STOVA

Data Processing Addendum

This Data Processing Addendum and its Annexes ("**DPA**") reflect the mutual agreement of Stova Group, LLC ("**Stova**") and The Meeting Planners (**"Client"**) regarding the ways in which Stova can process Personal Data on behalf of Client. This DPA is supplemental to, and forms an integral part of the terms of service (including any form of master services agreement entered by the parties, the "**Agreement**") that govern Client's use of Stova's Services. Any capitalized terms used but not defined in this DPA shall have the meaning given to them in the Agreement. In the event of a conflict between the terms of this DPA and the of of the Agreement, the terms of this DPA will govern.

Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, those of its Affiliates who are authorized to use the Services under the Agreement ("**Permitted Affiliates**"). For purposes of this DPA, and except where indicated otherwise, the term "Client" will include Client and its Permitted Affiliates.

1. Definitions

Unless otherwise defined in this DPA, all capitalized terms have the meaning given to them in the Agreement.

"Data Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, and includes a Business as such term is defined under the CCPA.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"Data Protection Laws" means all local, state, national and/or foreign data protection and privacy laws, treaties and/or regulations applicable to the collection, use, transfer, storage, processing, correction, disclosure, and deletion of Personal Data under this DPA, including but not limited to EU Data Protection Laws, and the California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq. ("**CCPA**") as amended by the California Privacy Rights Act.

"EEA" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein.

"EU Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), implementations of GDPR into national law, and other applicable data protection laws of EEA member states, Switzerland and the United Kingdom (as amended, replaced or superseded).

"**European Data"** means Personal Data that is subject to the protection of EU Data Protection Laws.

"Instructions" means those written, documented instructions issued by the Data Controller to the Data Processor, directing the latter to perform a specific or general action with regard to Personal Data (including but not limited to deleting, making available, and anonymizing).

"Personal Data" means any information collected, uploaded, transferred, stored, or otherwise Processed in connection with the Services provided to Client under the Agreement that relates to an identifiable natural person (each such person, a "**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data includes names, contact information and other information defined as personal data under applicable Data Protection Laws.

"Personal Data Breach" means any actual or reasonably suspected breach of security leading to, or likely to result in, the unlawful or unauthorized use, loss, access, misappropriation, alteration, or disclosure of Personal Data.

"Privacy Policy" shall mean the Stova privacy policy, as updated from time to time, located at https://www.Stova.io/privacy-policy/.

"Processing" or "Process" means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

"Standard Contractual Clauses" means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, pursuant to Commission Implementing Decision (EU) (2021/915), available on the European Commission's website at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN.

"Sub-Processor" means a Data Processor engaged by Stova or an Stova Affiliate to assist Stova or such Affiliate in its provision of Services to Client under the Agreement. The Data Processor may be an Stova Affiliate or a third-party entity.

"Valid Transfer Mechanism" means a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring European Personal Data to a recipient outside the EEA, including but not limited to the Standard Contractual Clauses.

2. Processing Personal Data

2.1 Scope and Role of the Parties. This DPA applies to the Processing of Personal Data by Stova in the course of providing the Services. As between the parties, Client (together with its Permitted Affiliates) is the Data Controller and Stova is the Data Processor of Personal Data. Stova shall Process the Personal Data as a Data Processor only for the purpose of providing the Services described in the Agreement. In no event will Stova Process the Personal Data for its own purposes or those of any third party.

2.2 Instructions for Processing. Stova shall Process Personal Data in accordance with the Privacy Policy and Client's Instructions. Client hereby instructs Stova to Process Personal Data as necessary to provide the Services in accordance with the Agreement (including this DPA). Client may provide additional Instructions to Stova to Process Personal Data, however Stova shall be obligated to perform such additional Instructions only if they are consistent with the terms and scope of the Agreement and this DPA.

2.3 Compliance with Laws. Stova shall comply with all Data Protection Laws applicable to Stova in its role as a Data Processor Processing Personal Data.

2.4 Client Authority. Client represents and warrants to Stova that Client has obtained the Personal Data in accordance with the requirements of applicable Data Protection Laws, and that Client is and will at all time remain duly and effectively authorized to give the instruction set out in Section 2.2.

3. Sub-Processors

3.1 Use of Sub-Processors. Client agrees that Stova and Stova Affiliates may engage Sub-Processors to Process Personal Data when necessary to provide the Services. Stova or the relevant Stova Affiliate shall ensure that each such Sub-Processor abides by data processing terms no less protective of Personal Data than those provided in this DPA (including, where appropriate, the Standard Contractual Clauses). Stova agrees that it will remain responsible to Client for each Sub-Processor's compliance with the obligations of this DPA, and shall be liable to Client for the acts and omissions of any Sub-Processors with respect to Personal Data, to the same extent as if the acts or omissions were performed by Stova.

3.2 Notification of New Sub-Processors. Stova has currently appointed, as Sub-Processors, those Stova Affiliates and third parties listed in Annex III attached hereto (the "Authorized Sub-Processors"), and shall provide written notice to Client as provided in the Agreement (or in any event at least 30 days in advance) if Stova adds any new Sub-Processor to Annex III.

4. Data Processing Location and Data Transfers

4.1 Location of Processing Personal Data. Client acknowledges and agrees that Stova may access and Process Personal Data on a global basis as necessary to provide the Services in accordance with the Agreement, and that Personal Data will be transferred to and Processed by Stova Group, LLC in the United States and to other jurisdictions where Stova Affiliates and other Sub-Processors have operations. Upon Client request, Stova will make available to Client a list of the locations where it Processes Personal Data.

5. Additional Terms for European Data. The provisions of this Section 5 shall apply only with respect to European Data, if any, Processed by Stova.

5.1 Scope. Stova will Process European Data only as necessary to provide the Services.

5.2 Roles. When Processing European Data, as between Stova and Client for the purposes of the descriptions in the Standard Contractual Clauses, the parties agree that Stova is the Data Processor and the "data importer" (as defined in the Standard Contractual Clauses), and that Client is the Data Controller and the "data exporter" (as defined in the Standard Contractual Clauses), notwithstanding that Client may be located outside the EEA and may itself be a Data Processor acting on behalf of third party Data Controllers.

5.3 Transfers of European Data. Stova will not transfer European Data to any country or recipient not formally recognized by the European Commission as providing an adequate level of data protection unless Stova has (i) implemented a Valid Transfer Mechanism for the European Data, or (ii) received prior written consent from Client. Client hereby consents to the transfer by Stova of Personal Data to its Sub-Processors identified on Annex III hereto, as necessary to provide Client with Services pursuant to the Agreement, and subject to a Valid Transfer Mechanism.

5.4 Transfers to Stova. Client acknowledges that in its provision of the Services, Stova is likely to receive European Data in the United States. The parties therefore acknowledge and agree the following:

5.4.1 Stova agrees to abide by and Process European Data in compliance with the Standard Contractual Clauses, and such Standard Contractual Clauses are incorporated by reference into and form an integral part of this DPA.

5.4.2 If and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail. In no event does this DPA restrict or limit the rights of any Data Subject or of any competent supervisory authority.

5.4.3 Although Stova does not rely on the EU-US Privacy Shield as a legal basis for transfers of European Data in light of the judgment of the EU Court of Justice in Case C-311/18, for as long as Stova is self-certified to the Privacy Shield, Stova will Process European Data in compliance with Privacy Shield principles.

5.4.4 To the extent Client requires Stova assistance to meet its obligations under Article 35 and 36 of the GDPR to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Client's use of the Service, Stova will, taking into account the nature of Processing and the information available to Stova, provide reasonable assistance to Client.

5.5 Sub-Processors of European Data.

5.5.1 Sub-Processor Objection Right. Stova will notify Client of any changes to Sub-Processors of European Data by updating Annex III to this DPA, and will provide Client the opportunity to object to the engagement of the new Sub-Processor on reasonable grounds relating to Personal Data protection within thirty (30) days of the update to Annex III. If Client notifies Stova of such an objection within thirty (30) days, the parties will discuss the Client's concerns in good faith and use commercially reasonable efforts to achieve a resolution. Should no resolution be reached, and should Stova choose to retain the objected-to Sub-Processor, Client may elect to suspend or discontinue using the relevant portion(s) of the Service and may terminate the relevant portion(s) of the Service. Upon any such termination by Client of the Service Agreement, in whole or in part, pursuant to this Section, Stova shall refund Client any prepaid fees for the terminated portion(s) of the Service that were to be provided after the effective date of termination.

5.5.2 Sub-Processor Agreements. For purposes of clause 9(c) of the Standard Contractual Clauses, Client acknowledges that Stova may be restricted from disclosing Sub-Processor agreements to Client, but Stova agrees to use reasonable efforts to request any Sub-Processor to disclose the Sub-Processor agreement to Client and will provide (on a confidential basis) all Sub-Processor information reasonably possible without breaching any obligations of confidentiality Stova may have to the Sub-Processor.

5.6 Access by Government Authorities. In accordance with Article 46 of the GDPR and the Standard Contractual Clauses, and without prejudice to any provisions of this DPA, Stova undertakes the following additional safeguards to secure European Data transferred pursuant to the Standard Contractual Clauses:

5.6.1 For the purposes of safeguarding European Data when any government or regulatory authority requests access to such data, and unless required by a valid court order or if otherwise Stova may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to European Data, or where the access is requested in the event of imminent threat to lives, Stova will:

5.6.1.1 not provide the source code or encryption keys to any government agency for the purpose of accessing European Data; and

5.6.1.2 upon Client's written request, provide reasonable available information about the requests of access to European Data by government agencies Stova has received in the 6 months prior to Client's request.

5.6.2 If Stova receives a request by a government agency to access European Data, Stova will notify Client of such request to enable the Client to take necessary actions, to communicate directly with the relevant authority and to respond to the request. If Stova is prohibited by law to notify the Client of such request, Stova will make reasonable efforts to challenge such prohibition through judicial action or other means at Client's expense and, to the extent possible, will provide only the minimum amount of information necessary.

5.7 **Standard Contractual Clauses**. For purposes of the Standard Contractual Clauses, the parties agree to the following (provided, if and to the extent a Permitted Affiliate relies on the Standard Contractual Clauses for the transfer of European Data, any references to "Client" in this Section 5 include such Affiliate):

5.7.1 The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA.

5.7.2 With respect to the transfer of European Data, the parties shall abide by the terms of the Standard Contractual Clauses as set out in **MODULE 2 (Controller to Processor)**.

5.7.3 The Docking Clause option under clause 7 shall apply.

5.7.4 The DPA and the Service Agreement are Client's complete and final documented Instructions at the time of signature of the Service Agreement for the Processing of Personal Data.

5.7.5 The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the audit provisions detailed in Section 12 of this DPA.

5.7.6 Option 2 under clause 9 of the Standard Contractual Clauses will apply with respect to any Sub-Processor. For purposes of clause 9(a), Stova has Client's general authorization to engage Sub-Processors in accordance with Section 3 and Section 5.5 of this DPA.

5.7.7 The option under clause 11 (Redress) shall not apply.

5.7.8 The information required for purposes of the Appendix to the Standard Contractual Clauses will be completed as follows:

5.7.8.1 The contents of Part A of Annex I of this DPA will form Annex I.A. to the Standard Contractual Clauses.

5.7.8.2 The contents of Part B of Annex I of this DPA will form Annex I.B. to the Standard Contractual Clauses.

5.7.8.3 The contents of Part C of Annex I of this DPA will form Annex I.C. to the Standard Contractual Clauses.

5.7.8.4 The contents of Annex II of this DPA will form Annex II to the Standard Contractual Clauses.

5.7.8.5 The contents of Annex III of this DPA will form Annex III to the Standard Contractual Clauses.

6. Cooperation; Rights of Data Subjects

6.1 Cooperation. Stova will, as necessary to enable Client to meet its obligations under applicable Data Protection Laws, provide reasonable and timely assistance to Client to (i) maintain up-to-date and accurate records regarding Personal Data, (ii) respond to any Data Subject Request (as defined in Section 6.4 below); and (iii) respond to any other correspondence, enquiry or complaint received from a Data Subject, regulator, court or other supervisory authority in connection with the Processing of Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Stova, Stova shall promptly inform Client and shall not respond to the communication unless required by law or authorized by Client.

6.2 Deletion or Restriction. Stova will either (i) provide Client the ability within the Service to correct or delete Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Client's behalf if such functionality is not available within the Service. Stova shall comply with Client's reasonable Instructions in relation to the correction, deletion and blocking of Personal Data.

6.3 Access to Personal Data. To the extent a Data Subject's Personal Data is not accessible to Client through the Service, Stova will, as necessary to enable Client to meet its obligations under applicable Data Protection Laws, provide reasonable assistance to make such Personal Data available to Client.

6.4 Handling of Data Subject Requests. Client is responsible for responding to a Data Subject's request to exercise any of its rights under relevant Data Protection Laws (including such Data Subject's rights of access, correction, objection, deletion, restriction of Processing and data portability of its Personal Data) ("**Data Subject Request**"). If Stova receives a Data Subject Request, Stova shall promptly redirect the Data Subject to Client.

6.5 Data Portability. During the term of the Agreement, Stova shall ensure that Client can extract Personal Data from the Service in a structured, commonly used and machine-readable format such that Client can provide the Personal Data to an individual who makes a data portability request under EU Data Protection Laws.

7. Government Access Requests

Unless prohibited by applicable law or a legally-binding request of law enforcement, Stova shall promptly notify Client of any request by government agency, judicial body or law enforcement authority for access to or disclosure of Personal Data.

8. Stova Personnel

Stova shall take reasonable steps to require screening of its personnel who may have access to Personal Data, and shall ensure such personnel (i) Processes Personal Data in accordance with Client's Instructions as set forth in this DPA; (ii) receives appropriate training on its responsibilities regarding the handling and safeguarding of Personal Data; and, (iii) is subject to confidentiality obligations designed to safeguard Personal Data from unauthorized access, use or disclosure.

9. Personal Data Breach

In the event Stova becomes aware of a Personal Data Breach, it shall, without undue delay (but in any event within forty-eight (48) hours), notify Client. Stova's notification shall include, to the extent known at the time of notification (i) a description of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) a description of the likely consequences of the Personal Data Breach, and (iii) a description of the measures taken or proposed to be taken by Stova to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. If Stova is unable to provide all of the information listed above as part of the initial notification, Stova will provide this information to Client as soon as reasonably practicable. To the extent Client requires additional information from Stova to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, Stova shall provide reasonable assistance to provide such information to Client taking into account the nature of Processing and the information available to Stova.

10. Security Program

Stova shall implement appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as set forth in the Agreement, including the implementation of appropriate Stova security policies, which are available to Client upon request.

11. Cardholder Data

In the event a Stova Affiliate Processes credit or debit card payment information, it does so in compliance with all applicable Payment Card Industry Security Standard (PCI DSS) requirements, and is PCI DSS Level 1 certified.

12. Audit; Demonstration of Compliance

Stova shall make available to Client, upon Client's written request, copies of any relevant summaries of external security certifications, security audit reports, penetration tests or other information reasonably necessary to demonstrate compliance with this DPA. Client shall be entitled to audit Stova's compliance with this DPA; provided, such audit shall occur not more than once a year, save for in the event of a Personal Data Breach where an additional audit may be conducted by Client. An audit shall be conducted following reasonable prior written notice and may include, but not be limited to, a site visit (during normal office hours and with reasonable prior notice), and a review of Stova's policies, procedures and other documentary evidence as reasonably required by Client.

13. Return and Deletion of Personal Data

Upon Client's request at any time during the term of the Agreement or upon termination of the Agreement, Stova shall immediately cease Processing the Personal Data and, if Client makes a request within sixty (60) days following the termination of the Agreement, Stova will provide Client with access to the Services solely to the extent necessary for Client to retrieve the Client Data from the Platform. Stova has no obligation to maintain or provide Client Data beyond such sixty-day period, after which Stova will remove or render unreadable all Client Data on the Platform, except for (A) data required to be retained by Applicable Law, or (B) data that has been archived on Stova's back-up systems, which will not be subject to further Processing and will be deleted pursuant with Stova's standard data deletion practices.

14. Additional Terms for California Personal Information. The provisions of this Section 14 will apply only with respect to Personal Data that is subject to California Civil Code Sec. 1798.100 et seq., also known as the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act (such Personal Data, "California Personal Information").

14.1 In connection with the Processing of California Personal Information pursuant to Client's Instructions, Stova is a "Service Provider," Client is a "Business," and the term Data Subject includes "Consumer" as such terms are defined under the CCPA, as amended.

14.2 The parties acknowledge and agree that Stova will Process California Personal Information strictly for the purpose of performing the Services under the Agreement or as otherwise permitted by the CCPA, as amended. In particular, Stova will not: (i) sell Client's California Personal Information; (ii) retain, use or disclose Client's California Personal Information for a commercial purpose other than providing the Services in accordance with the Agreement; or (iii) retain, use or disclose California Personal Information outside of the direct business relationship between Stova and Client. Additional information about Client's rights with respect to Stova's Processing of California Personal Information is included in the Stova Privacy Policy.

15. General Provisions

15.1 Disclosure of DPA Terms. Client or its Permitted Affiliates may disclose the terms of this DPA to a data protection regulatory authority to the extent required by law or regulatory authority.

15.2 Termination. The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement, or (ii) when all Personal Data is deleted from, or rendered unusable within, Stova's systems.

15.3 Conflict. This DPA is subject to the non-conflicting terms of the Agreement. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.

15.4 Headings. The section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPA.

15.5 Updates. Stova may update this DPA from time to time, and will provide Client with written notice of any such updates in accordance with the Agreement.

15.6 Miscellaneous. The legal entity agreeing to this DPA as Client represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and each of its Permitted Affiliates. Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Stova directly by itself, the parties agree that (i) solely the Client entity that is the contracting party to the Agreement will exercise any right or seek any remedy a Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Client entity that is the contracting party to the Agreement will exercise any such rights under this DPA in a combined manner for itself and all of its Permitted Affiliates together.

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

CLIENT	**STOVA GROUP, LLC**
By: ___________________________________	By: ___________________________________
Name: ________________________________	Name: ______________________________
Title: ________________________________	Title: ________________________________
Date: ________________________________	

STOVA

ANNEX I to the DPA
DETAILS OF PROCESSING/TRANSFER

PART A – LIST OF PARTIES

Data Exporter:

Name: The Client, as defined in the DPA, on behalf of itself and its Permitted Affiliates
Address: Client's address, as set out in the most recent Order Form entered by the parties
Contact person's name, position and contact details: Client's contact details, as set out in the most recent Order Form entered by the parties.
Activities relevant to the data transferred under these Clauses: The Processing of Personal Data in connection with Client's use of Stova Services pursuant to the Agreement.
Role: Controller

Data Importer:

Name: Stova Group, LLC.
Address: 16217 South Bringhurst Blvd., Suite 300, Bluffdale, Utah 84065, USA
Contact person's name, position and contact details: Jesse Braughler, Information Security Officer and Data Protection Officer, Email: privacy@stova.io Telephone: +1-800-516-4265
Activities relevant to the data transferred under these Clauses: The Processing of Personal Data in connection with Stova's provision of Stova Services to Client pursuant to the Agreement
Role: Processor

Feltkode ændret

PART B – DESCRIPTION OF PROCESSING AND TRANSFER

Categories of Data Subjects whose Personal Data is Processed/Transferred

Client may submit personal data to Stova, the extent of which is determined and controlled by the by the Client in its sole discretion, and which may include, but is not limited to, personal data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Client (who are natural persons);
- Employees or contact persons of Client's prospects, customers, business partners and vendors;
- Employees, agents, advisors, contractors of Client (who are natural persons);
- Natural persons who are invited to, register for, or otherwise attend events organized or hosted by Client; and
- Client's users authorized by the Client to access the services provided by Stova.

Categories of Personal Data Processed/Transferred:

In connection with its receipt of Services under the Agreement, Client may submit Personal Data to Stova, the extent of which is determined and controlled by the Client in its sole discretion. Such Personal Data may include, but is not limited to the following categories of personal data:

- Identification Data (Name, personal address, personal email addresses and other contact information)
- Employment Information (Title; Employer; Business address, business email address and other corporate contact information; Professional life data)
- Personal life data (e.g., meal preferences);
- Financial Data (payment information);
- Connection and usage data; and
- Location data.

Sensitive Data Processed/Transferred:

The parties do not anticipate the Processing or transfer of sensitive categories of data.

Frequency of the Processing

Continuous for the duration of the Agreement term.

Nature and Purpose of the Processing, and any Transfers or further Processing:

Stova is providing Client with a cloud-based event management platform and related services for the organization, hosting and management of conferences, business meetings, seminars and other corporate events organized or hosted by Client. Stova will be collecting, storing, transferring and otherwise Processing Personal Data of individuals who are invited to, register for, or otherwise participate in one or more of Client's events, and from Client's employees and agents who administer any such event. Processing shall occur upon the Instruction of the Client, as data exporter, in accordance with the terms of the Agreement (including this DPA) in effect between the Client and Stova. Personal Data may be subject to the following Processing activities:

1. Storage and other Processing activities necessary to provide, maintain and improve the Services provided to Client; and/or
2. Transfer or disclosure in accordance with the Agreement (including this DPA) and/or as required by Applicable Laws.

Period for which Personal Data will be Retained:

Unless otherwise agreed by the parties in writing, Stova will Process and retain Personal Data for the duration of the Agreement, subject to Section 13 (Return and Deletion of Personal Data) of the DPA.

PART C – COMPETENT SUPERVISORY AUTHORITY

For the purposes of European Data Processed in accordance with the Standard Contractual Clauses, the competent supervisory authority shall be as follows: (i) where Client is established in an EU member state, the supervisory authority with responsibility for ensuring Client's compliance with the GDPR shall act as competent supervisory authority; (ii) where Client is not established in an EU member state, but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU member state in which Client's representative is established shall act as competent supervisory authority; or (iii) where Client is not established in an EU member state but falls within the extra-territorial scope of the GDPR without however having to appoint a representative, the supervisory authority of the EU member state in which the Data Subjects are predominantly located shall act as competent supervisory authority.

In relation to Personal Data that is subject to (i) the GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); or (ii) the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"), the competent supervisory authority is the United Kingdom Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner (as applicable).

STOVA

ANNEX II to the DPA

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. Security Program and Standards

Stova, as a Data Processor and data importer, maintains appropriate administrative, physical and technical safeguards to protect the security, confidentiality and integrity of Personal Data provided to Stova in the course of performing the Services pursuant to the Agreement in effect between the parties, including but not limited to documented data and information security policies, secure coding practices, encryption policies, data storage and deletion protocols, anti-virus protections, password policies, system and facility access controls, service monitoring and management procedures, disaster recovery and business continuity plans, and personnel security training. Specific measures and safeguards are detailed below.

2. Access Controls

A. Preventing Unauthorized Product Access and Use

Outsourced processing: We host our Service with outsourced cloud infrastructure providers (Amazon Web Services, Microsoft). Additionally, we maintain carefully structured contractual relationships with vendors and contractors in order to provide the Services in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor due diligence and compliance programs in order to protect any data Processed or stored by 3rd parties.

Physical/environmental security: Our product infrastructure is hosted with multi-tenant, outsourced cloud service providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance annually, among other certifications.

Authentication: Multi Factor Authentication (MFA) is implemented and required for access to all our customer products in addition to all other environments.

Authorization: We enforce a least-privilege model and as such only appropriately assigned individuals can access relevant application features as assigned by their administrator. Customers are not allowed access to the underlying application infrastructure.

Storage: Data is stored in multi-tenant storage systems which is encrypted at rest. Access to the data storage repositories is also controlled by Multi Factor Authentication (MFA), in addition to signing an NDA for access to the customer data.

Internal Network: We have implemented industry standard technical access and detection capabilities to protect the internal network infrastructure that supports our products.

Logging and alerting: We log all system activity including system behavior, all communication, all levels of authentication and APE calls. Any abnormalities or malicious activities are alerted and investigated by

our security operations team. For any confirmed incidents we take appropriate steps to minimize product and customer disruptions. Notifications are in accordance with the terms of the agreement.
We implement a Virtual Private Network (VPC) with all our Cloud Service Providers (CSPs) giving us the ability to customize access controls and firewall rules at a granular level.

Penetration testing: We engage with industry recognized penetration testing service providers for annual penetration tests to identify and remediate any potential attack vectors.

Code testing: We perform static and dynamic code analysis: We perform security reviews of all code within our repositories against OWASP best practices and other vulnerabilities.

B. Limiting Internal Privileges and Authorization Requirements

Personnel Screening: All of our personnel are subject to a third-party background check prior to being extended an employment offer, subject to applicable laws.

Control Environment: Employees enter into written obligations of confidentiality, and are required to conduct themselves in a manner consistent with company privacy policies, non-disclosure requirements, and ethical standards. Access to data is provided to that subset of employees who have a "need to know" in order to provide the Services, including to provide customer support, mitigate potential problems, and detect and respond to security incidents. Employees are granted access based on role, and access products and data via controlled, password protected, interfaces.

Security Training and Awareness. Stova maintains a security awareness program that includes annual training of personnel on Stova's security policies and data privacy best practices.

3. Data Transmission Controls

In-transit: We implement encryption on all data communication (logins, customer sites) using NIST based cryptographic algorithms. All web traffic is via https with TLS.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

4. Availability Controls

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Backup replication: Our production databases are designed to replicate data between a primary and backup database using industry standard backup methods to create resiliency.

STOVA

ANNEX III to the DPA

LIST OF SUB-PROCESSORS

Third-Party Sub-Processor Name	Region(s)	Purpose of Processing
Amazon Web Services	Servers may be located in North America (United States), the EU (Ireland), or APAC (Australia), as selected by Client.	Cloud Hosting Services
Microsoft Azure	United States	Cloud Hosting Services (For Stova's On-Site Services Tools)
Google Analytics	United States	Usage analytics
Agora.io	United States	Video CDN Provider
Drift	United States	Website Chat Bot Provider
Firebase	United States	Real time database for statistics and real time chat in Stova Virtual Platform
IOIO.TV, LLC	United States	Video processing and streaming services
Mailgun Technologies, Inc.	Servers located in North America or the EU, as selected by Client.	Email delivery services (for Client emails sent through the Stova registration platform)
Mandrill	United States	SMTP Email for Stova Virtual Platform
Restream Inc.	United States	Video streaming services for live events.
Salesforce	United States	Client account and relationship management tool
SendInBlue	United States	SMTP Email for Stova Virtual Platform
Stripe	United States	Payment Processing
Twilio, Inc.	United States	Video CDN Provider
ZenDesk, Inc	United States	Client Support Tickets

Affiliate Sub-Processor Name	Region(s)	Purpose of Processing
*Aventri, LLC	United States Headquarters: 16217 South Bringhurst Blvd., Suite 300, Bluffdale, Utah 84065	Sales, Professional Services, Event Technology, and Customer Support Services
*MeetingPlay, LLC	United States Headquarters: 16217 South Bringhurst Blvd., Suite 300, Bluffdale, Utah 84065	Sales, Event Technology, Onsite Services, and Customer Support Services
*Eventcore, LLC	United States Headquarters: 16217 South Bringhurst Blvd., Suite 300, Bluffdale, Utah 84065	Sales, Event Technology, and Customer Support Services
*Aventri (UK) Ltd.	United Kingdom	Sales and Customer Support Services
*Aventri Asia Pacific Pty. Limited	Australia	Sales and Customer Support Services
*Aventri India Private Ltd.	Pune, India	Customer Support Services and Software Development
*TapCrowd BVBA	Belgium	Customer Support Services and Mobile Application Services
*ITN International LLC	United States: 16217 South Bringhurst Blvd., Suite 300, Bluffdale, Utah 84065	On-Site Services
*Aventri (Calgary) Corp.	Calgary, Alberta, Canada	On-Site Services and Software Development

* The marked Sub-Processors are Stova's wholly-owned operating subsidiaries.

STOVA

ANNEX IV to the DPA

STANDARD CONTRACTUAL CLAUSES

Module Two: Controller to Processor (C2P)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent suspensory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland (without reference to conflicts of law principles).

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the jurisdiction specified in Clause 17.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

This Addendum amends the Standard Contractual Clauses to transfers of Personal Data from the United Kingdom and transfers of Personal Data from Switzerland, to the extent that (i) the GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); or (ii) the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA") (in each case, as may be amended, superseded or replaced) apply to the data exporter's Processing activities.

The Standard Contractual Clauses shall be amended with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR or Swiss DPA (as applicable);

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to the "UK" or "Switzerland" (as applicable);

(v) Clause 13(a) is not used and the "competent supervisory authority" shall be the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

(viii) to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state: "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

(ix) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts."