SuSea, Inc.
Data Processing Agreement

Last updated: March 14, 2025

This Data Processing Agreement, including its Annexes, ("DPA") is incorporated by reference and/or forms part of the Master Subscription Agreement or other written electronic agreements (the "Agreement") between SuSea, Inc., dba you.com ("SuSea" or "Company") and the entity signing pursuant to the Agreement (the "Customer"; and together with SuSea, collectively, the "Parties," or individually, a "Party") for the processing of Personal Data in relation to SuSea's Services to Customer.

1. Definitions

1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the Controller of this DPA or the Agreement. "Control" for the purpose of this definition, means direct or indirect ownership or control of more than 50% of the voting interest of the Controller entity.

1.2. **"Applicable Data Protection Laws"** means all applicable laws, rules, regulations, and governmental requirements related to the privacy, confidentiality, or security of Personal Data, as they may be amended or updated. These include, without limitation, certain U.S. laws currently effective or due to become effective in 2025, such as Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("CCPA"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("CPA"), Connecticut's Data Privacy Act ("CTDPA"), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("UCPA"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("VCDPA), and the Maryland Online Data Privacy Act (MDODPA) (collectively "U.S. Privacy Laws").

1.3. **"Covered Data"** means Personal Data shared by Customer in relation to the provision of the Agreement.

1.4. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act, and its implementing regulations.

1.5. **"Data Controller"** means the entity that determines the purposes and means of the Processing of Personal Data.

1.6. **"Data Processor"** will have the following meaning (as applicable): the meaning given to "processor" under Applicable Data Protection Laws or the meaning given to "service provider" under Applicable Data Protection Laws**,** such as the CCPA definition.

1.7. **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

1.8. **"Personal Data"** means any data or information that may be linked or reasonably linkable to a natural person or legal entity (where such information is protected similarly as Personal Data or personally identifiable information under Applicable Data Protection Laws), where each such data is Customer data.

1.9. **"Process(ing)"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10. **"Service(s)"** means the services to be provided by SuSea pursuant to the Agreement.

1.11. **"Sub-processor"** means any Processor engaged by SuSea.

2. General Applicability of this DPA

2.1. This DPA is incorporated into part of the Agreement and applies only to the extent that the Company processes Customer Personal Data on behalf of Customer as Data Processor.

2.2. Customer acknowledges and agrees that Company may amend this DPA from time to time on reasonable notice to Customer where such changes are required because of changes in the Applicable Data Protection Laws.

3. Scope of Data Processing

3.1. This DPA shall apply to the extent that Company shall process Customer Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller (such third-party, the "Third-Party Controller") with respect to Customer Personal Data.

3.2. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data following such instructions will not violate applicable Data Protection Laws. The Parties agree that the Agreement (including this DPA) sets out the exclusive and final instructions to Company for all Processing of Customer Personal Data, and (if applicable) include and be consistent with all instructions from Third-Party Controllers.

3.3. Each party will comply with its respective obligations under Data Protection Laws. Customer agrees that (1) it will use the Service in a manner designated to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing up Customer Personal Data; and (2) it has obtained all consents, permissions and/or rights necessary under Data Protection Laws for Company to lawfully Process Customer Personal Data for the purpose of, without limitation, Customer's sharing and/or receiving of Customers Personal Data with third-parties via the Service.

3.4. The details of the Processing of Covered Data (such as subject matter, duration, purpose of the Processing, categories of Personal Data, and Data subjects) are described in the Agreement and in Part B of Annex 2 of this DPA.

3.5. Subject to any applicable restrictions and/or conditions in the Agreement, Customer may also include 'special categories of personal data' or similarly sensitive Personal Data (as defined in Data Protections Laws) in Customer Personal Data, the extent of which is determined and controlled by Customer in its discretion.

4. Sub-Processors

4.1. Customer provides Company with a general authorization to engage with any current or future Sub-processors, subject to section 4.2, which may be found at https://trust.you.com ("Sub-processor Site") as of the effective date of this DPA.

4.2. Company shall make available on its Sub-processor Site a mechanism to subscribe to notifications of addition or replacement new Sub-processors. Company shall provide such notifications (in writing) both to (1) email addresses that have subscribed notifications on the Sub-processor Site, and (2) email addresses designated by Customer as 'privacy notices' recipients within Service, at least twenty-eight (28) days in advance of allowing the new Sub-Processor to Process Customer Personal Data (the "Objection Period"). During the Objection Period, objections (if any) to Company's appointment of the new Sub-processor must be provided to Company in writing and based on reasonable grounds. In such event, the Parties will discuss these objections in good faith with the goal of achieving a resolution. If it can be reasonably demonstrated to Company that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Company cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Agreement with the Sub-processor with respect to only those aspects which cannot be provided by Company without the use of the new Sub-process by providing advance written notice to Company of such termination. Company will refund Customer any prepaid unused fees of such Sub-processor Agreement following the effective date of such termination.

5. Data Subject Rights Request

5.1. Company will send to Customer, within a reasonable time, any Data Subject Request received by Company related to the Covered Data and may suggest to the Data Subject to submit their request directly to Customer.

5.2. Company will fulfill its obligation under Applicable Data Protection Laws, taking into account the nature of the Processing of Covered Data, to respond to Data Subject Requests.

6. Security

6.1. Company shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for making an independent determination as to whether the use of the Service will meet Customer's requirements and legal obligations under Data Protection Laws.

6.2. Company shall at least implement the technical and organizational measures specified in Annex 2 to ensure the security of the personal data.

6.3. Company shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Customer Audit Rights

7.1. Company shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "Auditor"), access to reasonably requested documentation evidencing Company's compliance with its obligations under this DPA.

7.2. Customer may also send a written request for an audit of Company's applicable controls, including inspection of its facilities. Following receipt by Company of such request, Company and Customer shall mutually agree in advance on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. Company may charge a fee (rates shall be reasonable, taking into account the resources expended by Company) for any such audit. The audit and any information arising therefrom shall be considered Company's confidential information and may only be shared with a third party with Company's prior written agreement.

7.3. Customer may only use the results of an audit for the purpose of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of the DPA.

8. Data Transfers

8.1. If the Applicable Data Protection Laws have prescribed a specific mechanism for the transfer of Customer Personal Data to Company or if a contractual clause for processing Customer Personal Data exists, then this Agreement will serve as the requisite "**Transfer Mechanism.**"

8.2. Company shall notify Customer of changes to this Transfer Mechanisms as specified in this Agreement.

9. Security Incident Response

9.1. Customer acknowledges that because Company personnel may not have visibility to the content of Customer Personal Data, it is unlikely Company can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, and number of categories of affected Data Subjects. Communications by or on behalf of Company with Customer in connection with a security incident shall not be construed as an acknowledgment by Company of any fault or liability with respect to the security incident.

10. Relationship with the Agreement

10.1. Company may update this DPA and its terms of services periodically, with such updated version linked to the Terms & Conditions posted to www.you.com/terms, or a successor website designated by Company; provided, however, that no such update shall materially diminish the privacy or security of Customer Personal Data.

10.2. Notwithstanding anything to the contrary in the Agreement or this DPA, each Party's and all of its Affiliates' liability shall be subject to any aggregate limitations on liability set out in the Agreement.

11. Standard Contractual Clauses

11.1. The parties agree that, to the extent required by Applicable Data Protection Laws, the terms of the Standard Contractual Clauses (SCCs) Module 1 (Controller to Controller), Module Two (Controller to Processor) and/or Module Three (Processor to Processor), each as further specified in Annex 3 of this DPA, are hereby incorporated by reference and will be deemed to have been executed by the Parties.

11.2. To the extent required by Applicable Data Protection Laws, the jurisdiction-specific addenda to the SCCs set out in Annex 3 are also incorporated herein by reference and will be deemed to have been executed by the Parties.

11.3. If there is any conflict between the terms of this DPA and the terms of the SCCs, the SCCs shall govern.

11.4. SuSea will provide Customer reasonable support to enable Customer's compliance with the requirements imposed on international transfers of Covered Data. SuSea will, upon Customer's request and at Customer's cost, provide information to Customer that is reasonably necessary for Customer to complete a transfer impact assessment ("TIA") to the extent required under Applicable Data Protection Laws.

12. Termination and Erasure

12.1. Following the termination of the Agreement, the Company shall, at the choice of the Controller, delete all Personal Data processed on behalf of the Controller and certify to the Controller that is has done so, or return all the personal data to the Controller and delete existing copies unless Applicable Data Protection Laws requires storage of Personal Data. Controller acknowledges, however, that such deletion or return of Personal Data may adversely impact any remaining or outstanding functionality derived from Company's Service to Controller.

SuSea, Inc.:

Name: _____

Title: _____

Date Signed: _____

Customer Name: _____

Name: _____

Title: _____

Date Signed: _____

ANNEX 1
DETAILS OF PROCESSING AND TRANSFERS

PART A – List of Parties

The parties are established in the preamble to this DPA. Additional information regarding the data exporter (the "Controller") and data importer (the "Processor") concerning any transfers that fall within the scope of Applicable Data Protection Laws, are detailed below.

1. **Data exporter(s)/Controller**

Name:

Address:

Contact person's name, position, and contact details:

Signature: Date:

_____ _____

Role: Controller

2. **Data importer/Processor:**

Name: SuSea, Inc.

Address: 228 Hamilton Ave, Floor 3, Palo Alto, CA 94301, USA

Contact person's name, position and contact details: _____, Project Manager, _____@you.com,

Signature: Date:

_____ _____

Role: Processor

PART B – Description of Processing

3. **Categories of Data Subjects** – Banking Customers and/or as determined by Customer by the terms of the Agreement.
4. **Categories of Personal Data** – User Data, personal data in prompts and answers, and/or as determined by Customer by terms of the Agreement.
5. **Type of Processing** – Artificial intelligence
6. **Purposes for which the Personal Data is Processed** – Usage on behalf of the users and for service provision.
7. **Duration of Processing** – During the term of the Agreement.

PART C– Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13 of the approved EU Standard Contractual Clauses (as incorporated in Section 11 of this DPA).

Where the data exporter is established in an EU Member State*: The supervisory authority of the country in which the data exporter established is the competent authority.*

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR*: The competent supervisory authority is the one of the Member State in which the representative is established.*

ANNEX 2

TECHNICAL AND ORGANIZATIONAL MEASURES

The processor has prepared the following document(s):

SuSea will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data uploaded to the Service as described in the Informational Security policies (found on https://www.trust.you.com). SuSea will maintain an information security program (including adoption and enforcement of internal policies and procedures) reasonably designed to help (a) Customer secure Customer Personal Data against accidental or unlawful loss, access or disclosure, (b) identity reasonably foreseeable, internal risks to security and unauthorized access to the Company's network, and (c) minimize security risks, including through risk assessment and regular testing. SuSea will designate one or more employees to coordinate and be accountable for the information security program.

1. Management and Organization

Measures that ensure the management and organizational structures sufficient for the execution of the contract.

Technical Measures	**Organizational Measures**
Software solutions for data protection management in use	A suitable organizational structure for information security is in place and information security is integrated into processes and procedures throughout the organization
Central documentation of all data protection procedures and regulations with access for employees as required/authorized (e.g. wiki, intranet)	Security directives and guidelines have been defined, approved by management, and communicated to staff
	The roles of individual employees in the security process have been clearly specified
	Regular reviews of the effectiveness of technical and organizational measures according to the PDCA cycle (Plan-Do-Check-Act)
	Concepts and documentation in the security environment are being reviewed regularly and kept up to date
	Depending on the size of the company: Use of a suitable information security management system (ISMS), e.g. in accordance with ISO/IEC 27001, BSI standards, or ISIS12
	Roles and responsibilities in the area of security are known within the company and have been assigned

Technical Measures	Organizational Measures
	an (Information Security Officer (ISO), IT manager, and Data Protection Officer (DPO), among others)
	Employees receive regular training regarding information security and data protection issues and are obliged to observe confidentiality and data secrecy

2. Confidentiality

Measures to prevent unauthorized persons from gaining physical access to the data processing systems used to process personal data.

2.1. Control of Physical Access – No measures to control physical access are required because the data processing systems used to process personal data are operated by Amazon AWS and Microsoft Azure.

2.2. Access Control

Measures to prevent unauthorized persons from using data processing systems and procedures.

Technical Measures	Organizational Measures
Login with user name + password	Confidential administration of user authorizations, including documentation of identity and access rights as well as deprovisioning process and specification of sufficient complexity of authorizations in line with state-of-the-art technology
Login with two- factor authentication	Creation of user profiles and management of user rights by administrators
Use of an anti-virus solution or an endpoint protection system with regular, at least daily signature updates	Password directives implemented by the system
Use of a firewall at the central Internet gateway and DMZ concepts	Regulations regarding protective measures against unauthorized inspection of screen content and documents
Use of intrusion detection systems (IDS) or intrusion prevention systems (IPS)	Directive for the use of state-of-the-art cryptographic procedures
Mobile device management	Regulations for handling mobile data storage devices

Technical Measures	**Organizational Measures**
Encryption of data carriers of servers / stationary clients (e.g. desktop PCs) / mobile clients (e.g. notebooks, tablets and smartphones)	Regular review of assigned access and authorizations
Limiting the integration of external devices to the necessary minimum by means of technical measures (e.g. for USB drives, smartphones, external hard drives), and preventing automatic execution of programs that are on them	CrowdStrike USB Device Control
Automatic locking after a certain period of inactivity if manual locking cannot be guaranteed upon leaving the area of influence	15 minutes
Minutes until screen locking in the single-digit range	15 minutes
Restricting access to the IT infrastructure within the network to what is absolutely necessary	Role based access controls are used in conjunction with Entra, AWS IAM, and Google Workspace groups.
Logging of successful and unsuccessful authentication attempts	Directive on the use of strong passwords
Use of cryptographically strong encryption methods that are state of the art, and separation of key material and data needing encryption	Regulations for effective data deletion on hardware
	Immediate revocation of access authorizations if they are no longer required
	Prohibiting onward transfer of access data to countries that do not follow GDPR Article 44

2.3. Access Usage Control

Measures ensuring that those authorized to use the data processing procedures can only access the personal data that is subject to their access authorization.

Technical Measures	**Organizational Measures**
Logging of access to applications, specifically when entering, changing and deleting data	Use of authorization Concepts
Logging and monitoring events on system components	Number of administrators reduced to the required level
Restricting the personal data contained in the logs to the ex	Limiting access privileges to what is required for the respective role
Defined purposes and retention periods for log data	Administration concept to ensure that only trained and reviewed personnel have access to, including documented allocation and revocation of administration authorizations.
Separation of application and administration access	

2.4. Separation Control

Measures ensuring that data collected for different purposes can be processed separately.

Technical Measures	**Organizational Measures**
Separation of productive and test environments	Control via authorization concept
Physical separation (systems/databases/data carriers)	Definition of database rights

2.5. Pseudonymization

Processing personal data in such a manner that the data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separate and is subject to appropriate technical and organizational measures.

Technical Measures	**Organizational Measures**
Separation of attribution data and storage in separate and secure system (encrypted, if possible)	Internal instructions to anonymize/pseudonymize personal data as far as possible in the event of onward transfer or after the statutory deletion period has expired

3. Integrity

3.1. Onward Transfer Control

Measures to ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data is to be transmitted by data transmission devices.

- No onward transfer control measures are in place because our policy is not to share personal or private information with any third parties.

3.2. **Input Control**

Measures ensuring that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed in IT systems; an example of this is.

Technical Measures	**Organizational Measures**
Technical logging of entry, modification and deletion of data	Overview of which programs can be used to enter, modify or delete which data
Audit-proof archiving of log data	Traceability of entry, modification and deletion of data by means of individual user names (not user groups)
	Assigning rights to enter, modify, and delete data on the basis of an authorization concept
	Clear responsibilities for data deletion

4. **Availability and Resilience**

4.1. **Availability Control**

Measures to ensure that personal data is protected against accidental destruction or loss: Examples include in particular: Backup procedures

- Availability control measures are not required because the facilities are operated by Amazon AWS and Microsoft Azure.

5. **Procedures for Regular Review, Assessment, and Evaluation**

5.1. **Incident Response Management**

Support in responding to security breaches.

Technical Measures	Organizational Measures
	Documented process for detecting and reporting security incidents / data breaches (also with regard to the obligation to report to supervisory authority), including reporting to the responsible departments of the client
	Documented procedure for dealing with security incidents
	Involvement of DPO in security incidents and data breaches
	Documentation of security incidents and data breaches, e.g. via ticket system
	Process and responsibilities for the follow-up of security incidents and data breaches
	Existence of an emergency plan

6. **Default Settings with Special Regard to Data Protection**

6.1. **Privacy by Design/Default**

Technical Measures	Organizational Measures
No more personal data than necessary for the individual purpose is collected	
Simple exercise of the data subject's right of revocation through technical measures, in particular the possibility of extracting data from the system to guarantee the right under Art. 15 GDPR	
The system must enable deletion of personal data as soon as its processing is no longer necessary	

6.2. **Monitoring of Order Processing** (outsourcing to third parties)

Order processing in accordance with instructions must be guaranteed. In particular, technical and/or organizational measures for the delimitation of responsibilities between client and contractor need to be regulated.

- Measures for order processing are not required because our policy is not to share personal or private information with any third parties.

ANNEX 3

International Transfers

1. **EU SCCs**

The following elections apply to compliance with Module One (1), Two (2), and Three (3) of the EU's Standard Contractual Clauses ("EU SCCs"), and not specifically to the sections contained in this DPA. That said, collectively these elections are part of the DPA.

1.1. Clause 7 of EU SCCs (Docking clause) – Not applied.

1.2. Clause 9 of EU SCCs (use of sub-processors) – Option 2 (general written authorization) applied, and the time period is as specified in this DPA.

1.3. Clause 11 of EU SCCs (Redress) – optional wording not applied.

1.4. Clause 17 of EU SCCs (Governing Law) – Option (1) applied, and the governing law is the law of Ireland.

1.5. Clause 18 (Choice of forum and jurisdiction) – the applicable choice of forum and jurisdiction is Ireland.

1.6. For the purposes of Annex I of the Standard Contractual Clauses, Part A of Annex 1 contains the specifications regarding the parties, Part B of Annex 1 contains the description of transfer for Module Two and Module Three, and Part B of Annex 1 contains the description of transfer for Module 1, and Part C of Annex 1 contains the competent supervisory authority.

1.7. For the purpose of Annex II of the Standard Contractual Clauses, Annex 2 of this DPA contains the technical and organizational measures.

2. **UK ADDENDUM**

This UK addendum will apply to any Processing of Covered Data that is subject to the UK GDPR or both the UK GDPR and the GDPR.

2.1. For the purposes of this Paragraph 2:

"**Approved Addendum"** means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses.

"**Mandatory Clauses"** means "Part 2: Mandatory Clauses" of the Approved Addendum

2.2. With respect to any transfers of Covered Data falling within the scope of the UK GDPR from Customer (as data controller) to SuSea (as data processor)

2.2.1. To the extent necessary under Applicable Data Protection Law, the Approved Addendum as further specified in this section 2 of this Annex 3 is incorporated into and form part of this DPA;

2.2.2. For the purposes of Table 1 of Part 1 of the Approved Addendum, the parties' details are set out in Part A of Annex 1;

2.2.3. For the purposes of Table 2 of Part 1 of the Approved Addendum, the version of the Approved EU SCCs as set out in section 1 of this Annex 3 including the Appendix information are the selected SCCs; and

2.2.4. For the purposes of Table 4 of Part 1 of the Approved Addendum, SuSea (as data processor) may end the Approved Addendum.

3. **SWISS ADDENDUM**

This Swiss Addendum ("Swiss DPA") has been drafted in accordance with the Swiss Federal Data Protection Act ("FADP") and its respective Commissioner guidelines on the transfer of personal data.

3.1. Where this Addendum uses terms that are defined in the EU SCCs, those terms have the same meaning as in the EU SCCs.

3.2. For the purposes of the Swiss DPA as amended with the EU SCCs and this DPA, Customer agrees that Customer is the Controller ("data exporter"), and Company is the Processor ("data importer").

3.3. With regard to any Processing of Personal Data subject to FADP or to both FADP and the GDPR, the Swiss DPA amends this DPA and the SCC to the extent necessary so that they:

3.3.1. apply to transfers made by the Controller to the Processor, to the extent that FADP and/or the GDPR apply to the Controller's Processing when making that transfer; and

3.3.2. apply appropriate safeguards for the transfer by adhering to Article 46 of the GDPR and/or Article 6(2)(a) of the FADP, as applicable.

3.4. References to Regulation (EU) 2016/679 shall be interpreted as references to the Swiss DPA.

3.5. References to specific Articles of Regulation (EU) 2016/679 shall be replaced with the equivalent article or section of the Swiss DPA.

3.6. For the purposes of the Swiss Addendum, the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 EU SSCs. The references to the GDPR should be

understood as references to the FADP insofar as the data transfers are subject to the FADP.

3.7. Clause 13(a) and Part C of Annex 1 are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws

3.8. References to competent courts shall be replaced with references to the applicable courts of Switzerland. With respect to transfers to which the Swiss DPA applies, Clause 18(b) of the EU SCCs shall state that disputes shall be resolved before the applicable courts of Switzerland.

3.9. In the event of any direct conflict between this Addendum and the EU SCCs, the UK Addendum, and/or the Swiss DPA, the UK Addendum and/or the Swiss Addendum (as applicable) apply.

3.10. The Parties agree that if the Standard Contractual Clauses are replaced, amended or no longer recognized as valid under Data Protection Laws, or if a Supervisory Authority and/or Data Protection Legislation requires the adoption of an alternative transfer solution, the Data Exporter and Data Importer will: (i) promptly take such steps requested including putting an alternative transfer mechanism in place to ensure the processing continues to comply with Data Protection Laws; or (ii) cease the transfer of Personal Data and at the data exporter’s option, delete or return the Personal Data to the data exporter

3.11. The Swiss DPA will not be interpreted in a way that conflicts with the rights and obligations provided for in FDAP.

3.12. Customer warrants that it and/or Customer Affiliates have made any notifications to the Federal Data Protection and Information Commissioner which are required under the FDAP.