake a Review or Audit, the Customer shall take into account the relevant certifications held by OneTrust. Where required by a competent supervisory authority, the Parties shall make available any information provided pursuant to a Review or Audit to such supervisory authority.

1.11. *Transparency Reports:* OneTrust will not disclose or provide access to any Data to any public authorities unless required by law. OneTrust's policy on dealing with requests from public authorities in relation to Data ("**Legal Requests**") together with OneTrust's transparency report on Legal Requests, is available at https://www.onetrust.com/transparency-report/. Where the Data impacted by the request is governed by EU Data Protection Law, OneTrust commits to (i) reviewing the legality of the public authority's data requests and to challenging them where lawful and appropriate; and (ii) where the Legal Request is incompatible with Art. 46 of the GDPR, to informing the public authority of the same.

Appendix 1: OneTrust Information Security Controls

OneTrust has organized and implemented technical and organizational measures for personal data protection according to ISO 27001 and ISO 27701 to support its data protection program. The measures include the following types of controls:

Information Security Policies
- Provides management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

Organization of Information Security
- Establishes a framework for initiating and controlling information security implementation and operations at OneTrust.

Enterprise Risk Management
- Defines the methodology for the assessment and treatment of risks associated with the loss of confidentiality, integrity, and availability of information, and define the acceptable risk level.

Human Resource Security
- Ensures that all workforce members are well suited for, and understand, their roles and responsibilities.
- Ensures that potential workforce hires undergo background checks.
- Ensures that workforce members sign non-disclosure agreements and commit to acceptable use policies.
- Ensures that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations, such as adhering to OneTrust's password policies.
- Ensure that workforce members who handle personal data receive additional privacy and security training to better understand their responsibilities and obligations. These members must obtain both the Certified Information Privacy Professional/Europe (CIPP/E) and the Certified Information Privacy Manager (CIPM) certifications
- Ensures that the organization's interests are protected throughout the employment process, from pre-employment to termination.

Asset Management
- Identifies and classifies OneTrust's information assets, defines and assign appropriate responsibilities for ensuring their protection, and sets their retention schedules.
- Ensures an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization.
- Prevents the unauthorized disclosure, modification, removal, or destruction of information stored on media.

Access Control
- Sets forth management principals governing information security and cybersecurity to secure information in any form information in any for.
- Establishes governing principles for the protection of all OneTrust's information and to reduce the risk of unauthorized access to OneTrust's information.
- Provides the framework for user, system and application access control and management, and user responsibilities.
- Limits access to information and information processing facilities.
- Ensures authorized user access and prevents unauthorized access to systems and services.
- Makes users accountable for safeguarding their authentication information.
- Prevents unauthorized access to systems and applications.

Cryptography
- Ensures proper and effective use of cryptography in order to protect the confidentiality, authenticity, and integrity of information.
- Provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.
- Establishes procedures on proper encryption for data in motion encryption, data at rest encryption and key management.
- Uses end-to-end encryption and encrypts data in transit and at rest.

Physical and Environmental Security
- Establishes procedures for properly defining secure areas, entry, threat protection, equipment security, secure disposal, clear desk and clear screen policies, and visitor access in order to prevent (1) unauthorized physical access, damage, and interference with OneTrust's information and information processing facilities; and (2) loss, damage, theft, or compromise of OneTrust's assets, and interruption of its operations.

Operations Security
- Establishes procedures on the proper management of IT systems, including change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, and audit controls
- Ensures that information and information processing facilities are operated securely and protected from malware and loss of data.
- Ensures that security events are recorded appropriately.
- Maintains operational system integrity and avoids exploitation of technical vulnerabilities.

Communications Security
- Establish controls related to network security, network segregation, network services, transfer of information internally and externally, messaging, and more.

System Acquisition, Development, and Maintenance
- Establishes security requirements for the procurement and deployment of technology solutions, as well as the requirements for internal development and support processes.

OneTrust

Supplier Relationships

- Provides a framework for OneTrust to perform vendor risk management, including due diligence, identification of contractually required privacy and security controls, and the management and monitoring of third-party suppliers (i.e., vendors, service providers, and processors) from onboarding to offboarding to ensure proper information security and service delivery.

Information Security Incident Management

- Establishes policies to reduce the impact of security incidents to the confidentiality, integrity, and availability of OneTrust's technology resources, services and information.
- Enables OneTrust to provide consistent, repeatable, and measurable guidance that reduces or eliminates the ambiguity and questions that would otherwise commonly appear and result in inconsistent processes

Information Security Aspects of Business Continuity Management

- Establishes business continuity framework and defines how OneTrust should recover its IT architecture and IT services within set deadlines in the event of a disaster or other disruptive incident.
- Ensures data backup for cloud-hosted implementations.
- Maintains a business continuity plan and ensures annual technical and tabletop tests.

Compliance

- Ensures OneTrust's compliance with respect to the organization's internal policies and procedures and contractual obligations related to information privacy and security, and applicable privacy, information security, and data protection laws and regulations.

Other Industry Standard Security Controls

- Penetration Testing
- Vulnerability Management
- Application Architecture Security
- Application Password Policy
- OAuth-based Authorization
- API Security
- Privacy by Design
- Government Personal Data Request Policy

Appendix 2: Details on the processing of Data

Categories of Data subjects:

- ☒ Customer employees, contractors, agents, consultants, vendors and customers whose personal information is shared with OneTrust for the purpose of providing and using the Software.
- ☐ Other [Customer may elect to include additional data subjects defined here]

Categories of personal data processed:

- The Personal Data processed is personal data provided by Customer and processed by OneTrust in the course of providing the Software.
- The personal data processed may concern the following categories of data:
- ☒ Identification data
- ☐ Personal characteristics
- ☐ Physical details
- ☐ Profession and employment
- ☐ Other [To be defined by Customer] _____

Special categories of data (if appropriate)

The personal data processed will not include sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, government issued identification numbers, credit card details, PCI-related sensitive data (including but not limited to magnetic strips and chip data, CAV2/CVC2/CVV2/CID4 numbers, and personal identification numbers (PINs)), health or medical records and criminal records. To the extent Customer elects to upload special categories of data, Customer does so at its own risk.

Nature & Purpose of Processing operations

The personal data processed may be subject to the following basic processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, consult, use, align or combine, block, erase or destruct, disclose by transmission, disseminate or otherwise make available Customer Data as described herein, as strictly necessary and required to provide the Software and otherwise in accordance with Customer's instructions.

Specifically, processing operations include:

- Processing of name and e-mail addresses to provide login credentials, processing of name and e-mail address to provide support and help desk, storage of login credentials of users for authentication purposes.
- Hosting Customer environment which contains Data.

Duration of Processing

The Data may be processed during the Term of the Agreement and any additional period which it is retained pursuant to Section 1.9 of Annex 1 (Data Processing Addendum).