onetrust

OneTrust® Data Processing Addendum

Last Updated: June 3, 2024

This Data Processing Addendum ("**DPA**") 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 DPA shall have the meaning given to them in the Agreement:

"**Adequate Country**" a country that The European Commission, the United Kingdom's ("**UK**") Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner (as applicable based on respective area of competence) has determined as ensuring an adequate level of data protection.

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

"**Authorized Affiliate**" a Customer Affiliate which is an Authorized User under the Agreement and is subject to Applicable Data Protection Law of a jurisdiction requiring the signature of a binding contract between the controller and the processor.

"**Controller**", "**data subject**", "**personal data**", "**processor**", and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law. Any references in this DPA to "personal data", "processor", and "controller" shall be deemed to include their equivalent concepts under the CCPA and CPRA, respectively, "personal information", "service provider", and "business".

"**Data Privacy Framework**" the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework, set forth by the U.S. Department of Commerce and the European Commission, the UK Government, and the Swiss Federal Administration.

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and (c) any EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

"**Processing**" and "**Process**" any operation or sets of operations performed upon the Data by automated means or otherwise, including the sell or share, combination, retention, use, or disclosure of Data.

"**Swiss Data Protection Law**" the Swiss Federal Act on Data Protection (Revised FADP) of 2020, as amended or superseded from time to time.

"**Third Country**" a country outside of the EEA, the UK or Switzerland (as applicable) which is not an Adequate Country.

"**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.

2.1. Customer (on behalf of itself and its Authorized Affiliates) (the controller) appoints OneTrust as a processor to process the personal data described in Appendix 2 (the "Data") for the purposes of providing the Services to Customer and complying with OneTrust's obligations under the Agreement as further described in Appendix 2 (or as reasonably instructed in writing by Customer, to the extent consistent with (and not in addition to) the terms of the Agreement) (the "Permitted Purpose"). Customer shall ensure that its instructions comply with Applicable Data Protection Law and that the Data submitted to OneTrust is limited to what is necessary in relation to the purpose for which it is processed.

2.2. OneTrust shall not Process the Data outside the direct business relationship between the Parties and for any purpose (including any commercial purpose) other than the Permitted Purpose, or as otherwise permitted by Applicable Data Protection Law.

2.3. OneTrust shall promptly notify Customer if it determines that (a) a Customer instruction infringes Applicable Data Protection Law, or (b) it can no longer meet its obligations under Applicable Data Protection Law.

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

3. International Transfers & Data Localization Laws.

3.1. If any Data is protected under EU Data Protection Law, then OneTrust shall only transfer such Data to a Third Country subject to measures to ensure the transfer is compliant with EU Data Protection Law. Such measures may include transferring the Data to a recipient that has (a) achieved binding corporate rules authorisation in accordance with EU Data Protection Law; or (b) executed standard contractual clauses adopted or approved by the European Commission.

3.2. If Data protected under EU Data Protection Law is transferred to OneTrust in a Third Country, the applicable standard contractual clauses ("SCCs") at https://legal.onetrust.com/ shall be deemed entered into by the Parties and incorporated into the Agreement. If Customer requires a fully executed version of the SCCs, it can countersign the applicable pre-signed SCCs from https://legal.onetrust.com/ and email a copy to legal@onetrust.com.

3.3. Prior to transferring Data to a 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 obligations.

3.4. Customer acknowledges that OneTrust has self-certified its adherence to the Data Privacy Framework. In the event that OneTrust withdraws from the Data Privacy Framework or if the Data Privacy Framework is otherwise invalidated in any of its parts, (a) OneTrust will inform Customer, and (b) any affected transfers of Data will be subject to such measures as are necessary to ensure their compliance with Applicable Data Protection Law, in accordance with Section 3.1. For the avoidance of doubt, a transfer of Data to an entity in the United States certified under the Data Privacy Framework shall be deemed a transfer to an Adequate Country, to the extent that the framework is based on an adequacy decision by the relevant authority.

3.5. For Data originating from the United Kingdom ("UK") or Switzerland references in this Section 3 to: (a) "EU Data Protection Law" shall be replaced with "UK Data Protection Law" or "Swiss Data Protection Law", as applicable;

and (b) the "European Commission" shall be replaced with the "Information Commissioner's Office" or the "Federal Data Protection and Information Commissioner", as applicable.

3.6. If any data originates from a Third 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 tenant 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).

4. Security & Confidentiality

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 (a) accidental or unlawful destruction, and (b) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Privacy Breach**").

4.2. All penetration or other testing conducted by Customer on the Services shall be done in a designated testing environment pursuant to a written agreement between the Parties. OneTrust LLC's Information Security Management System (ISMS) is ISO/IEC 27001:2022 and ISO/IEC 27017:2015 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 and its applicable Affiliates ("**SOC Report**").

4.3. OneTrust shall process the Data as Confidential Information and shall only share it with authorised persons who need access to the Data for the Permitted Purpose and are subject to a statutory or contractual duty of confidentiality or as explicitly permitted under the Agreement.

5. Subprocessing.

5.1. OneTrust maintains a list of its subprocessors at https://my.onetrust.com/s/list-of-subprocessors ("**Subprocessors List**"). Customer consents to OneTrust engaging subprocessors to process the Data for the Permitted Purpose. OneTrust shall (a) enter into a written contract with each subprocessor requiring the subprocessor to protect the Data in accordance with Applicable Data Protection Law, including privacy obligations no less protective of Data than this DPA; and (b) be responsible for any breach of this DPA caused by its subprocessors.

5.2. OneTrust shall update the Subprocessors List at least thirty (30) days in advance of any change to the list, except to the extent shorter notice is required due to an emergency. Customer may sign-up to e-mail notifications of any change to the Subprocessors List via the Support Portal.

5.3. Customer may object to OneTrust's appointment of a subprocessor within thirty (30) days following OneTrust's notification of a change in the Subprocessor List, provided such objection is based on reasonable data protection grounds. Following such an objection (a) OneTrust will, if possible, either reasonably assist Customer to configure the Services to disable the use of the objected-to subprocessor, or use commercially reasonable efforts to replace the subprocessor, and (b) in the event OneTrust has not disabled use of or replaced the objected-to subprocessor within sixty (60) days following notice of Customer's objection, Customer may terminate the affected Services by providing OneTrust notice (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 to enable Customer to respond to: (a) any request from a data subject to exercise its rights under Applicable Data Protection Law related to Customer's use of the Services; 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 under the Agreement (each, a "**Data Subject Request**"). To the extent Customer cannot address a Data Subject Request through its use of the Services, Customer will be responsible for the costs of any additional assistance provided by OneTrust to respond to such Data Subject Request. If OneTrust directly receives a Data Subject Request, OneTrust will, to the extent legally permitted, promptly provide Customer with details of the request, and will not respond to the request unless required by Applicable Data Protection Law.

7. Consultation and Assistance.

Taking into account the nature of the processing, and to the extent required by Applicable Data Protection Law, OneTrust shall provide Customer with reasonable cooperation and such information available to OneTrust (that is not available to Customer) to enable Customer to (a) conduct a data protection or transfer impact assessment related to Customer's use of the Services; and (b) consult competent supervisory authorities prior to a processing operation under the Agreement.

8. Privacy Breaches.

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.

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, which shall be deleted in accordance with its security procedures, provided that OneTrust shall continue to protect such Data in accordance with its obligations herein.

10. Review, Assessment and Audit.

10.1. To the extent applicable, OneTrust's latest ISO Certifications and SOC Report (or industry-standard comparable certifications and third-party audit reports) shall be used to satisfy any information or audit requests. If Customer requires additional information to review compliance with this DPA or ensure OneTrust processes the Data in accordance with Customer's obligations under Applicable Data Protection Law, OneTrust shall, upon reasonable notice from Customer (no less than forty-five (45) days) and subject to a reasonable fee (taking into account the resources expended and the duration of an audit), allow its procedures and documentation not otherwise addressed in OneTrust's ISO Certifications or SOC Report to be inspected by Customer (or its designee, agreed by the Parties) ("**Audit**"). Following OneTrust's receipt of Customer's notice, the Parties shall mutually agree on the scope and timing of the Audit, taking into consideration resource availability.

10.2. Customer (and where applicable, together with its Authorized Affiliates) shall only be permitted to conduct one Audit per year (unless there is a material Privacy Breach, in which case a second Audit is permitted). Audits must occur during OneTrust's business hours, and without interrupting OneTrust's business operations. 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 an Audit to such supervisory authority. Audits shall not include financial records of OneTrust or any records concerning OneTrust's other customers.

10.3. Upon reasonable notice to OneTrust, Customer may take reasonable and appropriate steps to stop and remediate OneTrust's unauthorized use of Data received in connection with the Agreement to the extent required under Applicable Data Protection Law.

onetrust

11. Transparency Reports.

11.1. OneTrust will not disclose or allow any public authorities to access any Data unless required by law. OneTrust's policy on Data-related requests from public authorities ("**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 a Legal Request and challenge the request where lawful and appropriate; and (b) where the Legal Request is incompatible with Applicable Data Protection Law, inform the public authority of the incompatibility (in each case to the extent required by the Applicable Data Protection Law governing the Legal Request).

12. Authorized Affiliates.

12.1. To the extent required by Applicable Data Protection Law, Customer enters into this DPA on behalf of itself and, on behalf of its Authorized Affiliates who are controllers of Data processed by OneTrust. Except where expressly indicated otherwise, and only where applicable, for the purposes of this DPA only, "**Customer**" shall include Customer and Authorized Affiliates.

12.2. All rights of Authorized Affiliates under this DPA shall be exercised by Customer on behalf of the Authorized Affiliate and only Customer (and not Authorized Affiliates) shall be permitted to directly enforce this DPA (including on behalf of an Authorized Affiliate), except where Applicable Data Protection Law requires an Authorized Affiliate to enforce directly.

12.3. For the avoidance of doubt, each Party's and its Affiliates' total aggregate liability to the other Party and its Affiliates, arising out of or relating to the Agreement (including this DPA and any addendum between OneTrust and an Authorized Affiliate) shall be calculated on a total aggregate basis in accordance with the liability provisions of the Agreement. For purposes of the liability provisions in the Agreement, Authorized Affiliates' losses shall be considered Customer's losses.

onetrust

Appendix 1: OneTrust Information Security Controls

OneTrust has organized and implemented technical and organizational measures for personal data protection according to ISO 27001, 27017 and 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 may 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.

onetrust

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

onetrust

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 processed by OneTrust 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.

Customer may, at its sole discretion, submit special categories of personal data to the Services, including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, medical and criminal records, genetic data, or biometric data for the purposes of uniquely identifying a natural person.

Notwithstanding the foregoing, Customer shall not submit PCI-DSS-protected data (including but not limited to magnetic strips and chip data, CAV2/CVC2/CVV2/CID4 numbers, and personal identification numbers (PINs)) ("**Financial Data**"), or Protected Health Information (as the term is defined in the Health Insurance Portability and Accountability Act of 1996). If Customer wishes to instruct OneTrust to process Financial Data or Protected Health Information, Customer shall inform OneTrust in advance so the Parties can agree on the appropriate safeguards applicable to such processing (and the fees for such services).

Purpose & Nature of Processing operations.

Personal data is primarily processed for the purpose of providing the Services to Customer under the Agreement and complying with OneTrust's obligations under the Agreement.

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 initiated by users through use of the Services.
- 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 DPA.