SOTI

ONE PLATFORM – CONNECTING EVERYTHING

SOTI DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is between SOTI and the Customer. This DPA forms part of the software licensing agreement available at https://www.soti.net/about/legal/, or other agreement for the provision of Services ("Agreement") between Customer and SOTI.

1. Definitions:

"Business Contact Information" means information such as an individual's name, title, business address, telephone number or email addresses that is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment or profession.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"Customer" means the individual(s) or entity that has an Agreement with SOTI.

"Data Privacy Laws" means all data protection or privacy laws applicable to the parties which may include GDPR, UK GDPR or CCPA.

"Data Subject Request" means any request by an individual (or by another person acting on behalf of an individual) to exercise a right under any Data Privacy Laws, or any other complaint or inquiry or similar communication about the Processing of the individual's Personal Data.

"EU SCCs" mean Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oja, and as completed in the Restricted Transfer Schedule.

"GDPR" means 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, and repealing Directive 95/46/EC.

"Personal Data" means any information relating to an identified or identifiable individual, that the Customer provides to SOTI through the Services. Notwithstanding the foregoing, Personal Data shall not include Business Contact Information, to the extent such information is not considered Personal Data under Data Privacy Laws.

"Restricted Transfer" means any transfer of Personal Data where the Data Privacy Laws require an onward transfer mechanism to lawfully transfer Personal Data. Restricted Transfers do not include transfers to recipients in countries whose data protection regimes have been declared adequate by relevant data protection authorities or which are otherwise not restricted.

"Restricted Transfer Schedule" means the schedule to the DPA dealing with Restricted Transfers attached herewith as Schedule 4.

"SCCs" mean the EU SCCs, and where applicable, the UK Addendum.

"Services" mean the software and/or services provided by SOTI to Customer pursuant to the Agreement.

"SOTI" means the SOTI entity that has entered into an Agreement with Customer.

"UK Addendum" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force from 21 March 2022, available here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as updated and/or replaced from time to time.

Any capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Agreement. The terms "data subject", "processing", "controller", "processor", and "supervisory authority" as used in this DPA have the meanings given in GDPR irrespective of whether GDPR applies.

2. The Data Controller and the Data Processor
    a. Under the Agreement, the Customer may act as either a Controller or Processor and SOTI shall be a Processor. SOTI shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and any applicable order forms; and (ii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

    b. Should SOTI reasonably believe that a specific processing activity beyond the scope of the Customer's instructions is required to comply with a legal obligation to which SOTI is subject, SOTI shall inform the Customer of that legal obligation and seek explicit authorization from the Customer before undertaking such processing.

    c. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

    d. Customer warrants that it has all necessary rights and authorizations to provide the Personal Data to SOTI for the Processing to be performed in relation to the Services. To the extent required by Data Privacy Laws, Customer is responsible for ensuring it has a lawful basis for disclosing Personal Data to SOTI including obtaining any necessary Data Subject consents and authorizations. Should such a consent or authorization be revoked by a Data Subject, Customer is responsible for communicating the fact of such revocation to SOTI.

    e. An overview of the categories of Personal Data, the categories of Data Subjects, and the nature and purposes for which the Personal Data are being processed is provided in Schedule 1.

3. Confidentiality
    Without prejudice to any existing contractual arrangements between the parties, SOTI shall treat all Personal Data as confidential and it shall inform all its employees, agents and/ or approved Subprocessors (defined below) engaged in processing the Personal Data of the confidential nature of the Personal Data. SOTI shall ensure that all such persons or parties are subject to confidentiality obligations.

4. Subprocessors
    a. Customer acknowledges that SOTI may engage third-party contractors or service providers for the provision of Services under the Agreement ("Subprocessors"). SOTI shall ensure that each Subprocessor is subject to obligations that are substantially similar to the provisions of this DPA.

    b. A current list of Subprocessors is attached herewith as Schedule 3 and Customer hereby consents to the engagement of these Subprocessors by SOTI. To the extent required by Data Privacy Laws, SOTI shall notify Customer of the appointment of a new Subprocessor. Customer may reasonably object to SOTI's use of a new Subprocessor within thirty (30) days of a written notice by SOTI. If Customer reasonably objects to a new Sub-processor as permitted in the preceding sentence, SOTI will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If SOTI is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by SOTI without the use of the objected-to new Subprocessor by providing written notice to SOTI.

    c. Notwithstanding any authorisation by the Customer within the meaning of the preceding paragraph, SOTI shall remain fully liable vis-à-vis the Customer for the performance of any such Subprocessor that fails to fulfill its data protection obligations.

5. Security

a. 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, SOTI shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include, at a minimum, the security measures attached herewith as Schedule 2.

b. Both Customer and SOTI shall maintain security policies that are fully implemented and applicable to the processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the Processing.

c. SOTI's ISO 27001 Certificate is available at https://soti.net/resources/security-compliance/. Additionally, upon request, and under a confidentiality agreement, SOTI shall also provide Customer with a copy of its SOC 2 Type II report (SOTI's IS0 27001 Certificate and SOC 2 Type II report shall collectively be referred to as "Reports"). To the extent Customer's audit requirements under the SCCs or Data Privacy Laws cannot reasonably be satisfied through the Reports, or any other documentation SOTI makes available to its Customers, at the request of the Customer, SOTI shall demonstrate the measures it has taken pursuant to this Section 5 and shall allow the Customer to audit and test such measures at the Customer's sole expense no more than once every 12-months. Unless otherwise required by Data Privacy Laws or the Customer's competent supervisory authority, the Customer shall be entitled upon giving at least thirty (30) days' notice to SOTI to carry out or have carried out by a reputable third-party auditor who has entered into a confidentiality agreement with SOTI, audits of SOTI´s premises and operations as these relate to the Personal Data. SOTI shall cooperate with such audits carried out by or on behalf of the Customer and shall grant the Customer´s auditors reasonable access to any premises and devices involved with the Processing of the Personal Data during normal business hours and with minimum disruption to regular business activities. SOTI shall provide the Customer and Customer's auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Customer to ascertain SOTI's compliance with this DPA, and/or to ascertain SOTI's compliance with any approved code of conduct or approved certification mechanism. Neither Customer nor its auditors shall have access to any data from SOTI's other customers or to SOTI's systems or facilities not involved in providing the applicable Services

6. Data Transfers

a. The Parties hereby enter into the EU SCCs where the Services involve a Restricted Transfer of Personal Data that is subject to GDPR or the Swiss Federal Act on Data Protection (FADP). The Parties agree that references to "GDPR" in the EU SCCs shall be understood to also be references to the FADP and interpreted to permit data subjects in Switzerland to seek redress for their rights in Switzerland.

b. The Parties hereby enter into the UK Addendum where the Services involve a Restricted Transfer of Personal Data that is subject to the UK GDPR. For the purposes of the UK Addendum: (i) the information required for Table 1 is contained in Schedule 4 of this DPA and the start date shall be the commencement of the Services (ii) in relation to Table 2, the version of the EU SCCs to which the UK Approved Addendum applies is Module Two where Customer is acting a Controller and Module 3 when Customer is acting as a Processor; (iii) in relation to Table 3, the list of parties and description of the transfer are as set out in Schedules 1 and 4 of this DPA; SOTI's technical and organisational measures are as specified in Schedule 2, and the list of SOTI's sub-processors is attached herewith as Schedule 3.

c. To the extent the SCCs are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the parties agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

7. Information Obligations and Incident Management

a. SOTI shall notify Customer without undue delay, but no later than 72 hours after becoming aware of a breach of SOTI's security safeguards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data ("Breach").

b. SOTI's notification of a Breach will describe: the nature of the Breach; the measures SOTI has taken, or plans to take, to address the Breach and mitigate its potential risk; the measures, if any, SOTI recommends that Customer take to

address the Breach; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, SOTI's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

8. Returning or Destruction of Personal Data
   To the extent permitted by applicable law, within ninety (90) days of the termination of the Agreement or at any time upon the written request of Customer, Customer Personal Data in SOTI's possession or control shall be (i) destroyed in a manner that prevents its recovery or restoration or, (ii) if so directed by Customer, returned to Customer in a secure manner without SOTI retaining any actual or recoverable copies thereof. Until Customer Personal Data is deleted or returned, SOTI shall continue to comply with this DPA.

9. Assistance to Data Controller
   a. SOTI shall, to the extent legally permitted, promptly notify Customer of any Data Subject Request. SOTI shall not respond to a Data Subject Request itself, except that Customer authorizes SOTI to redirect the Data Subject Request as necessary to allow Customer to respond directly.

   b. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SOTI shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SOTI is legally permitted to do so and the response to such Data Subject Request is required under Data Privacy Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from SOTI's provision of such assistance.

   c. Taking into account the nature of Processing and the information available to SOTI, SOTI shall assist Customer in fulfilling the Customer's obligation under Data Privacy Laws to conduct a data protection impact assessment related to the Customer's use of the Services.

10. CCPA
    For any Personal Data Processed by SOTI pursuant to the Agreement that is subject to the CCPA, SOTI will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. SOTI agrees not to (a) sell (as defined by the CCPA) Customer's Personal Data; (b) retain, use, or disclose Customer's Personal data for any commercial purpose (as defined by the CCPA) other than providing the Services in accordance with the Agreement; or (c) retain, use, or disclose Customer's Personal Data outside of the scope of the Agreement.

11. Liability
    Either party's total aggregate liability arising out of or related to this DPA, including its exhibits and attachments, whether in contract, tort or under any other theory of liability, is subject to the terms of the Agreement.

12. Duration and Termination
    a. This DPA shall come into effect on the effective date of the Agreement.

    b. This DPA shall terminate on date of expiration or termination of the Agreement, or until Customer's Personal Data is returned or destroyed.

13. Conflict
    In the event of any inconsistency between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

Signed for and behalf of SOTI:		Signed for and behalf of the Customer:	
Sign:	_____	Sign:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Schedule 1 – Description of Processing

1. Subject Matter of the Processing of the Personal Data
SOTI's provision of Services to Customer in accordance with the Services Agreement

2. Duration of the Processing
For the term of the Agreement or earlier if requested by Customer in accordance with this DPA.

2. The nature and purpose of the Processing of the Personal Data
SOTI is engaged to provide Services to Customer, which involve the Processing of Personal Data. The scope of the Services is set out in the Agreement, and Personal Data will be Processed by SOTI to deliver the Services in accordance with the terms of the Services Agreement and this DPA.

3. The types of the Personal Data to be Processed
Any Personal Data disclosed or made available to SOTI by Customer in course of the Services which include name, title, gender, personal contact details (address, telephone number, email address), device ID, IP address, geo-location, purchase history and other types of Personal Data.

4. The categories of Data Subject to whom the Personal Data Relates
The categories of data subjects are determined by the nature of the client engagement, the details of which are covered in the Agreement, but may include Personal Data about Customer's end users, customers, employees or contractors.

6. Sensitive Data
Customer shall ensure that no sensitive data is disclosed or made available to SOTI pursuant to the Services.

7. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)
Depends on the nature of Services purchased by the Customer under the Agreement.

Schedule 2 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

- SOTI encrypts data at rest and data in transit using industry-standard strong encryption, hashing and communication protocols.

- All SOTI employees and contractors that have access to information assets are required to sign off on their understanding of, and willingness to comply with, SOTI's information security policies upon hire, and regularly (for example, annually) thereafter, to account for policy changes over time.

- SOTI's employees sign non-disclosure agreements and participate in security training events and testing.

- SOTI uses anti-malware systems and blocks unnecessary access to networks and computers, enabling early detection and mitigation of security incidents.

- SOTI uses antivirus software to detect and defend against viruses, trojans, worms and spyware.

- SOTI uses Web Application Firewalls (WAF) for multi-tenant products to protect web applications or APIs against common web exploits that may affect availability, compromise security or consume excessive resource.

- SOTI uses tools to provide near real-time detection and automatic inline mitigations and defence against denial-of-service (DDoS) attacks that target websites or applications.

- SOTI policies, procedures and guidelines are all developed following National Institute of Standards and Technology (NIST), ISO 27001 and other industry best practices.

- SOTI conducts internal and independent third-party audits to ensure that controls are adequate and effective to maintain the confidentiality, integrity and availability of SOTI information resources.

- SOTI has an established incident response plan to help protect the confidentiality, integrity and availability of information, prevent loss of service and comply with legal requirements.

- SOTI maintains business continuity and disaster recovery policies for the recovery of SOTI's IT infrastructure, IT and cloud services in the case of a disaster or other disruptive incident.

Schedule 3 – List of Subprocessors

No.	Subprocessor	Primary Scope of Processing
1	Amazon Web Services Inc. (AWS)	Hosting and service delivery
2	Atlassian	Software development management tool
3	DocuSign	Contract signature and management
4	Google Maps	Location based services
5	Microsoft Corporation (Azure)	Hosting
6	Workday	Invoice/Payment Processing
7	Microsoft (Bing Maps)	Location based services
8	Salesforce	Order and Support processing
9	SOTI Ireland	Support services and business operations
10	SOTI Ltd (United Kingdom)	Support services and business operations
11	SOTI India Private Limited	Support services and business operations
12	SOTI GmbH (Germany)	Support services and business operations
13	SOTI Pty Ltd (Australia)	Support services and business operations

Schedule 4 – Restricted Transfers

1. Module Two (Controller to Processor) of the EU SCCs will apply where Customer is a Controller of Personal Data;

2. Module Three (Processor to Processor) of the EU SCCs will apply where Customer is a Processor of Personal Data;

3. For each Module, where applicable:
   i. in Clause 7 of the EU SCCs, the optional docking clause will not apply;
   ii. in Clause 9 of the EU SCCs, Option 2 will apply and the time period for notice of sub-processor changes will be as set forth in the DPA;
   iii. in Clause 11 of the EU SCCs, the optional language will not apply;
   iv. in Clause 17 (Option 1), the EU SCCs will be governed by Irish law;
   v. in Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of Ireland;
   vi. in Annex I, Part A of the EU SCCs:

      Data Exporter: Customer
      Contact details: The email address(es) designated by Customer in Customer's account or in the Agreement
      Data Exporter Role: The Data Exporter's role is set forth in the relevant section of DPA
      Signature and Date: By entering into the DPA, Data Exporter is deemed to have signed the EU SCCs including their Annexes, as of the effective date of the DPA

      Data Importer: SOTI Inc. and its Affiliates
      Contact details: SOTI Privacy Team – privacy@soti.net
      Data Importer Role: The Data Importer's role is set forth in the relevant section of the DPA
      Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed the EU SCCs including their Annexes, as of the effective date of the DPA

   vii. The schedule to the DPA that provides a description of the processing of Personal Data serves as Annex 1, Part B of the EU SCCs

   viii. In Annex I, Part C of the EU SCCs: The Irish Data Protection Commission will be the competent supervisory authority

   ix. The technical and organizational security measures available in Schedule 2 serve as Annex II of the EU SCCs.