onetrust

OneTrust Data Processing Addendum

Last Updated: February 1, 2023

This Data Processing Addendum ("**Addendum**") supplements the agreement between Customer and OneTrust into which it is incorporated by reference ("**Agreement**").

1. Definitions.

Unless otherwise defined below, all capitalized terms in this Addendum shall have the meaning given to them in the Agreement:

"**Adequate Country**" a country that the European Commission, the Information Commissioner's Office or the Federal Data Protection and Information Commissioner (as applicable) have determined as ensuring an adequate level of protection for their respective area of competence.

"**Applicable Data Protection Law**" applicable data protection and privacy laws including, where applicable, US Data Protection Law, EU Data Protection Law, UK Data Protection Law and Swiss Data Protection Law.

"**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**" 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.

"**EEA**" European Economic Area.

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Directive); and (c) any EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

"**Swiss Data Protection Law**" the Swiss Federal Act on Data Protection (FADP) of 1992 until the December 31, 2022, and from January 1, 2023, onward, the Revised Swiss Federal Act on Data Protection (Revised FADP) of 2020, as amended or superseded from time to time.

"**UK Data Protection Law**" 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 (UK DPA) and the UK GDPR (Retained Regulation (EU) 2016/679 (UK GDPR) pursuant to section 3 of the European Union (Withdrawal) Act 2018), as amended or superseded from time to time.

"**US Data Protection Law**" (a) the California Consumer Privacy Act of 2018 (CCPA), as amended and integrated by the California Privacy Rights Act of 2020 (CPRA) and following implementing regulations; (b) the Virginia Consumer Data Protection Act of 2021 (VCDPA); (c) the Colorado Privacy Act of 2021 (CPA); (d) the Connecticut Data Privacy Act of 2022 (CTDPA); and (e) the Utah Consumer Privacy Act of 2022 (UCPA); in each case as amended or superseded from time to time.

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. Each Party shall comply with its respective obligations under Applicable Data Protection Law.

3. International Transfers & Data Localization Laws.

3.1. For any Data protected under EU Data Protection Law, OneTrust shall only transfer the Data outside of the EEA or an Adequate Country subject to 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 that has (a) achieved binding corporate rules authorisation in accordance with EU Data Protection Law; and (b) executed standard contractual clauses adopted or approved by the European Commission.

3.2. If in the course of providing the Services, Data governed by EU Data Protection Law is transferred to OneTrust outside of the EEA to a country which is not an Adequate Country, (a) the applicable standard contractual clauses ("**SCC's**") at https://www.onetrust.com/legal-sccs ("**SCC's Webpage**") shall be deemed incorporated into the Agreement; or (b) if Customer requires a fully executed version, it can countersign the applicable pre-signed version on the SCC's Webpage and email a copy to legal@onetrust.com.

3.3. 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 Support Portal. OneTrust shall (a) notify Customer by email or through the Support Portal if OneTrust is unable to comply with its legal or contractual obligations related to international transfers under EU Data Protection Law; and (b) suspend the applicable transfers of Data until it is able to comply with such legal and contractual obligations.

3.4. 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 Cloud Services, 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 Cloud Services 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).

3.5. For Data originating from the United Kingdom ("UK") or Switzerland references in this Section 3 to: (a) the "EEA" shall be replaced with the "UK" or "Switzerland", as applicable; (b) "EU Data Protection Law" shall be replaced with "UK Data Protection Law" or "Swiss Data Protection Law", as applicable; and (c) the "European Commission" shall be replaced with the "Information Commissioner's Office" or the "Federal Data Protection and Information Commissioner", as applicable.

4. Security.

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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 from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "Privacy Breach").

4.2. All penetration or other testing conducted by Customer shall be done in a designated testing environment and pursuant to mutual written 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 ("**ISO Certifications**"). 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 ("**SOC Report**").

5. Subprocessing.

5.1. 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 (a) 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; (b) 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 (c) remain liable for any breach of this Addendum that is caused by an act, error or omission of its subprocessor.

5.2. Customer may object to OneTrust's appointment of a subprocessor prior to its appointment, provided such objection is based on reasonable data protection grounds. In such event, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

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: (a) any request from a data subject to exercise its rights under Applicable Data Protection Law; and (b) 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.

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 (a) conduct any data protection or transfer impact assessments that it is required to undertake under Applicable Data Protection Law; and (b) consult competent supervisory authorities prior to processing where required by Applicable Data Protection Law.

8. Privacy Breaches.

8.1. If it becomes aware of a Privacy 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 Privacy Breach and shall keep Customer informed of all material developments in connection with the Privacy Breach.

8.2. Customer acknowledges that in the event of a Privacy Breach impacting a subprocessor of OneTrust, Customer may receive notification directly from the subprocessor in accordance with the Standard Contractual Clauses between OneTrust and such subprocessor. In such event, Customer agrees to provide any reasonable co-operation or assistance required by OneTrust and the subprocessor in order to facilitate such notification.

9. Deletion or Return of Data.

Following termination of the Agreement, Customer shall have sixty (60) days to export its Data from the Cloud Services 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: (a) OneTrust is required by applicable law to retain some or all of the Data; or (b) 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.

10. Review & Audit.

10.1. Customer agrees that to the extent applicable, the ISO Certifications and SOC Report (or industry standard comparable reports) shall be used to satisfy any audit requests. If Customer requires additional information, including information to review compliance with this Addendum, OneTrust shall, upon reasonable notice from

Customer (no less than forty-five (45) days) and payment of a reasonable fee, not more than once a year (unless there is a material Privacy Breach, in which case a second audit is permitted), allow its procedures and documentation not otherwise addressed in OneTrust's SOC Report or ISO Certifications 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 obtain the information reasonably necessary to assess compliance with this Addendum.

10.2. 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 Addendum and shall not include financial records of OneTrust or any records concerning OneTrust's other customers.

10.3. Remote audits shall be utilized where possible, with on-site audits occurring only where a walkthrough of the premises is required. 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.

10.4. Where required under CCPA, Customer has the right to: (a) take reasonable and appropriate steps to ensure OneTrust processes Data received in connection with the Agreement in a manner consistent with Customer's obligations under Applicable Data Protection Laws; and (b) upon reasonable notice to OneTrust, take reasonable and appropriate steps to stop and remediate OneTrust's unauthorized use of Data received in connection with the Agreement.

11. Transparency Reports.

11.1. 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/.

11.2. OneTrust shall: (a) review the legality of the Legal Requests and to challenging them where lawful and appropriate; and (b) where the Legal Request is incompatible with Art. 46 of the GDPR, or any other relevant provision for the lawful transfer of personal data, to inform the public authority of the same (in each case to the extent required by the Applicable Data Protection Law governing the Legal Request).

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 assigns 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 principles governing information security and cybersecurity to secure information in any form.
- 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 and uses end-to-end encryption and encrypts data in transit and at rest.
- 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.

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.

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's employees, contractors, agents, consultants, vendors, customers and web visitors, whose personal data is processed by OneTrust for the purposes of providing and Customer using the Services, including end users using or interacting with the Services.

Categories of personal data processed.

Personal data typically includes: (a) identification data such as user account information including name, username, email, contact details, job title, and IP address; (b) information of end users interacting with the Services, such as IP address, UID, user preferences, or geolocation (optional); (c) information voluntarily disclosed by the data subjects when using the Services; and (d) any personal data submitted to the Services or to OneTrust or its Affiliates in the course of performing the Services.

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 sensitive data, Customer does so at its own risk.

Purpose & Nature of Processing operations.

Personal data is primarily processed for the purpose of providing the Services.

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 Data as described herein, as strictly necessary and required to provide the Services 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 IP to access and interact with the Cloud Services, 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 9 of the Data Processing Addendum).