GDPR DATA PROCESSING AGREEMENT FOR ORGANIZERS

This General Data Protection Regulation Data Processing Addendum ("DPA") is entered into by and between Organizer and ATIV Solutions, LLC, on behalf of itself, and forms part of the Contract for Services previously entered into under the EventPilot Technical Provider Agreement (the "Principal Agreement") by and between the Organizer and ATIV to reflect the parties agreement with regard to the Processing of Personal Data in accordance with the requirements of applicable data protection laws. This DPA is entered into as of the later of the dates beneath the parties signatures below. This DPA includes the European Union's Standard Contractual Clauses (Processor) incorporated herein as Attachment 1. All capitalized terms not defined shall have the meaning set forth in the Principal Agreement.

How to Execute this DPA

This DPA has been pre-signed on behalf of the applicable ATIV entities and consists of two parts; the main body of the DPA and Attachment 1. When ATIV receives the completed and signed DPA as specified below, this DPA will become a legally binding addendum to the Principal Agreement.

Data Processing Terms

In providing the Services to the Organizer pursuant to the Principal Agreement, ATIV may process Personal Data on behalf of Organizer. ATIV will comply with the provisions in this DPA with respect to its processing of any Personal Data

Capitalized terms used but not defined in this DPA have the same meanings as set out in the Principal Agreement.

1. Definitions

1.1 For the purposes of this DPA:

a. "Controller" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

b. "Organizer" means the non-ATIV party to both the Agreement and this DPA that has access to the Services.

c. "Data Subject" means the individual to whom the Personal Data relates.

d. "Applicable Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom, applicable to the Processing of Personal data under the Principal Agreement.

e. "Personal Data" means any personally identifiable information under Applicable Data Protection Laws.

f. "Organizer Personal Data" means any Personal Data processed by the Organizer as a Controller, or, as the case may be (and in accordance with Sec 3.1 below), as a Processor as set out in Attachment 1.

g. "Processor" means an entity which processes Personal Data on behalf of the Controller.

h. "Sub-processor" means any person appointed by or on behalf of the Processor, or by or on behalf of an existing Sub-processor, to process Personal Data on behalf of the Controller.

i. "Services" means the Software as a Service and associated professional services provided by ATIV to Organizer under the Principal Agreement.

j. "Security Incident" means accidental or unlawful destruction, loss, alterations, unauthorized disclosure, access or use.

k. "Standard Contractual Clauses" means, as applicable, the agreement executed by and between Organizer and ATIV and attached hereto as Attachment 1 pursuant to the European Commission on 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.

2 Applicability of DPA

2.1 **Applicability**: This DPA shall apply only to the extent Organizer or ATIV are established within the United Kingdom, EEA or Switzerland and/or to the extent ATIV processes Organizer Personal Data of Data Subjects located in the United Kingdom, EEA, or Switzerland on behalf of Organizer or Organizer Affiliate or otherwise Organizer or ATIV are subject to the Applicable Data Protection Laws.

3 Roles and Responsibilities

3.1 **Parties Roles**: Organizer, as Controller, appoints ATIV as a Processor to process the Organizer Personal Data on Organizer's behalf. In some circumstances Organizer may be a Processor, in which case Organizer appoints ATIV as Organizer's sub-processor, which shall not change the obligations of either Organizer or ATIV under this DPA, as ATIV will remain a Processor with respect to the Organizer in such event. However, the Organizer shall notify and keep ATIV updated on whether ATIV acts, in relation to specific processing activities, as a Processor or a Sub-processor, and if the latter is the case on the identity of the actual Controller.

3.2 **Purpose Limitation:** ATIV shall process Organizer Personal Data for the purposes set forth in the Principal Agreement and only in accordance with the lawful, documented instructions of the Organizer (including with regard to transfers of Organizer Personal Data to a third country), unless ATIV is required to process Organizer Personal Data by the Applicable Data Protection Laws to which ATIV is subject to (in such a case, ATIV shall inform the Organizer of that legal requirement before processing, unless applicable law prohibits such information). The Organizer's instructions may be specific or of a general nature as set out in this DPA or as otherwise notified by the Organizer from time to time and not for ATIV's own purposes. ATIV may refrain from execution of the Organizer's instructions if it notifies the Organizer immediately that, in ATIV's opinion, an instruction for the processing of Organizer Personal Data given by the Organizer infringes Applicable Data Protection Laws. The purpose of this Section 3.2 is only to determine the scope and purposes of processing Organizer Personal Data by ATIV and nothing in this DPA will be deemed an obligation of ATIV to accept any instructions of the Organizer other than provided under the Principal Agreement.

3.3 **Training**: ATIV shall ensure that its relevant employees, agents, and contractors receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Organizer Personal Data.

3.4 **Compliance**: Organizer, irrespective of the Organizer's role as a Controller or a Processor, shall be responsible for ensuring that, in connection with the Organizer Personal Data and the Services:

a. It has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including Applicable Data Protection Laws; and

b. it has, and will continue to have, the right to transfer, or provide access to, the Organizer Personal Data to ATIV for processing in accordance with the terms of the Principal Agreement and this DPA.

3.5 If Organizer uses the Services to process any categories of Personal Data not expressly covered by this DPA, Organizer acts at its own risk and ATIV shall not be responsible for any potential compliance deficits related to such use.

3.6 **ATIV Employees/Contractors Personal Data**: Where ATV discloses ATIV employees'/contractors' Personal Data to the Organizer or an ATIV employee/contractor provides Personal data directly to Organizer, which the Organizer processes to manage its use of the Services, Organizer shall process that Personal Data in accordance with its privacy policies and

applicable privacy laws, in particular Applicable Data Protection Laws. Such disclosures shall be made by ATIV only where lawful for the purposes of contract management, service management or security purposes.

4. Security

4.1 **Security**: ATIV shall implement appropriate technical and organizational measures designed to protect the Organizer Personal Data from a Security Incident and in accordance with ATIV's security standards as set forth in the Principal Agreement as well as the Applicable Data Protection Laws (including Article 32 of the GDPR). ATIV will also, taking into account the nature of processing and the information available to ATIV, assist the Organizer in ensuring its compliance with the obligations pursuant to Article 32 of the GDPR.

4.2 **Confidentiality of Processing**: ATIV shall ensure that any person that it authorizes to process Organizer Personal Data (including its staff, agents, and subcontracts) shall be subject to a duty of confidentiality (whether contractual or a statutory duty) that shall survive the termination of their employment and/or contractual relationship.

4.3 **Security Incidents**: Upon becoming aware of a confirmed Security Incident, ATIV shall notify Organizer without undue delay and pursuant to the terms of the Principal Agreement and shall provide such timely information as Organizer may reasonably require to enable Organizer to fulfill any data breach reporting obligations under Applicable Data Protection Laws. ATIV will take steps to identify and remediate the cause of such Security Incident and to minimize its possible harm. For the avoidance of doubt, Security Incidents will not include unsuccessful attempts to, or activities that do not compromise the security of the Organize Personal Data including, without limitation, unsuccessful login attempts, denial of service attacks and other attacks on firewalls or networked systems.

5. Onward Transfers: Sub-Processing

5.1 ATIV makes available the transfer mechanisms listed below which shall apply, in the same order of precedence as set out below, to any transfers of Organizer Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such Applicable Data Protection Laws:

a) Standard Contractual Clauses attached as Attachment 1.

5.2 In the event that EU authorities or courts or UK Information Commissioner's Office determine that any of the transfer mechanisms above is no longer an appropriate basis for transfers, ATIV and Organizer shall promptly take all steps reasonably necessary to demonstrate adequate protection for the Organizer Personal Data, using another approved mechanism. ATIV understands and agrees that Organizer may terminate the transfers as needed to comply with the Applicable Data Protection Laws. In the event the Standard Contractual Clauses (or any other approved mechanism allowing for EU-US Personal Data transfers) are applicable, nothing in this DPA modifies or affects any commission or supervisory authority's or Data Subject's rights under the Standard Contractual Clauses (or any such other approved mechanism).

5.3 Organizer agrees that ATIV may engage third parties as sub-processor to process the Organizer Personal Data on ATIV's behalf. ATIV shall provide on its website a list of Sub-Processors that are currently engaged by ATIV to carry out specific processing activities on behalf of the Organizer. ATIV will update the list at the following website: https://ativ.me/subprocessors. Notwithstanding other provisions in this section, ATIV may add or replace a Sub-Processor immediately if it is necessary to ensure business continuity and recovery in case of emergency, except as prohibited by Applicable Data Protection Laws. ATIV will ensure sub-processors provide at least the level of data protection required of ATIV by this DPA and shall remain liable for any breach of the DPA caused by a Sub-Processor. Where the Standard Contractual Clauses are applicable, ATIV shall enter into Standard Contractual Clauses with such Sub-Processors or use/take advantage of any other approved mechanism, including Binding Corporate Rules or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

6. Cooperation

6.1 **Data Subjects' Rights**. ATIV shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Organizer to respond to any inquiry, communication, or request from a Data Subject seeking to exercise his or her rights under Applicable Data Protection Laws, including rights of access, correction, restriction, objection, erasure or data portability, as applicable. In the event such inquiry, communication, or request is made directly to ATIV, ATIV shall promptly inform Organizer by providing the full details of the request. For the avoidance of doubt, Organizer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure, or data portability of that Data Subject's Personal Data. ATIV will be responsible for responding to Data Subject's request for access, correction, restriction, objection, erasure or data portability or any other request from a Data Subject seeking to exercise his or her rights under Applicable Data Protection Laws to the extent Organizer itself does not have the ability, with the available standard functionalities of the Services, to respond to such request. ATIV reserves the right to reimbursement from Organizer for the reasonable cost of any time, expenditures, or fees incurred in connection with such assistance provided to Organizer.

6.2 **Data Protection Impact Assessments and Prior Consultation**: ATIV shall, to the extent required by Applicable Data Protection laws, provide Organizer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that the Organizer is required to carry out under Applicable Data Protection Laws.

7. Security Reports and Audits

7.1 ATIV will allow for and contribute to audits, including inspections, conducted by Organizer in accordance with Organizer's rights under the Principal Agreement. If the Principal Agreement does not include audit rights, ATIV and Organizer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit; and ATIV reserves the right to charge a reasonable fee (based on ATIV's reasonable costs) for any such audit. ATIV will provide further details of any applicable fee and the basis of its calculation to Organizer in advance of such audit. The purpose of an audit pursuant to this clause will be strictly limited to verifying whether ATIV is processing Organizer Personal Data in accordance with the obligations hereunder and Applicable Data Protection Laws.

7.2 Notwithstanding the above, ATIV will, subject to the confidentiality arrangements that will satisfy both parties, make available to Organizer all information held by ATIV necessary to demonstrate its compliance with the obligations laid down in the Applicable Data Protection Laws. If Organizer wishes to receive such further information to which it is entitled under Applicable Data Protection Laws, Organizer shall submit a request for additional information to ATIV in writing for that additional information. Where ATIV is in possession of such information, and subject to the aforementioned confidentiality arrangements, ATIV shall supply this information to Organizer as soon as reasonably practicable.

8. Deletion or Return of Organizer Personal Data

8.1 **Deletion or Return of Data**: Upon termination or expiration of the Principal Agreement, ATIV shall, in accordance with the terms of the Principal Agreement, delete all project data, including all Organizer Personal Data in ATIV's possession. Organizer is responsible for downloading and storing analytics reports or other content for reference before the expiration of the Principal Agreement. To the extent that ATIV is required by any applicable law or a governmental or regulatory order to retain some or all of the Personal Data, or if it is otherwise subject to liability for not retaining some or all of the Personal Data. In such event, ATIV shall extend the protection of the Principal Agreement and this DPA to such Organizer Personal Data and limit any further processing of such Organizer Personal Data to only those limited purposes that require the retention for so long as ATIV maintains the Organizer Personal Data.

9. Miscellaneous

9.1 In the event that ATIV, any of its Sub-processors, or Organizer receives any regulatory request, order, or other binding decision or recommendation from the competent authority that requires amendments to the provisions hereof or any changes to the processing of Organizer Personal Data hereunder ("**Regulatory Request**"), ATIV and Organizer as well as, to the extent

necessary and/or reasonably practicable, representatives of a respective Sub-processor, shall, within a reasonable time after receiving and reviewing the Regulatory Request, discuss and work in good faith towards agreeing on a plan ("**Compliance Review Plan**") to determine the details of how the Regulatory Request can be addressed. A timeframe for reviewing the Regulatory Request and preparing the Compliance Review Plan will be agreed between the parties, taking into account the requirements of Applicable Data Protection Laws and the urgency of the matter as well as doing everything commercially reasonable given the circumstances and nature of the Services to meet specific time frames set by the relevant authority in connection with the Regulatory Request. If ATIV, any of its Sub-processors, or Organizer believe that it is not possible to meet a specific time frame set by the relevant authority in connection with the Regulatory Request, ATIV and/or its Sub-processor will assist Organizer to explain this to the relevant authority, including by providing details of the reasons why the timeframes cannot be met.

9.2 Except as amended by this DPA, the Principal Agreement will remain in full force and effect.

9.3 If there is a conflict between the Principal Agreement and this DPA the terms of this DPA will control.

9.4 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations, set forth in the Principal Agreement.

IN WITNESS WHEREOF, this DPA is entered into with effect as of the later of the dates set out below.

On behalf of Organizer:	**On behalf of ATIV Solutions, LLC:**
	Silke Fleischer
Name (written out in full)	Name (written out in full)
	CEO
Position	Position
	ATIV Solutions, LLC
Organization	Organization
	340 S Lemon Ave #4605, Walnut CA 91789
Address	Address
	
Signature	Signature
	23 August 2022
Date Signed	Date Signed

ATTACHMENT 1: EU Standard Contractual Clauses

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on

STANDARD CONTRACTUAL CLAUSES

for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

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)[1] 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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

(a) 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)

(a) 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.

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 organizational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

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

(a) 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

(a) 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 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

(a) 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

(a) 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 organizational 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 authorized 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

(a) 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

(a) 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[2] (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 benefiting 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 defense 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.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORIZATION The data importer has the data exporter's general authorization 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 10 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfills 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(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 fulfill 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.

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. (9) 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

MODULE TWO: Transfer controller to processor

(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 authorized 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 organizational 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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) 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.

(b) 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.

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

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

(e) 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] 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.

(a) [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(a) [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organizational 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). [For Module Three: The data exporter shall forward the notification to the controller.]

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(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 supervisory 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 of 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) [For Modules One, Two and Three: 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 Ireland.

Clause 18: Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 Ireland.

(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.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: _____

Address: _____

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

_____

_____

Activities relevant to the data transferred under these Clauses: *Use of ATIV Services pursuant to the Principal Agreement*

Signature and date: _____

Role (controller/processor): *Controller*

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: *ATIV Software LLC*

Address: *340 S Lemon Ave #4605, Walnut CA 91789*

Contact person's name, position and contact details: *Silke Fleischer, CEO*

Activities relevant to the data transferred under these Clauses: *Processing necessary to provide Services pursuant to the Principal Agreement*

Signature and date: Silke Fleischer 24 August 2022

Role (controller/processor): *Processor*

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Data subjects include the Data Exporter's authorized users, employees, contractors, agents, representatives, or customers accessing and/or using ATIV Services in connection with the Data Exporter Organizer event(s) ("Consumers").

Categories of personal data transferred

The data transferred to ATIV Solutions, LLC is the personal data collected by the data exporter Organizer in connection with its use of ATIV services to host its event on the EventPilot meeting platform. Such personal data may include:

- Data used for users to sign in (which may include single sign-on user token information, first and/or last names, email address, authorization data, account information, passcodes, conference codes)
- Job title, employer, affiliation, or organization name
- Connection data (the device used to access the platform)
- As requested by Data Exporter, recordings, videos, photos, documents, or other multimedia
- Information provided for monitoring, training and quality purposes.

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

ATIV Solutions LLC does not intentionally collect special categories of data, but the data exporter, at its own discretion, may collect such data. These categories may include racial or ethnic origin, political opinions, philosophical beliefs, trade union membership, health or sex data. Data exporter is solely responsible for meeting all obligations regarding the collection, use, and transfer of such data.

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

Continuously, for the length of the Agreement between the parties.

Nature of the processing

Personal data transferred will be processed to (i) provide ATIV Services to the data exporter and fulfill the data importer's obligations under the ATIV Terms of Service and/or the governing ATIV Services Agreement; (ii) provide customer support to the data exporter; and (iii) compliance with applicable law.

Purpose(s) of the data transfer and further processing

To (i) provide ATIV services to the data exporter and fulfill the data importer's obligations under the ATIV Terms of Service and/or the governing ATIV Services Agreement; (ii) provide customer support to the data exporter; and (iii) compliance with applicable law.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data shall be retained for the length of time necessary to provide the ATIV services under the Agreement, or as otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subprocessors for ATIV Solutions LLC will process personal data to assist ATIV in providing the ATIV services pursuant to the Agreement, for as long as needed for ATIV to provide the ATIV services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Where the EU GDPR applies, the competent supervisory authority is the Data Protection Commission (DPC) of Ireland.

Where the UK GDPR applies, the competent supervisory authority is the UK Information Commissioner's Office.

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data importer will maintain a written and comprehensive information security program, which includes appropriate physical, technical, and administrative controls to protect the security, integrity, confidentiality, and availability of personal data, including without limitation, protecting personal data against any unauthorized or unlawful acquisition, access, use, disclosure or destruction. For more information about the data importer's security practices and technical controls, please see: https://www.ativsoftware.com/legal/security/.

ANNEX III: LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The controller has authorized the use of the following sub-processors: https://ativsoftware.com/legal/subprocessors/