## VirtualFest Data Processing Addendum

This Data Processing Addendum (“Addendum”) forms part of the Terms of Service or any other agreement pertaining to the delivery of the Service (the “Agreement”) between Yeti LLC (“Yeti”) and the Host identified in such Agreement (the “Customer”), to reflect the parties’ agreement with regard to the Processing of Personal Data (as those terms are defined below). All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Service to Customer pursuant to the Agreement, Yeti may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

If the entity signing this Addendum is not a party to an effective Agreement with Yeti, this Addendum shall not be valid or legally binding. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control to the extent of such conflict.

## Definitions

* 1. “Anonymous Data” means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person
	2. “Applicable Data Protection Law” means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Law and the CCPA.
	3. “Authorized Employee” means an employee of Yeti who has a need to know or otherwise access Personal Data to enable Yeti to perform their obligations under this Addendum or the Agreement.
	4. “Authorized Individual” means an Authorized Employee or Authorized Subprocessor.
	5. “Authorized Subprocessor” means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Personal Data to enable Yeti to perform its obligations under this Addendum or the Agreement.
	6. “CCPA”means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.
	7. “Data Controller” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
	8. “Data Processor” means the entity which Processes Personal Data on behalf of the Data Customer.
	9. “Data Subject” means an identified or identifiable person to whom Personal Data relates.
	10. “GDPR” means Regulation (EU) 2016/679, the General Data Protection Regulation, including as implemented or adopted under the laws of the United Kingdom.
	11. “Instruction” means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Customer to Yeti and directing Yeti to Process Personal Data.
	12. “Personal Data” means any information relating to Data Subject which Yeti Processes on behalf of Customer other than Anonymous Data.
	13. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
	14. “Process” or “Processing” means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
	15. “Yeti” or “data importer” means Yeti.
	16. “Service” shall have the meaning set forth in the Agreement.
	17. “Standard Contractual Clauses” means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Commission Decision (2010/87/EU) available on the European Commission’s website at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\_en.
	18. “Supervisory Authority” means an independent public authority with jurisdiction to oversee the processing of personal data covered by this Addendum.

## Processing of Data

* 1. For purposes of this Addendum, Customer and its affiliates are the Data Controller(s) and Yeti is the Data Processor. With respect to the CCPA, Yeti shall Process Personal Data as a “service provider,” as defined therein.
	2. The rights and obligations of the Customer with respect to this Processing are described herein. Customer shall, in its use of the Service, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with Applicable Data Protection Laws. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Customer’s instructions will not cause Yeti to be in breach of Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Yeti by or on behalf of Customer; (ii) the means by which Customer acquired any such Personal Data; and (iii) the instructions it provides to Yeti regarding the Processing of such Personal Data. Customer shall not provide or make available to Yeti any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Service, and shall indemnify Yeti from all claims and losses in connection therewith.
	3. Yeti shall Process Personal Data only (i) for the purposes set forth in the Agreement; (ii) in accordance with the terms and conditions set forth in this Addendum and any other documented instructions provided by Customer; and (iii) in compliance with Applicable Data Protection Law. Customer hereby instructs Yeti to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of the Service.
	4. Following completion of the Service, at Customer’s choice, Yeti shall return or delete the Personal Data, except as required to be retained by law, rule or regulation that is binding upon Yeti or, if the Personal Data is in the possession of an Authorized Subprocessor or Subprocessors, as required to be retained by an Authorized Subprocessor by law, rule or regulation that is binding upon the Subprocessor. If return or destruction is impracticable or prohibited by law, rule or regulation, Yeti shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess Personal Data, require the Authorized Subprocessor to take the same measures that would be required of Yeti. If Customer and Yeti have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Yeti to Customer only upon Customer’s request.

## Authorized Employees

* 1. Yeti shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.
	2. Yeti shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Yeti, any Personal Data except in accordance with their obligations in connection with the Service.
	3. Yeti shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals.

## Authorized Subprocessors

* 1. Customer hereby agrees and provides a general prior authorization that Yeti may (i) engage its Authorized Subprocessors to access and Process Personal Data in connection with the Service and (ii) from time to time engage additional third parties for the purpose of providing the Service, including without limitation the Processing of Personal Data. Yeti shall ensure that every Authorized Subprocessor has entered into an written agreement that is no less protective of Personal Data than this Addendum. Yeti shall be liable to Customer for the acts and omissions of Authorized Subprocessors to the same extent that Yeti would itself be liable under this Addendum had it conducted such acts or omissions.
	2. If Customer and Yeti have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Customer’s prior written consent to the subcontracting by Yeti of the processing of Personal Data if such consent is required under the Standard Contractual Clauses.

## Security of Personal Data

* 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Yeti shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.
	2. Yeti shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
		1. the pseudonymisation and encryption of personal data;
		2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and service;
		3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
		4. a process for regularly testing, assessing and evaluating the effectiveness of security measures.

## Transfers of EU Personal Data

* 1. Any transfer of Personal Data made subject to this Addendum from member states of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by Yeti through the Standard Contractual Clauses, which are incorporated by reference in this Addendum, with the following clarifications:
		1. *Subject Matter, Nature, Purpose, and Duration of Processing*. Yeti will Process the Personal Data to provide the Service. The duration of the Processing shall be for the Term of the Agreement plus the period until Yeti deletes all Personal Data processed on behalf of Customer in accordance with the Agreement.
		2. *Types of Personal Data and Categories of Data Subjects*. The types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to the Standard Contractual Clauses, which is hereby incorporated into this Addendum by reference and shall be binding as if it were set out in this Addendum in its entirety.
		3. Appendices 1 and 2 to this Addendum shall be deemed automatically incorporated into Appendices 1 and 2 of the Standard Contractual Clauses.
		4. For the avoidance of doubt, the parties agree that this Section is not intended to amend or modify the Standard Contractual Clauses, but to provide clarity regarding Yeti’s practices for complying with the Standard Contractual Clauses. In the event of any conflict between this Section and the Standard Contractual Clauses, the Standard Contractual Clauses shall control.

## Rights of Data Subjects

* 1. Yeti shall, to the extent permitted by Applicable Data Protection Law, promptly notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject’s right of: access, rectification, restriction of Processing, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively “Data Subject Request(s)”). If Yeti receives a Data Subject Request in relation to Customer’s data, Yeti will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Service.
	2. Yeti shall, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer’s obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Yeti’s assistance and (ii) Yeti is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Yeti.

## Actions and Access Requests

* 1. Yeti shall, taking into account the nature of the Processing and the information available to Yeti, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Applicable Data Protection Law to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information.
	2. Yeti shall, taking into account the nature of the Processing and the information available to Yeti, provide Customer with reasonable cooperation and assistance with respect to Customer’s cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by Applicable Data Protection Law.
	3. Yeti shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum. Customer shall, with reasonable notice to Yeti, have the annual right to review such records at Yeti’s offices during regular business hours.
	4. In the event of a Personal Data Breach, Yeti shall, without undue delay after confirming that a breach of personal data has occurred, inform Customer of the Personal Data Breach and take such steps as Yeti in its sole discretion deems necessary and reasonable to remediate such violation.
	5. In the event of a Personal Data Breach, Yeti shall, taking into account the nature of the Processing and the information available to Yeti, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.
	6. The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Yeti’s obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by Yeti of any fault or liability with respect to the Personal Data Breach.

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

## Data exporter

The data exporter is a customer of the data importer’s software-as-a-service applications.

## Data importer

The data importer is a provider of software-as-a-service applications.

## Data subjects

Individuals about whom data is provided to Yeti via the Service by (or at the direction of) Customer or Customer’s end users, including without limitation Customer’s employees, consultants, contractors, agents, end users, and guests at virtual events provided via the Service.

## Categories of data

Any Personal Data provided to Yeti via the Service, by (or at the direction of) Customer or Customer’s end users, including but not limited to the following:

**Identifying information**: First Name, Last Name, Email, Password (if SSO is not used)

**Personal information shared through interactive features:** contact information such as First Name, Last Name, Email, Phone Number, Address; work history

## Special categories of data (if appropriate)

None

## Processing operations

 Storage and processing of Personal Data necessary to offer software-as-a-service applications

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

## Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

* 1. the pseudonymisation and encryption of personal data;
	2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing system and services;
	3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
	4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.