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**" shall mean any and all applicable data protection and privacy laws including, where applicable, EU Data Protection Law.

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

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

"**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and (iii) any and all EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

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 Applicable Data Protection Law, (c) that has executed standard contractual clauses adopted or approved by the European Commission. Where OneTrust LLC is party to the Agreement, the Standard Contractual Clauses at https://www.onetrust.com/legal-sccs shall automatically be deemed to be a part of the Agreement, with Customer as the "Data Exporter." Alternatively Customer may enter into the Standard Contractual Clauses with OneTrust LLC by executing the pre-signed version at https://www.onetrust.com/legal-sccs and emailing a copy to legal@onetrust.com. The Parties may also agree to implement any other valid transfer mechanism then in existence.

If any Data originates from any country (other than an EEA country) with laws imposing data transfer restrictions and Customer has informed OneTrust of such data transfer restrictions, Customer and OneTrust shall ensure an appropriate transfer mechanism is in place, as mutually agreed upon by both Parties, before transferring or accessing Customer Data outside of such country. For the avoidance of doubt, this transfer restriction does not pertain to Authorized Users who have access to the Software and Customer Data, and OneTrust shall not be held responsible for actions of Authorized Users. Authorized Users shall not be entitled to use the Software in any country with data localization laws that would require Customer's Environment to be hosted in said country.

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 (as specified in Article 32 of the EU General Data Protection Regulation) 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. 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 details of any change in subprocessors at least 30 days' prior to any 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 the Agreement 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 grounds relating to data protection. 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, processor assists the controller by appropriate technical and organisational measures, insofar as this is possible, OneTrust shall provide reasonable and timely assistance to Customer (at Customer's expense at Customer's expense where the scope, frequency or volume of requested assistance exceeds that which OneTrust could have reasonably foreseen or anticipated before entering into the Agreement, to be agreed in advance) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection,

erasure and data portability, as applicable); 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. *Data Protection Impact Assessment:* OneTrust shall provide Customer with reasonable cooperation (at Customer's expense at Customer's expense where the scope, frequency or volume of requested assistance exceeds that which OneTrust could have reasonably foreseen or anticipated before entering into the Agreement, to be agreed in advance) to enable Customer to conduct any data protection impact assessment that it is required to undertake under 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.

1.9. *Deletion or Return of Data:* Following termination or expiry 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. *Audit:* 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 by Customer (or its designee) during business hours, and without interrupting OneTrust's business operations, in order to ascertain compliance with the obligations set forth in this Data Processing Addendum. For the avoidance of doubt, the scope of such audit shall be limited to documents and records allowing the verification of OneTrust's compliance with the obligations set forth in 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.

Appendix 1: OneTrust Information Security Controls

OneTrust technical and organizational measures for data protection have been organized and implemented according to ISO 27001 and include the following types of controls:

- A.5: Information security policies
- A.6: Organization of information security
- A.7: Human resource security
- A.8: Asset management
- A.9: Access control
- A.10: Cryptography
- A.11: Physical and environmental security
- A.12: Operations security
- A.13: Communications security
- A.14: System acquisition, development and maintenance
- A.15: Supplier relationships
- A.16: Information security incident management
- A.17: Information security aspects of business continuity management
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws

OneTrust maintains the following policies and procedures in support of its privacy and security program:

Information Security Policies

To provide management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

Organization of Information Security

To establish a framework for initiating and controlling information security implementation and operations at OneTrust.

Human Resource Security

To ensure that all workforce members are well suited for, and understand, their roles and responsibilities. To ensure that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations. To ensure that the organization's interests are protected throughout the employment process, from pre-employment to termination.

Asset Management

To identify OneTrust's information assets, and to define and assign appropriate responsibilities for ensuring their protection. To ensure an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization. To prevent the unauthorized disclosure, modification, removal or destruction of information stored on media.

Access Control

Provides the framework for user, system and application access control and management, and user responsibilities. To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

Cryptography

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

Physical and Environmental Security

To prevent unauthorized physical access, damage and interference with OneTrust's information and information processing facilities. To prevent loss, damage, theft or compromise of OneTrust's assets, and interruption of its operations.

Operations Security

To ensure that information and information processing facilities are operated securely, protected from malware and loss of data. To ensure that security events are recorded appropriately. To ensure that operational system integrity is maintained, and exploitation of technical vulnerabilities is avoided.

Communications Security

To establish controls for the protection of information in networks and their associated facilities. To ensure the security of information being transferred within OneTrust and with external parties.

System Acquisition, Development and Maintenance

To establish information security as a vital part of information systems throughout the entire information lifecycle, including designing information security into the development of such systems. To ensure that sufficient controls are established to protect data used in testing.

Supplier Relationships

To ensure protection of OneTrust assets that are accessible by suppliers. To maintain an agreed-upon level of information security and service delivery in accordance with supplier agreements.

Information Security Incident Management

To ensure a consistent and effective approach to managing information security events, including incidents and weaknesses.

Information Security Aspects of Business Continuity Management

To embed information security continuity in OneTrust's business continuity management systems. To ensure availability of information processing facilities. Third party integrations are provided by third parties and not subject to OneTrust's security program.

Appendix 2: Details on the processing of Customer 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 privacy management 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 ____IP id _and audit trail log_____

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, 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.

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 Customer Data.

Duration of Processing

The personal 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).