

Ontra Data Processing Addendum

Last Updated: December 17, 2024

This Data Processing Addendum (this “DPA”) is entered into between the Customer identified in the Order Form and Ontra, and is governed by the Ontra Customer License General Terms and Conditions (the “General Terms”). By executing the Order Form, Customer agrees to the terms and conditions set forth in this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates, if any. This DPA incorporates the terms of the General Terms, and any terms not defined in this DPA shall have the meaning set forth in the General Terms.

Subject to the terms and conditions set forth herein, the Parties agree as follows:

1. Definitions

- 1.1 “Authorized Sub-Processor” means a Sub-Processor (as defined below) who is either (i) listed at <https://trust.ontra.ai/subprocessors> (the “List”) or (ii) subsequently authorized under Section 3.1(b) or Section 3.2 of this DPA, and that may process Customer Personal Data in connection with the provisions of those services.
- 1.2 “Data Protection Laws” means any applicable laws and binding regulations in any relevant jurisdiction relating to the processing of Personal Data including: (i) the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 *et seq.*), as amended by the California Privacy Rights Act of 2020 (“CCPA”) and other U.S. state comprehensive data protection laws (collectively, “US Data Protection Laws”); (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”) and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “UK GDPR”) (together, collectively, the “GDPR”); (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (vi) the Personal Data (Privacy) Ordinance (Chapter 486 of the laws of Hong Kong); in each case, as updated, amended or replaced from time to time. The terms “Data Subject”, “Personal Data”, “Personal Data Breach”, “processing”, “processor”, “controller”, and “supervisory authority”, “Third Country”, and any analogous terms, shall have the meanings set forth in the GDPR or under other applicable Data Protection Laws as the case may be.
- 1.3 “EU SCCs” means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 5.2 of this DPA.
- 1.4 “Ontra Group” means InCloud, LLC d/b/a Ontra (“Ontra”) and all of its Affiliates.
- 1.5 “Services” shall have the meaning set forth in the General Terms.
- 1.6 “Standard Contractual Clauses” means the EU SCCs and the UK SCCs.
- 1.7 “Sub-Processor” means a third-party engaged by Ontra to enable Ontra to perform its obligations under this DPA or the General Terms.
- 1.8 “UK SCCs” means the EU SCCs, as amended by the UK Addendum.

2. Relationship of the Parties; Processing of Data

- 2.1 The Parties acknowledge and agree that, except as set forth in Section 8 of this DPA, Ontra shall act as a processor in connection with the processing of Personal Data provided to Ontra by or on behalf of Customer through the Services. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer’s instructions will not cause Ontra to violate any Data Protection Laws. Customer shall ensure the accuracy, quality, and legality of (i) the Personal Data provided to Ontra by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides, or that are provided by any third party acting on its behalf and at its direction, to Ontra regarding the processing of such Personal Data. Customer shall not provide or make available to Ontra any Personal Data in violation of the General Terms or otherwise inappropriate for the nature of the Services, and Customer shall remain fully responsible for, and Ontra shall have no liability resulting from, such Personal Data.
- 2.2 Ontra shall not process Personal Data (i) for purposes other than those set forth in the General Terms and/or Exhibit 1 to this DPA, (ii) in a manner inconsistent with this DPA, the General Terms, or any other documented instructions provided by Customer, except where Ontra is required by applicable law to Process Personal Data in a different manner in which case Ontra will inform Customer of such applicable law unless prohibited from doing so by such applicable law), or (iii) in violation of Data Protection Laws to which Ontra is subject in connection with the delivery of the Services. Customer hereby instructs Ontra to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its lawful use of the Services. If Ontra determines it can no longer meet its obligations under Data Protection Laws, and to the extent required by Data Protection Laws, Ontra will notify Customer without undue delay.
- 2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit 1 to this DPA.
- 2.4 Ontra shall ensure that any employees authorized to process Personal Data are subject to appropriate confidentiality obligations that are no less restrictive than those contained in the General Terms.
- 2.5 Following completion of the Services or upon Customer’s written request, at Customer’s choice, Ontra shall return or delete Customer’s Personal Data, unless further storage of such Personal Data is required or authorized by applicable law, including Data Protection Laws. Customer acknowledges and agrees that (a) any request to return or delete Customer’s Personal Data may impact Customer’s ability to access or use the Services, and (b) Ontra has no liability for the occurrence or any subsequent effects arising from the circumstances described in the foregoing clause (a). If return or destruction is impracticable or prohibited by law, rule or regulation, Ontra shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to reasonably protect the Personal Data remaining in its possession, custody, or control. If Customer and Ontra

have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d), Clause 8.5 and Clause 16(d), as applicable, of the EU SCCs shall be provided by Ontra to Customer only upon Customer's request.

- 2.6 To the extent the CCPA applies to Customer's Personal Data processed within the Services ("California Personal Data"), the Parties acknowledge and agree that, except as set forth in Section 8 of this DPA, Ontra shall act as a service provider to Customer and Ontra is receiving Personal Data from Customer in order to provide the Services pursuant to the General Terms, which constitutes a Business Purpose (as defined by the CCPA). Customer shall disclose Personal Data to Ontra only for the limited and specified purposes described in Exhibit 1 to this DPA. With respect to California Personal Data, Ontra shall provide a level of protection for Personal Data as required by the CCPA, and shall not:
 - 2.6.1 "sell" or "share" (as defined by the CCPA) Personal Data provided by Customer under the General Terms;
 - 2.6.2 retain, use, or disclose Personal Data provided by Customer pursuant to the General Terms for any purpose, including a Commercial Purpose (as defined by the CCPA), other than as necessary for the specific purpose of performing the Services for Customer pursuant to the General Terms, or as otherwise set forth in the General Terms or as permitted by the CCPA;
 - 2.6.3 retain, use, or disclose Personal Data provided by Customer pursuant to the General Terms outside of the direct business relationship between Ontra and Customer, except where and to the extent permitted by the CCPA; and
 - 2.6.4 combine Personal Data received from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Data Subject in violation of Section 1798.140(ag)(1)(D) of the CCPA.
- 2.7 To the extent required under US Data Protection Law, where Ontra creates or processes Deidentified data (as defined by US Data Protection Law), Ontra shall:
 - 2.7.1 adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being associated with, a particular natural person or, where the CCPA applies, a household;
 - 2.7.2 publicly commit to maintain and use such Deidentified data in a Deidentified form and to not attempt to re-identify it, except that, where permitted by US Data Protection Law, Ontra may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of US Data Protection Law; and
 - 2.7.3 contractually obligate any recipients of the Deidentified data, if any, to comply with the provisions of this Section 2.7.

3. Authorized Sub-Processors and Third Parties

- 3.1 Customer acknowledges and agrees that Ontra may (a) share Personal Data with all entities that are a part of Ontra Group and the Authorized Sub-Processors to allow Ontra Group and Authorized Sub-Processors to access and process Personal Data in connection with the Services, (b) share Personal Data with additional Sub-Processors as directed or approved by Customer pursuant to any Order Form entered into by the Parties or in the course of Ontra performing its obligations under this DPA, the General Terms, or as otherwise necessary in connection with the provision of Services to Customer, including without limitation any Sub-Processor who performs the Document Abstracting Services or Data Migration Services, as applicable, approved by Customer, and (c) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data, such as auditors or advisers; provided that, with respect to any additional Sub-Processor engaged by Ontra as described in the foregoing clause (b) Customer's failure to object to such Sub-Processors engagement pursuant to Section 3.2 below will render such Sub-Processor an Authorized Sub-Processor under this DPA without the need to amend the DPA. By way of this DPA, Customer provides general written authorization to Ontra to engage Sub-Processors as necessary to perform the Services in accordance with this Section 3.1 and Section 3.2 below.
- 3.2 The List will be made available to Customer at a link provided to Customer in this DPA, via email, or through another means made available to Customer. Such List may be updated by Ontra from time to time. Ontra will provide a mechanism to subscribe to email notifications of new Authorized Sub-Processors that are added to the List and Customer agrees to subscribe to such notifications by filling out this form: [Sub-Processor Notification Subscription](#). At least ten (10) days before enabling any Sub-Processor other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Ontra will add such Sub-Processor to the List and notify subscribed individuals via email. Customer may object to such an engagement by informing Ontra in writing within ten (10) days of receipt of the aforementioned notice by Customer (the "Sub-Processor Notice Period"), provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain Sub-Processors are essential to providing the Services and that objecting to the use of a Sub-Processor may prevent Ontra from offering the Services to Customer.
- 3.3 If Customer reasonably objects to an engagement in accordance with Section 3.2 during the Sub-Processor Notice Period, and Ontra cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service (or the affected portion(s) thereof) by providing written notice to Ontra within ten (10) days after receiving notice from Ontra that an alternative has not been located. To the extent that Ontra, in its sole, reasonable discretion, determines that termination of the applicable Services pursuant to this Section 3.3 materially adversely affects Ontra's ability to provide the remaining Services to Customer, then, Ontra, in its sole, reasonable discretion, may terminate the Agreement in accordance with Section 6(b) of the General Terms. Termination of the Agreement shall not relieve Customer of its obligation to pay any Fees owed to Ontra pursuant to any Order Form incurred through the date of such Termination.
- 3.4 If Customer does not object to the engagement of a third party in accordance with Section 3.2 during the Sub-Processor Notice Period, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.
- 3.5 Ontra will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Ontra under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Ontra,

Ontra will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

- 3.6 If Customer and Ontra have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Ontra of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the Parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Ontra to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Ontra beforehand, and that such redacted copies will be provided by Ontra only upon request by Customer.

4. Security of Personal Data.

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 Data Subjects, Ontra shall maintain reasonable technical and organizational measures to meet a level of security appropriate to the risk of processing Personal Data. Exhibit 3 to this DPA sets forth additional information about Ontra's technical and organizational security measures, provided that Ontra reserves the right to modify Exhibit 3 to this DPA to account for technical progress and related developments so long as the overall security of the relevant Services is not degraded.

5. Transfers of Personal Data

- 5.1 The Parties agree that Ontra may transfer Personal Data processed under this DPA outside the country in which the Customer or relevant Data Subjects are located, including outside of the EEA, the UK, or Switzerland, as necessary to provide the Services. Customer acknowledges that Ontra's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. Ontra will ensure that appropriate safeguards have been implemented for the transfer of Personal Data as required by Data Protection Laws.
- 5.2 Subject to Section 5.3, the Standard Contractual Clauses will only apply to Customer's Personal Data subject to the GDPR that is transferred, directly or by onward transfer, to any Third Country. Where the Standard Contractual Clauses apply, the Parties acknowledge and agree that the Standard Contractual Clauses are entered into and completed in accordance with Exhibit 4 to this DPA.
- 5.3 The Standard Contractual Clauses will not apply to transfers of Customer's Personal Data where Ontra has adopted an alternative recognized compliance mechanism for the lawful transfer of such Personal Data, such as the EU-U.S., UK-U.S., or Swiss-U.S. Data Privacy Framework, to the extent valid.

6. Rights of Data Subjects

- 6.1 Ontra shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right granted by Data Protection Law (such requests individually and collectively "Data Subject Request(s)"). If Ontra receives a Data Subject Request in relation to any Personal Data provided by Customer, Ontra will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests are satisfied, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.
- 6.2 Ontra shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, use reasonable technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request, where possible, provided that (i) Customer is itself unable to respond without Ontra's assistance and (ii) Ontra is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Ontra.

7. Actions and Access Requests; Audits

- 7.1 Ontra shall, taking into account the nature of the processing and the information available to Ontra, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Data Protection Laws to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Ontra.
- 7.2 Ontra shall, taking into account the nature of the processing and the information available to Ontra, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by Data Protection Laws. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Ontra.
- 7.3 Ontra shall maintain records or information sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records to the extent required by applicable law, including Data Protection Laws. Customer shall, with reasonable notice to Ontra, have the right to review, audit and copy such records or information at Ontra's offices during regular business hours.
- 7.4 Ontra will allow for and cooperate with reasonable inspections or audits, to the extent required by Data Protection Laws and in accordance with this Section 7.4. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Ontra shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Ontra's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to the foregoing clause (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of

Ontra's data security infrastructure and procedures that is sufficient to demonstrate Ontra's compliance with its obligations under Data Protection Laws; provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Ontra's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Ontra for any time expended for on-site audits. If Customer and Ontra have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 7.4.

- 7.5 Ontra shall immediately notify Customer if an instruction, in Ontra's opinion, infringes the Data Protection Laws or Supervisory Authority.
- 7.6 In the event of a Personal Data Breach, Ontra shall, without undue delay (i) inform Customer of the Personal Data Breach, and (ii) take such steps as Ontra, in its sole discretion, deems necessary and reasonable to remediate such violation (to the extent that remediation is within Ontra's reasonable control).
- 7.7 In the event of a Personal Data Breach, Ontra shall, taking into account the nature of the processing and the information available to Ontra, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.
- 7.8 The obligations described in Sections 7.6(ii) and 7.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer, including as a result of Customer's breach of the Agreement. Ontra's obligation to report or respond to a Personal Data Breach under Sections 7.6 and 7.7 will not be construed as an acknowledgement by Ontra of any fault or liability with respect to the Personal Data Breach.
8. **Ontra's Role as a Controller.** The Parties acknowledge and agree that with respect to Account Data and Usage Data, Ontra is an independent controller, not a joint controller with Customer, for the purposes set out in this Section 8. Ontra will process Account Data and Usage Data as a controller (i) to manage the relationship with Customer and each Authorized User, including without limitation to create, modify, combine or otherwise manage such Authorized User's account(s) with the Ontra Group (whether via Customer's account or an individual account) or for any other purpose as instructed by such Authorized User consistent with the Agreement or any other agreement entered into between a member of the Ontra Group and such person (whether in their capacity as an Authorized User or otherwise); (ii) to carry out Ontra's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Ontra is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the General Terms. Ontra may also process Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by Ontra as a controller shall be in accordance with Ontra's privacy policy and/or the Ontra's Terms of Service, as applicable, in each case, as made available on Ontra's website and as may be updated from time to time.
9. **Assignment.** In addition to the rights of the Parties set forth in Section 17(i) of the General Terms, Ontra may subcontract its obligations under this DPA in accordance with Section 3 (Authorized Sub-Processors) to an Authorized Subprocessor.
10. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the General Terms; and (4) Ontra's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the General Terms.

Exhibit 1

Details of Processing

Nature and Purpose of Processing: Ontra will process Customer's Personal Data as necessary to provide the Services under the General Terms, for the purposes specified in the General Terms and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

Receiving data, including collection, accessing, retrieval, recording, and data entry;

Holding data, including storage, organization and structuring;

Using data, including analysis, consultation, testing,

Updating data, including correcting, adaptation, alteration, alignment and combination;

Protecting data, including restricting, encrypting, and security testing;

Sharing data, including disclosure, dissemination, allowing access or otherwise making available;

Returning data to the data exporter or data subject; and

Erasing data, including destruction and deletion.

Duration of Processing: Ontra will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the General Terms; (ii) for Ontra's legitimate business needs; or (iii) by applicable law or regulation. Account Data and Usage Data will be processed and stored as set forth in Ontra's privacy policy.

Categories of Data Subjects: Customer's individual employees, consultants, agents, partners, fund participants, investors, and other Authorized Users.

Categories of Personal Data: Ontra processes Personal Data contained in Account Data, Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Ontra in order to provide the Services or as otherwise set forth in the General Terms or this DPA. Categories of Personal Data include name, email addresses, phone numbers, and mailing addresses.

Sensitive Data or Special Categories of Data: None.

Exhibit 2

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Appendix 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s): The Customer

Contact person's name, position and contact details: As designated by Customer on the Order Form.

Signature and date: By entering into the General Terms, Data Exporter is deemed to have signed the Standard Contractual Clauses incorporated herein, as of the Effective Date of the General Terms.

Role (controller/processor): The Data Exporter's role is set forth in Section 2 of this DPA.

Data importer(s): Ontra

Address:

2041 East Street PMB 39 Concord, CA 94520

Contact details: Tel: (415) 358-6460; email: privacy@ontra.ai

Signature and date: By entering into the General Terms, Data Importer is deemed to have signed the Standard Contractual Clauses incorporated herein, as of the Effective Date of the General Terms.

Role (controller/processor): The Data Importer's role is set forth in Section 2 of this DPA.

2. Description of the Transfer

Data Subjects	As described in Exhibit 1 of this DPA.
Categories of Personal Data	As described in Exhibit 1 of this DPA.
Special Category Personal Data (if applicable)	As described in Exhibit 1 of this DPA.
Nature of the Processing	As described in Exhibit 1 of this DPA.
Purposes of Processing	As described in Exhibit 1 of this DPA.
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit 1 of this DPA.
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the General Terms or this DPA.
Recipients of Personal Data Transferred to the Data Importer	Ontra will maintain and provide a list of its Authorized Sub-Processors upon request.

3. Competent Supervisory Authority

The Supervisory Authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The Supervisory Authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Office.

4. List of Authorized Sub-Processors

Where Customer receives the Ontra Services, Customer acknowledges and agrees that the entities set forth on the List shall be deemed Authorized Sub-Processors that may Process Personal Data pursuant to this DPA.

Exhibit 3

Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

The following technical and organizational measures are implemented as to the Ontra Services:

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Data is encrypted at rest with 256-bit Advanced Encryption Standard (AES-256) using AWS Server Side Encryption and KMS. Personal data storage and transmission services are provided by AWS, which require SSL encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Ontra will employ administrative and technical measures in accordance with applicable industry practices to protect Customer's Personal Data and prevent the accidental loss or unauthorized access, use, alteration or disclosure of Customer's Personal Data under its control during each order term.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	<p>Ontra utilizes the AWS Aurora database platform which provides continuous backup to Amazon S3 and replication across three Availability Zones (AZs). AWS Aurora handles the recovery of data and the moving of load between AZs in the case of failure. In addition, full database snapshots are taken and stored in AWS S3 and the GCP Google Storage system.</p> <p>Ontra continuously and securely backs up all data. Ontra maintains backups of Customer Data as may be required to meet contractual and regulatory compliance requirements and in compliance with its internal policies.</p>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Ontra's Platform undergoes third party penetration testing SOC 2 Type II auditing annually.
Measures for user identification and authorization	Strong passwords are required for client authentication with their email address and two-step authentication is available. Sign-in attempts are rate-limited and trigger notifications to the user and our security team. Security Assertion Markup Language authentication is also available for customers who utilize Single Sign-On.
Measures for the protection of data during transmission	<p>All non-secure connections to Ontra's application are redirected to HTTPS and connected over TLS.</p> <p>Personal data storage and transmission services are provided by Cloudflare and AWS, which require SSL encryption.</p>
Measures for the protection of data during storage	Ontra's application database is encrypted at rest with 256-bit Advanced Encryption Standard (AES-256) using AWS Server Side Encryption and KMS.

Technical and Organizational Security Measure	Details
Measures for ensuring physical security of locations at which personal data are processed	Ontra's application and database are managed by physical infrastructure hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Services (AWS) technology.
Measures for ensuring events logging	Activity on the Platform is routinely logged for security purposes. Each time a user requests, accesses, or changes personal or customer information, the user, activity, and time are saved to a third party monitoring system.
Measures for ensuring system configuration, including default configuration	<p>Ontra's application configuration handles everything that is likely to vary between deployments of the Platform (staging, production, developer environments, etc.).</p> <p>System configuration is intentionally stored in environment variables, separate from the codebase.</p>
Measures for internal IT and IT security governance and management	<p>Ontra has developed a security program and implemented controls to meet or exceed security compliance requirements, including but not limited to NIST Standards, SOC 2 Security Criteria, ISO certification, and other applicable industry best practices.</p> <p>An overview of Ontra's security program includes:</p> <ul style="list-style-type: none"> ● Inventory and protection of all critical assets; ● Visibility into and the management of data lifecycle, from creation to retention to deletion; ● Protection of data-at-rest, data-in-transit, and data-in-use; ● Automated security configuration and remediation; ● Centralized identity and access management ● Secure product development; ● Continuous monitoring and auditing; ● Validated plan and practice for business continuity, disaster recovery, and emergency response; and ● End-user computing protection and awareness training. <p>The security program and its policies and procedures cover all Ontra workforce members, including full-time employees, temporary staff, contractors, managers, executives, and relevant third parties. All policies are reviewed and approved by Ontra's management annually.</p>
Measures for certification/assurance of processes and products	Ontra's undergoes annual SOC 2 Type II auditing by a licensed CPA firm.
Measures for ensuring data minimisation	Ontra only processes Customer's Personal Data in accordance with its rights and obligations under applicable agreements and as authorized in writing by such customer. Constituent access to Ontra networks, applications, and data (including customer data) is granted based upon business requirements and limited according to need-to-know and least-privilege principles.

Technical and Organizational Security Measure	Details
Measures for ensuring data quality	Upon request from Customer and in the manner specified in an applicable agreement with such Customer, Ontra will assist the Customer with its duties relating to Data Subjects, including to rectify any Personal Data of Data Subjects held that is inaccurate or incomplete.
Measures for ensuring limited data retention	Upon request from Customer, Ontra will, except as otherwise set forth in any agreement with such Customer, delete all customer data, including Personal Data.
Measures for ensuring accountability	Ontra maintains, monitors, and enforces data protection and security policies, including policies governing employee and contractor data security obligations, Personal Data Breach response, data destruction, acceptable use, data protection, and system access. Additionally, Ontra requires all employees to complete annual security awareness training.
Measures for allowing data portability and ensuring erasure	Customer's Personal Data is stored in a single bucket but is logically separate by path in database and storage which is enforced by the code to ensure no lateral movement. Ontra can manually provide a copy of the data if needed for migration as well as delete the data.
Technical and organizational measures of Sub-Processors	Ontra completes an annual review of all critical vendors and Authorized Sub-Processors. This process is reviewed annually as part of Ontra's policies and procedures.

Exhibit 4

European Data Transfers

1. Definitions

- 1.1 "Data Exporter" means Customer.
- 1.2 "Data Importer" means Ontra.
- 1.3 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the EEA, and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR or an alternative recognized transfer mechanism.
- 1.4 "ex-Switzerland Transfer" means the transfer of Personal Data subject to the Revised FDAP (defined below), from the Data Exporter to the Data Importer (or its premises) outside Switzerland, and such transfer is not governed by an adequacy decision made by the FDPIC (defined below) or an alternative recognized transfer mechanism.
"ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the UK, and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018 or an alternative recognized transfer mechanism.

2. Ex-EEA Transfer Terms

- 2.1 The Parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
 - 2.1.1 Module One (Controller to Controller) of the EU SCCs apply when Ontra is processing Personal Data as a controller pursuant to Section 8 of the DPA.
 - 2.1.2 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Ontra is processing Personal Data for Customer as a processor pursuant to Section 2 of the DPA.
 - 2.1.3 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Ontra is processing Personal Data on behalf of Customer as a Sub-Processor.
- 2.2 For each module, where applicable the following applies:
 - 2.2.1 The optional docking clause in Clause 7 does not apply;
 - 2.2.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Sub-Processor changes shall be as set forth in Section 3.2 of the DPA;
 - 2.2.3 In Clause 11, the optional language does not apply;
 - 2.2.4 All square brackets in Clause 13 are hereby removed;
 - 2.2.5 In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;
 - 2.2.6 In Clause 18(b), disputes will be resolved before the courts of Ireland;
 - 2.2.7 Exhibit 2 to the DPA contains the information required in Annex I and Annex III of the EU SCCs;
 - 2.2.8 Exhibit 3 to the DPA contains the information required in Annex II of the EU SCCs; and
 - 2.2.9 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

3. Ex-Switzerland Transfers

- 3.1 The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:
 - 3.1.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.
 - 3.1.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.
 - 3.1.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU Supervisory Authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.
 - 3.1.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

4. Ex-UK Transfers

- 4.1 The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed as follows (collectively, the "UK Addendum"):

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Ontra
Key Contact	See Exhibit 2 of the DPA	See Exhibit 2 of the DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Sections 5.2 and 5.3 of the DPA.
---------	---

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	See Exhibit 2 of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	See Exhibit 3 of the DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	See Exhibit 2 of the DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	<input checked="" type="checkbox"/> <u>Importer</u> <input type="checkbox"/> <u>Exporter</u> <input type="checkbox"/> <u>Neither Party</u>
---	--

Entering into this UK Addendum:

- Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

- Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Appendix Information	shall be as set out in Table 3
----------------------	--------------------------------

Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section Error! Reference source not found. of the UK Addendum.
ICO	means the Information Commissioner of the United Kingdom.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.
7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.
10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.
11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:
 - a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and
 - c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.
13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.
15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:
 - a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;
 - b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",
 - c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
 - d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
 - e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
 - f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

- g) References to Regulation (EU) 2018/1725 are removed;
- h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
- i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
- j) Clause 13(a) and Part C of Annex I are not used;
- k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
- l) In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";
- m) Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";
- n) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and
- o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved UK Addendum which:
- a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or
 - b) reflects changes to UK Data Protection Laws;
- The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.
19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:
- a) its direct costs of performing its obligations under the UK Addendum; and/or
 - b) its risk under the UK Addendum,
- and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Previous Versions

Customer Data Processing Addendum, October 19, 2023

Customer Data Processing Addendum, July 1, 2024