onetrust

Amendment to Incorporate Standard Contractual Clauses

Last Updated: February 1, 2023

This Amendment to the Agreement is entered into between Customer and the OneTrust entity entering into or that has entered into the Agreement with Customer ("**OneTrust**") and that is a signatory to this Amendment (each a "**Party**", collectively, the "**Parties**") to incorporate Standard Contractual Clauses (the "**Amendment**").

In consideration of the mutual covenants and agreements contained herein, the Parties hereto agree as follows:

Definitions

Unless otherwise defined in the Agreement, the terms listed below and used in this Amendment shall have the following meanings:

"**Agreement**" (a) the OneTrust Master Terms of Service at https://legal.onetrust.com/ together with any Order Forms and other documents incorporated by reference into the Terms; or (b) the preexisting signed agreement that formed the basis of the commercial transaction between the Parties.

"**Customer**" (a) the Customer identified in the signature block below; or (b) where the SCCs are automatically deemed incorporated into the Agreement, the Customer identified on the Order Form.

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and (c) any and all EU Member State laws made under or pursuant to any of the foregoing; in each case as amended or superseded from time to time.

"**EU SCCs**" the standard contractual clauses set out by the decision (EU) 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**IDTA**" the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office under S119A(1) Data Protection Act 2018, Version B1.0, in force March 21, 2022.

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1, 2023 onward, the Revised Swiss Federal Act on Data Protection (Revised FADP) of September 2020, as amended or superseded from time to time.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

All other capitalized terms used but not defined in this Amendment shall have the meanings given to them in the Agreement.

onetrust

Amendment

1. EU SCCs.

The Agreement is hereby amended to include and incorporate Module Two (transfers controller to processor, where Customer is a controller of the transferred Data) and Module Three (transfers processor to processor, where Customer is a processor of the transferred Data) of the EU SCCs by reference, which are completed as follows:

1.1. Docking clause. The option in Clause 7 will not apply.

1.2. Instructions. For the purposes of Clause 8.1(b), the Parties agree that the documented instructions from Customer, including those provided on behalf of the controller, are set out in the Agreement and the Data Processing Addendum, including with respect to international transfers of data.

1.3. Certification of Deletion. Pursuant to Clause 8.5, the Parties agree that OneTrust will certify to Customer that it has deleted the personal data upon Customer's written request.

1.4. Audits. It is understood by the Parties that the audit rights set out in Clause 8.9 shall be performed in accordance with the provisions regarding audits in the Agreement or in the Data Processing Addendum.

1.5. Subprocessors. In Clause 9(a), Option 2 will apply and OneTrust will inform Customer of changes in the subprocessors thirty (30) days prior to the change in accordance with the terms set out in the Agreement or the Data Processing Addendum.

1.6. Redress. In Clause 11, the optional language will not apply.

1.7. Liability. The Parties agree that OneTrust's liability to Customer under Clause 12 shall be subject to the liability limitations and exclusions contained in the Agreement and/or the Data Processing Addendum.

1.8. Governing law. For the purposes of Clause 17 (Option 1), the Parties agree that the EU SCCs will be governed by the laws of the Republic of Ireland.

1.9. Forum and jurisdiction. For the purposes of Clause 18(a) and (b), the Parties agree that any dispute arising from these EU SCCs shall be resolved by the courts of the Republic of Ireland.

1.10. Annexes. Annexes I, II and III to the EU SCCs shall be deemed completed with the information set out in Appendix 1 to this Amendment.

1.11. Conflict. In the event of any conflict or inconsistency between the body of this Amendment or the Agreement to which it is incorporated and the SCCs, the SCCs shall prevail.

2. UK SCCs.

To the extent any personal data transferred to OneTrust under the Agreement is governed by UK Data Protection Law and originates from the United Kingdom, the IDTA will be deemed executed and it shall integrate and supplement the EU SCCs as follows:

2.1. Parties. Part 1, Table 1 is completed with the details set out in Appendix 1 to this Amendment.

2.2. SCCs, Modules and Clauses. Part 1, Table 2 is completed with the information set out in Section 1 above.

2.3. Annexes. The "Appendix Information" mentioned in Part 1, Table 3 is completed with the information set out in Appendix 1 to this Amendment.

2.4. Ending. OneTrust, as the Importer, may end this IDTA in accordance with Section 19 of the IDTA.

3. Swiss SCCs.

To the extent any personal data transferred to OneTrust under the Agreement is governed by Swiss Data Protection Law and originates from Switzerland, the EU SCCs shall apply with the following adaptations:

3.1. Place of jurisdiction. The term "Member State" shall not be interpreted in such a way to exclude data subjects in Switzerland from the possibility of suing their rights in Switzerland in accordance with Clause 18(c) of the EU SCCs.

3.2. Supervisory Authority. The Federal Data Protection and Information Commissioner of Switzerland shall be competent in accordance with Clause 13 of the EU SCCs where the transfer of personal data is subject to Swiss Data Protection Law.

4. This Amendment shall terminate and replace any prior versions of the standard contractual clauses which are part of the Agreement immediately prior to this Amendment becoming effective.

5. Except as set forth in this Amendment, the Agreement is unaffected and shall continue in full force and effect in accordance with its terms, and the SCCs shall be otherwise subject to the terms and conditions of the Agreement. If there is conflict between this Amendment and the Agreement or any earlier amendment, the terms of this Amendment will prevail.

6. This Amendment shall only be valid if Customer's pre-existing Agreement is with OneTrust LLC, OT Technology Inc., Convercent Inc. or OT (Australia) Privacy Limited.

7. This Amendment shall become effective (i) upon delivery of a fully executed copy to legal@onetrust.com and OneTrust's confirmation of receipt thereof; or (ii) where the SCCs are automatically deemed incorporated into the Agreement, from the date of the first transfer of Data to a country outside of the EEA, the UK, Switzerland, or an Adequate Country, as applicable.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment as of the latest signature date below. Such signatures on this Amendment shall constitute acceptance and signature of the SCCs including, where applicable, the IDTA and the Swiss amendments.

onetrust

Appendix 1

I. Details of processing

A. List of Parties.

	Data Exporter	Data Importer
Name & Trading name (if different)	Customer identified in the signature block or in the Order Form	OneTrust entity that is part to the Agreement as identified in the signature block
Official registration number (if any) (company number or similar identifier)	As identified in the signature block or in the Order Form	As identified in the signature block
Address	As identified in the signature block or in the Order Form	As identified in the signature block
Contact person's name, position and contact details	As identified in the signature block or in the Order Form	Linda Thielová, DPO, dpo@onetrust.com
Activities relevant to the data transferred under the EU SCCs	As set out in the Agreement	As set out in the Agreement
Signature & date	The EU SCCs will be deemed executed upon execution of this Amendment	The EU SCCs will be deemed executed upon execution of this Amendment
Role	Controller/Processor, as set out in the Agreement	Processor/Sub-processor, as set out in the Agreement

B. Description of Transfer.

Categories of data subjects *whose personal data is transferred*

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

Categories of personal data *transferred*

The personal data transferred is that provided by or on behalf of Customer and processed by OneTrust while providing the Services. The 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.

Sensitive data transferred (if applicable) *and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*

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.

The frequency of the transfer *(e.g., whether the data is transferred on a one-off or continuous basis)*

Continuous basis during the provision and use of the Services.

Nature of the processing The personal data processed may be subject to the following processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, and consult.
Purpose(s) of the data transfer *and further processing* Personal data is processed for the purposes described in the Agreement and/or Order Form (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**").
The period for which the personal data will be retained, *or, if that is not possible, the criteria used to determine that period* The personal data will be processed during the Term of the Agreement and any additional period for which it is retained pursuant to the Data Processing Addendum to the Terms, or any other provisions or agreement on data processing entered into by the parties pursuant to the Agreement.
For transfers to (sub-) processors, *also specify subject matter, nature and duration of the processing* The identity of the subprocessors engaged by OneTrust, and the subject matter, nature and duration of the processing performed by the subprocessors is set forth at https://my.onetrust.com/s/list-of-subprocessors.

C. Competent Supervisory Authority.

Means the competent Supervisory Authority of the EU Member State determined in accordance with Clause 13.

II. Technical and Organisational Measures including Technical and Organisational Measures to ensure the Security of the Data

Without prejudice to the security controls applicable to the Services in accordance with the Agreement, OneTrust holds the certifications and has implemented the Supplementary Measures described below.

A. Certifications.

Certifications & Audit Reports	Detail
ISO/IEC 27001:2013 Information Security Management Systems (ISMS) Certification	OneTrust LLC's ISMS is ISO 27001:2013 certified. The certification verifies that OneTrust adheres to the ISO 27001 requirements for establishing, implementing, maintaining and continually improving the ISMS.
ISO/IEC 27701:2019 Privacy Information Management System (PIMS) Certification	OneTrust LLC's PIMS is ISO 27701:2019 certified. The certification verifies that OneTrust adheres to the ISO 27701 requirements and guidance for establishing, implementing, maintaining, and continually improving the PIMS.
SOC 2 Type 2 report	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. The report also maps the security, availability and confidentiality services criteria to the ISO 27001:2013 certification and GDPR requirements.
Payment Card Industry Data Security Standard (PCI-DSS)	Customers can elect to purchase from OneTrust a Cloud Services Environment which has been certified to align with the PCI-DSS v.3.2.1 requirements.

B. Supplementary Measures.

OneTrust maintains the following supplementary measures based on the EDPB's non-binding guidance:

Technical Measures

- OneTrust uses end-to-end encryption.
- OneTrust encrypts data in transit and at rest.

Additional Contractual Measures

- Transparency.
    - Upon request, OneTrust will take reasonable commercial efforts to provide information (to the best of its knowledge) on the access to data by public authorities, including in the field of intelligence, to evaluate whether the legislation complies with the EDPB European Essential Guarantees, in the destination country.
    - OneTrust certifies that: (1) it has not built, and will not purposefully build, backdoors or similar programming that public authorities could use to access its personal data or information systems; (2) it has not changed, and will not purposefully change, its processes in a manner that facilitates public authorities' access to data; and (3) national law or government policy do not require OneTrust to create or maintain back doors or to facilitate access to personal data or systems or for it to be in possession or to hand over the encryption key (subject to change based on legislative developments).
    - OneTrust will notify the customer if OneTrust is unable to comply with the legal obligations and/or contractual commitments related to international transfers and as a result with the required standard of "essentially equivalent level of data protection."
- Specific Actions.
    - OneTrust shall: (i) review the legality of the Legal Requests and to challenging them where lawful and appropriate; and (ii) 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).

Organisational Measures

- Internal policies for governance of transfers.
    - OneTrust has internal policies for the governance of international transfers, including clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data, as well as data mapping and the implementation of lawful transfer mechanisms.
- Transparency and Accountability.
    - OneTrust has documented policies and procedures for handling and responding to government or law enforcement requests for customer data.
    - OneTrust documents and records the requests for access received from public authorities and the responses provided and can provide this information to customers upon request.
    - OneTrust makes available, and regularly maintains, a Government Data Request Policy & Transparency Report webpage that describes its policies for government/law enforcement data requests and documents the number of public authorities' requests and our responses, available at https://www.onetrust.com/transparency-report/.

- Adoption and Review of Internal Policies.
    - OneTrust monitors legal and regulatory developments related to cross-border transfers of personal data outside the EU/EEA to ensure that the data continues to enjoy an essentially equivalent level of data protection.
    - OneTrust regularly reviews internal policies to assess the appropriateness/effectiveness of supplementary measures and to identify and implement additional or alternative solutions when necessary. Where applicable and appropriate, OneTrust will work diligently to implement any additional required technical, organizational, and/or contractual measures.
- Organisational Methods and Data Minimisation Measures.
    - OneTrust has adopted organisational controls to comply with the accountability principle, including strict and granular data access, confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits, and enforced through disciplinary measures.
    - OneTrust practices data minimisation to limit the exposure of personal data to unauthorised access.
    - OneTrust has adopted best practices to appropriately and timely involve and provide access to information to the DPO and legal and internal auditing services on matters related to international transfers of personal data transfers.
- Data Security/Privacy Standards/Best practices.
    - OneTrust has adopted strict data security and data privacy policies, based on international standards (i.e., ISO norms) and best practices with due regard to the state of the art, in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it.
- Measures related to OneTrust's subprocessors.
    - OneTrust regularly reviews and monitors subprocessors to ensure that they maintain appropriate technical and organisational measures, which effectively meet the Applicable Data Protection Law requirements.
    - OneTrust must impose on each subprocessor data protection obligations that require it to protect the personal data to the standard required by Applicable Data Protection Law.
    - To receive notifications of changes in the subprocessors, log in to your my.onetrust.com account and sign-up for notifications at the Subprocessors List page.
    - OneTrust and its sub-processors have entered into the relevant SCCs to ensure the lawfulness of the personal data transfers to countries outside of the EU, Switzerland and the UK.
    - For more information about Subprocessors' controls, access the OneTrust Subprocessor Controls Datasheet.

III. List of Subprocessors

Customer has consented to OneTrust using the subprocessors (including its Affiliates) listed in the Subprocessors List.