DATA PROCESSING ADDENDUM

The parties conclude this Data Processing Addendum ("**DPA**"), which forms part of the Agreement between Customer and Supplier ("Flipnode LLC"), meaning the Digital Signage SaaS Agreement (the "Agreement") to reflect their agreement about the Processing of Personal Data, in accordance with the requirements of Data Protection Laws and Regulations, including the GDPR, the UK GDPR, the FDPA, the CCPA, the Data Privacy Framework (DPF), and the UK Extension to the DPF, as well as the Swiss-US Data Privacy Framework, to the extent applicable. To the extent Supplier, in providing the Services set forth in the Agreement, processes Personal Data on behalf of Customer, the provisions of this DPA apply.

References to the Agreement will be construed as including this DPA. Any capitalized terms not defined hereinshall have the respective meanings given to them in the Agreement.

This DPA consists of two parts: (i) the main body of this DPA, and (ii) Attachments 1, 2, 3, 4, 5, and 6 hereto.

HOW TO EXECUTE THIS DPA

To complete this DPA, Customer should:

a.   Sign the main body of this DPA in the signature box below.

b.   Complete any missing information and sign Attachment 1, Attachment 2, Attachment 3, Attachment 4, 5, and 6, if applicable. Submit the completed and signed DPA to Supplier via email to support@yodeck.com. Upon receipt of a validly completed DPA, this DPA will be legally binding (provided that Customer has not overwritten or modified any of the terms beyond completing the missing information).

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to and formspart of the Agreement.

If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to the Agreement directly with Supplier, but is instead a customer indirectly via an Authorized Reseller or a Partner, this DPA is not valid and is not legally binding. Such entity should contact the Authorized Reseller or the Partner to discuss whether any amendment to its agreement with that Reseller or Partner may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Personal Data contained in the Agreement.

DATA PROCESSING TERMS

Customer and Flipnode hereby agree to the following provisions with respect to any Personal Data Customer processed by Flipnode in relation to the provision of the Services under the Agreement.

1. DEFINITIONS

"Adequacy Decision" means a European Commission Decision and/or a decision of the Secretary of State of the UK and/or the Swiss Federal Council that a third country or an international organization ensures an adequate level of data protection as defined in the GDPR and the UK GDPR as well as the FDPA.

"Affiliate" means, with respect to any entity, any other entity Controlling, Controlled by or under common Control with such entity, for only so long as such Control exists;

"Authorized Affiliate" means any of Customer's Affiliate(s), which (i) is subject to Customer's Binding Corporate Rules or to similar contractual clauses, including Standard Contractual Clauses or contractual clauses approved by a Supervisory Authority, where applicable, with the Customer to ensure adequate level of protection of Personal Data, (ii) is not established in a Restricted Third Country, and (iii) is permitted to use the Services pursuant to the Agreement between Customer and Supplier, but is not a signatory Party to the Agreement and is not a "Customer" as defined under the Agreement;

"Behavioral Data" means data that tracks or otherwise monitors a Data Subject's activities online or the Data Subject's product and service usage;

"Binding Corporate Rules" are binding internal rules that regulate the transfer of Personal Data within an organization which, where applicable, have been approved by EU data protection authorities as providing an adequate level of protection to Personal Data;

"CCPA" means the California Consumer Privacy Act (CAL. CIV. CODE § 1798.100 et. seq.), as amended by the California Privacy Rights Act, and its implementing regulations.

"Control" means the direct or indirect ownership of more than 50% of the voting capital or similar right of ownership of an entity, or the legal power to direct or cause the direction of the general management and policies of that entity, whether through the ownership of voting capital, by contract or otherwise. Control and Controlling shall be construed accordingly;

"Dashboard" for applicable Services, means the user interface features of the hosted Software (as

described in the Agreement);

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data, as defined in the GDPR, the UK GDPR, and the FDPA, and has the same meaning as "business," as that term is defined by the CCPA;

"Data Privacy Framework" or "DPF" means the Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, as in force from time to time;

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, as defined in the GDPR, the UK GDPR and the FDPA, and has the same meaning as "service provider," as that term is defined by the CCPA;

"Data Protection Laws and Regulations" means all laws and regulations applicable to the Processing of Personal Data as part of or in connection with the Services, including but not limited to (i) laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR, ii) Adequacy Decisions, including the Data Privacy Framework ("DPF") and the UK Extension of the DPF, as well as the Swiss-US DPF, (iii) the UK GDPR, (iv) the FDPA, and (v) the CCPA, as either of (i) or (ii) or (iii) or (iv) or (v) may be amended and are in force from time to time;

"Data Subject" means the individual to whom Personal Data relates, as defined in the GDPR, the UK GDPR, and the FDPA and has the same meaning as "consumer" as that term is defined under the CCPA;

"FDPA" means the Swiss Federal Data Protection Act including its implementing ordinances (Bundesgesetz über den Datenschutz), or any succeeding Swiss data protection law;

"Flipnode" means the Supplier and its Greek Affiliate, Flipnode Single Member LTD, established in Athens, Lykourgou 1, 10551, +30 211 800 1709, which is a signatory party to this DPA, but is not a signatory Party to the Agreement and is not a "Supplier" as defined under the Agreement.

"Flipnode's Representative" means a natural or legal person established in the European Union who is designated by and represents Flipnode with regard to its respective obligations under the GDPR, as applicable. Flipnode's Representative is Flipnode Single Member LTD, established in Athens, Lykourgou 1, 10551, +30 211 800 1709;

"Flipnode's UK Representative" means a natural or legal person established in the UK who represents Flipnode with regard to its respective obligations under the UK GDPR, as applicable. Flipnode's UK Representative is Lionheart Squared Limited, with registered offices at 17 Glasshouse Studios, Fryern Court

Road, Fordingbridge, Hampshire, SP6 1QX United Kingdom, email: Yodeck@LionheartSquared.co.uk.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as may be amended from time to time;

"Personal Data" means data about a natural person processed by Flipnode in relation to the provision of the Services under the Agreement, from which that person is identified or identifiable, as defined in the GDPR, the UK GDPR and the FDPA; for the avoidance of doubt, Personal Data includes but is not limited to Support Data, Behavioral Data and Unique Identifier Data, and has the same meaning as "personal information" as that term is defined under the CCPA;

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, blocking, erasure or destruction;

"Restricted Third Country" means a country to which a transfer of Personal Data, or from which access to Personal Data, would be prohibited by applicable Data Protection Laws and Regulations;

"Standard Contractual Clauses" means contractual clauses adopted by the European Commission and/or the UK Secretary of State and/or the UK Information Commissioner and/or the Swiss Federal Data Protection and Information Commissioner, based on the GDPR and/or the UK GDPR and/or the FDPA, as applicable;

"Software" means the object code version of YODECK software and/or any software to which Customer is provided access to as part of the Services, including any updates or new versions;

"Supplier" means the Flipnode entity, which is a party to this DPA and the Agreement, namely Flipnode LLC, 505 Montgomery Street, Suite 1100, San Francisco, CA 94111, United States.

"Sub-processor" means any non-Affiliate or Affiliate Data Processor, engaged by Supplier, who agrees to receive from Supplier Personal Data exclusively intended for the Processing to be carried out on behalf of the Customer, in accordance with its instructions, the terms of this DPA, and the terms of the written Sub-processor contract;

"Supervisory Authority" means an independent public authority which is established by an EU Member State, pursuant to the GDPR, and/or the Information Commissioner of the UK, and/or the Swiss Federal

Data Protection and Information Commissioner, as applicable;

"Support Data" means information that Flipnode collects, when Customer submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files;

"Swiss-US Data Privacy Framework" or "Swiss-US DPF" means the decision of the Swiss Federal Council of 14 August 2024 on the adequate level of protection of personal data under the Swiss-US Data Privacy Framework, as in force from time to time;

"Technical and organizational security measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

"UK Extension to the DPF" means the extension to the DPF which the United States Department of Commerce administers in relation to transfers of Personal Data from the United Kingdom, as in force from time to time;

"UK GDPR" means the GDPR as retained in UK Law after UK's withdrawal from the EU, and as amended and in force from time to time.

"Unique Identifier Data" means a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that for the purposes of this DPA Customer is the Data Controller and Supplier is the Data Processor, that Supplier engages in the Processing, i.e. in the operation, maintenance and support of the Services, including acting as super-administrator of the accounts in YODECK

Software, its Greek Affiliate and that Flipnode is entitled to engage Sub-processors pursuant to the requirements set forth in Clause 5 of this DPA. Customer may permit the use of the Services to Authorized Affiliate(s) pursuant to the conditions set out in Clause 14 and 15 of this DPA.

2.2 Customer's Processing of Personal Data. a. Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Laws and Regulations. Customer's instructions to the Flipnode for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer, after its assessment of the requirements of Data Protection Laws

and Regulations, considers that this DPA is compliant with Data Protection Laws and Regulations, especially local laws applicable on Customer In addition, Customer shall have sole responsibility for the accuracy, reliability, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services or whose Personal Data are Processed in Customer's Use of the Services. It is expressly stated that Customer is solely responsible (i) for the legality of the purposes of the Processing, (ii) for the necessity of the Processing to serve these purposes, (iii) to inform any and all Data Subjects, whose Personal Data is processed by using the Services, about the scope, the purpose, the duration and the means of the Processing, their rights with respect to the Processing (iv) to acquire the consent of the Data Subjects, whose Personal Data is being processed by using the Services, where applicable v) to conduct a Data Protection Impact Assessment Study (DPIA) within the meaning of the GDPR, the UK GDPR and the FDPA, where applicable. b. To the extent permitted by applicable Data Protection Laws and Regulations, Customer shall have the right, upon reasonable notice, to take steps reasonably necessary to stop and remediate any unauthorized use of Personal Data by Flipnode.

2.3   Flipnode's Processing of Personal Data. a. Flipnode shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA, including with respect to the "business purpose," as such term is defined by CCPA, for this Agreement; (ii) Processing initiated by Authorized Affiliates or Authorized Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. b. Customer takes full responsibility to keep the amount of Personal Data provided to Flipnode to the minimum necessary for the performance of the Services. c. Flipnode shall not be required to comply with or observe Customer's instructions, if such instructions would violate the Data Protection Laws and Regulations. Flipnode shall immediately inform Customer if, in its opinion, an instruction infringes the Data Protection Laws and Regulations. d. Flipnode shall process Personal Data, if required to do so by European Union or Member State law to which Flipnode is subject; in such a case, Flipnode shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Flipnode shall promptly notify Customer of any legally binding request for disclosure of Personal Data by a law enforcement authority, or other legal process, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. **e**. Flipnode shall not sell or share, as those terms are defined by the CCPA, any Personal Data provided by Customer to Flipnode, and shall not combine the Personal Data of any California residents that it receives from, or on behalf of, Customer with Personal

Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with those California residents, except as permitted by the CCPA.

2.4 Scope of the Processing. The subject-matter of Processing of Personal Data by Flipnode is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Complaints or Notices related to Personal Data. In the event Flipnode receives any official complaint, notice, or communication that relates to Processing of Personal Data for or on behalf of the Customer or either party's compliance with Data Protection Laws and Regulations, to the extent legally permitted, Flipnode shall promptly notify Customer and, to the extent applicable, Flipnode shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Flipnode's provision of such assistance.

3.2 Data Subject Requests. To the extent legally permitted, Flipnode shall promptly notify Customer, if Flipnode receives a request from a Data Subject to exercise the Data Subject's right to consent, and to withdraw the consent, right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"), and for the avoidance of doubt, similar requests to exercise any of the Data Subject rights as provided by the CCPA. Factoring into account the nature of the Processing, Flipnode shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Flipnode shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Flipnode is legally permitted to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Flipnode's provision of such assistance.

4. FLIPNODE'S PERSONNEL

4.1. Confidentiality. Flipnode shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate

training on their responsibilities and have executed written confidentiality agreements. Flipnode shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2.   Reliability. Flipnode shall take commercially-reasonable steps to ensure the reliability of its personnel engaged in the Processing of Personal Data.

4.3.   Limitation of Access. Flipnode shall ensure that Flipnode's access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement, and that access is limited to those personnel that is necessary for the provision of the Services.

4.4.   Data Protection Officer. Flipnode shall appoint, a Data Protection Officer, if and whereby such appointment is required by the GDPR, the UK GDPR, and the FDPA, as applicable. Any such appointed person and Flipnode's personnel responsible for privacy issues, may be reached at privacy@yodeck.com

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer authorizes and agrees that:

(i) Flipnode is entitled to retain its current and future Affiliate(s) as Sub-processors. Currently the Greek Affiliate, Flipnode Single Member Ltd is engaged in the Processing of Personal Data under this DPA. Flipnode shall inform the Customer of any intended changes to its Affiliates, acting as Sub-processors.

(ii) Flipnode is entitled to engage any third parties from time to time to process Personal Data in connection with the provision of Services.

5.2. List of Sub-processors. Flipnode maintains an up-to-date list of Sub-processors, which is available on its website at the Yodeck sub-processors page (https://www.yodeck.com/subprocessors/), which it will update with details of any change of sub-processors at least 30 days prior to the change. Customer shall be notified of any change to the list of Sub-processors, by registering an email in the "Get Notifications for Subprocessors list change" text field in the Yodeck sub-processors page.

5.3. Objection Right for New Sub-processors. Customer, in order to exercise its right to object to Supplier's use of a new Sub-processor, whether Affiliate or not, shall notify the Supplier promptly in writing within thirty (30) days after the change. Personal Data shall by no means be processed by the Sub-processor against which the Customer has explicitly objected. If Supplier and Customer cannot find a mutually agreeable resolution to address the Customer's objection within a reasonable time period, which shall not exceed thirty (30) days, the Customer may terminate the Services. The

Supplier shall refund Customer any prepaid fees covering the remainder of the Service following the effective date of termination with respect to such terminated Service. Customer shall return at Customer's own delivery expenses any hardware (i.e. YODECK player) acquired by Flipnode.

Contractual relationships. Flipnode shall only engage and disclose Personal Data to non-Affiliate Sub- processors that are parties to written agreements with Flipnode containing data protection obligations no less protective that the obligations of this DPA and comply with any requirements for such processing in the Data Protection Laws and Regulations. Flipnode agrees and warrants, upon request of the Customer, to send promptly a copy of any Sub-processor contract to the Customer, and to make available to the Data Subject upon request a copy of the DPA, or any existing Sub-processing contract, unless the DPA or contract contain commercial information, in which case it may remove such commercial information, with the exception of Attachment 2, which shall be replaced by a summary description of the security measures, in those cases where the Data Subject is unable to obtain a copy from the Customer.

5.4. **Liability.** Flipnode shall be liable for the acts and omissions of its non-Affiliate Sub-processors to the same extent Flipnode would be liable, if performing the services of each Sub-processor directly under the terms of this DPA.

6. ~~DELETED CLAUSE~~

7. SECURITY

Taking into account the state of 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, Flipnode shall implement appropriate organizational and technical measures to ensure a level of security, appropriate to the risk (including protection from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to Personal Data Processed under this DPA), as set forth in Attachment 2 to this DPA. Flipnode shall regularly monitor compliance with these measures. Flipnode shall not materially decrease the overall security of the Services during Customer's subscription term. Attachment 2 may be amended from time to time, upon parties' written agreement, to meet higher standards of safety and privacy. In such case Attachment 2 shall be replaced.

Customer represents that after its assessment of the requirements of the Data Protection Laws and Regulations, Customer considers that the security measures set out in Attachment 2 are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of

Personal Data to be protected having regard to the state of the art and the cost of their implementation.

8. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Flipnode has in place reasonable and appropriate security incident management policies and procedures, specified in Attachment 2 of this DPA, and shall notify Customer without undue delay after becoming aware of an unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Flipnode or its non-Affiliate Sub-processors of which Flipnode becomes aware ("Personal Data Incident"), as required under the Data Protection Laws and Regulations. Flipnode shall make reasonable efforts to identify the cause of such Personal Data Breach, and take those steps as it deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach, to the extent that the remediation is within Flipnode's reasonable control.

9. CERTIFICATIONS AND AUDITS

9.1 Audits. Upon Customer's request, and subject to the confidentiality set forth in the Agreement, Flipnode shall make available to the Customer that is not a competitor of Flipnode all information necessary to demonstrate compliance with the obligations of Flipnode under this DPA, and allow for and contribute to audits, including on-site audits, conducted by the Customer or by Customer's independent, third-party auditor, in possession of the required professional qualifications bound by a duty of confidentiality, that is not a competitor of Flipnode. The parties agree that the audits shall be carried out in accordance with the following specifications: Customer may contact Flipnode to request an on-site audit of the architecture, systems, and procedures relevant to the protection of Personal Data. Customer shall reimburse Flipnode for any time expended by Flipnode or its third party Sub-processors for any such on-site audit at the Flipnode's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Flipnode shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Flipnode or its third party Sub-processors. Customer shall promptly notify Flipnode and provide information about any actual or suspected non-compliance discovered during an audit.

9.2 Certifications. Flipnode shall also allow and provide third-party certifications and audit results upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement. Flipnode shall make available to Customer that is not a competitor of Flipnode (Customer's independent third-party auditor that is not a competitor of Flipnode) a copy of

Flipnode's then most recent third-party certifications or audit results, as applicable.

10. RECORDS AND COOPERATION WITH THE SUPERVISORY AUTHORITY

10.1. Records. Where required by the Data Protection Laws and Regulations, or as reasonably requested by Customer, Flipnode shall maintain a record, in electronic form, of all categories of processing activities carried out on behalf of the Customer.

10.2. Cooperation with the Supervisory Authority. Where applicable, Flipnode shall, upon request, cooperate with the Supervisory Authority in the performance of its tasks, as per the GDPR, the UK GDPR and the FDPA, as applicable.

11. RETURN AND DELETION OF PERSONAL DATA

Flipnode shall, at the choice of the Customer, return Personal Data, to Customer or delete existing copies after the end of the provision of the Services and certify to the Customer that it has done so in accordance with the procedures specified in Attachment 2 to this DPA, unless mandatory laws require storage of Personal Data. In that case Flipnode warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

12. DATA PROTECTION IMPACT ASSESSMENT

Upon Customer's request, Flipnode shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR, the UK GDPR and the FDPA, as applicable, to carry out a Data Protection Impact Assessment("DPIA") related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Flipnode. Flipnode shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under the GDPR, the UK GDPR, and the FDPA.

13. DATA TRANSFERS

Transfers of Personal Data under this DPA from the European Union, the European Economic Area, including Switzerland, and/or their member states, and the United Kingdom to countries outside of the European Economic Area, including Switzerland, and the United Kingdom are made only in accordance with the following:

i.   the transfer is to a jurisdiction for which an appropriate (EU or UK or Swiss) Adequacy Decision has been issued and subject to the terms of that Adequacy Decision;

ii.   in the absence of an Adequacy Decision, the transfer is subject to appropriate form of the

Standard Contractual Clauses.

iii.   in case the DPF or the UK Extension to the DPF or the Swiss-US DPF cease to be in force, Attachments 4 and 5 and 6 of this DPA shall automatically apply accordingly.

14. AUTHORIZED AFFILIATES

14.1 Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Flipnode and each such Authorized Affiliate subject to the provisions of the Agreement and this Clause and Clause 15 of this DPA. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

14.2. Communication. The Customer that is contracting party to the Agreement shall remain responsible for coordinating all communication with Flipnode under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. Customer informs Flipnode of the Authorized Affiliate(s) to which Customer intends to permit the use of the Services, thereby giving Flipnode the opportunity to object, in case the requirements set out in the Definition of an Authorized Affiliate under this DPA are not met.

14.3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Flipnode, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

i.   Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Flipnode directly by itself, the parties agree that (a) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (b) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 13.3.ii below).

ii.   The parties agree that the Customer that is the contracting party to the Agreement shall, when

carrying out an on-site audit on the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Flipnode and its non-Affiliate Sub-processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

15. LIABILITY

For the avoidance of doubt, Flipnode's total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

16. LEGAL EFFECT; TERMINATION; VARIATION

This DPA shall only become legally binding between Customer and Flipnode when fully executed following the formalities steps set out in the Section "How to Execute this DPA" and will terminate when the Main Agreement terminates, without further action required by either party.

The parties undertake not to vary or modify the DPA. This does not preclude the parties from adding clauses on business related issues, where required as long as they do not contradict the DPA.

17. CONFLICT

This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control.

IN WITNESS WHEREOF, the parties have caused this Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories, whose signatures appear below, are on the date of signature duly authorized.

CUSTOMER	**FLIPNODE LLC**
Name:	Name: EVANGELOS MICHALOPOULOS
Title:	Title: CEO
Date:	Date: February 21, 2025
Authorised Signature	Authorised Signature: *Evangelos Michalopoulos*

ATTACHMENT 1

Details of the Processing

This attachment includes certain details of the Processing of Personal Data.

Nature and Purpose of Processing

Flipnode will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Clause 11 of the DPA, Flipnode shall Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Unless otherwise agreed upon in writing, Flipnode shall, at the choice of the Customer, return Personal Data, to Customer or delete existing copies after the end of the provision of the Services and certify to the Customer that it has done so in accordance with the procedures specified in Attachment 2 to this DPA, unless mandatory laws require the storage of Personal Data. In that case Flipnode warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

Categories of Data Subjects

- Customers
- Customer's Agents, Employees, Authorized Users

Type of Personal Data

- Identification data:
  - name, address, email, phone number and access rights.
- Customer Content:
  - Images
  - Videos
  - Power point
  - Pdf files etc

CUSTOMER	**FLIPNODE LLC**
Name:	Name: EVANGELOS MICHALOPOULOS
Title:	Title: CEO
Date:	Date: February 21, 2025
Authorised Signature	Authorised Signature:

ATTACHMENT 2

Description of the technical and organizational security measures implemented by Flipnode, which form part of the DPA:

‾ Personnel

Confidentiality and reliability. Personnel engaged in the processing of Personal Data are reliable, are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, are regularly trained, and have executed written confidentiality agreements. Confidentiality obligations survive the termination of the personnel engagement. Access privileges are terminated upon termination of employment. All personnel with access right to Accounts are engaged full-time.

Segregation of Duty and Limitation of Access. Personnel's access to Personal Data is appropriate and necessary to their role. A Security Officer has been appointed in written and supervises compliance with security measures. Personnel have individual accounts for accessing systems with safe codes. Personnel is separated into three levels of access i) developers, ii) support/sales, and iii) others. Developers have access to the whole system, to ensure that everything is running smoothly. Support has limited access to the system, i.e. only when handling a support request. All others do not have access to Accounts.

Access Control and Authentication. a. A procedure for user account creation and deletion, with appropriate approvals is in place; b. Industry standard practices to identify and authenticate users who attempt to access information systems are utilized; c. De-activated or expired identifiers are not granted to other individuals; d. All Personnel actions are logged to an internal audit log. Providing support also appears to the Users of an Account, if the Account is on the Enterprise plan that provides for the "Audit logs" features.

‾ Physical and Environmental Security

Physical Access. Flipnode utilizes facilities with access control (e.g. CCTV, reception, access code), and with emergency and contingency plans for various disasters, including fire. Drills are in practice regularly.

Exposure of Documents. A Clean Desk Policy is implemented. All physical files are kept in cabinets or drawers.Photo copy and fax machines are not in common view.

Destruction of Documents. Papers with personal data are dispensed exclusively in paper shredders. After retention period, electronic data are not just deleted, but destroyed (including their back-ups) by

overwriting with the use of special software, like file erasers, file shredders, file pulveritizers or, alternatively, for destruction on a daily basis, by formatting.

Portable Devices. Laptops are encrypted and accessed only by secure codes.

Data Security

Anti-virus. Flipnode ensures that antivirus, anti-malware and anti-spyware software of the latest update are installed. Updates are installed at regular intervals. Flipnode undertakes specific hardening activities, to minimize the architectural weaknesses of operating systems, application, and network devices.

Remote Access. Security of remote access to the system is based on encryption and safe protocols. For providing advanced remote support, YODECK Player establishes an encrypted connection to Flipnode's online server. Only direct communication between the device and the server is allowed, no traffic forwarding or between devices traffic is allowed.

Firewall. An industry-standard firewall is installed to inspect all connections routed to the system's environment.

Vulnerability and Penetration Tests. Flipnode regularly performs vulnerability analysis aimed at specifying the status of exposure to known vulnerabilities, in relation to both the infrastructural and application environments, considering the systems in operation or in the development phase. These checks take place in real time supplemented by an annual external third-party penetration test

Change Control. All changes to platform, application, and production infrastructure (for example software update, development of new software, antivirus installation or deinstallation) are tested, before implementing, in an isolated and updated environment not affecting real data or data of the production system, with the exception of users that have enrolled to the Beta Set Up. There are regular controls on installed software to verify that no software has been installed outside of the regular process. All changes are administered centrally only by specific users.

Data separation. Content uploaded in YODECK Software shall be maintained logically separated from Flipnode's corporate infrastructure and from Flipnode's other Customers' content.

Log Retention Policy

General. Log files are retained for all crucial systems. Flipnode retains the following types of logs: Web Access Logs / Application Logs / Audit Logs (detailed). Following information are necessarily retained at a minimum:

a) identification of user who required access to personal data, date and time of the request, system for which access was requested, whether access has been granted or not.

b) Same information with regard to non-authorized access efforts

c) Printing requests of files with personal data

d) Modifications in crucial files of the system or in the users' rights

e) Changes in the parameters of apps and systems

f) Crucial events and of any action that may be considered as an attack or a security incident (e.g. port scanning). The retention of events is directly supervised by the Security Officer and the System Administrators.

Log files may only be assessed by the Security Officer and the system administrators. Deletion of log files has to be authorized by both the Security Officer and a member of the senior management.

Log Storage. All Logs are uploaded from each server to Amazon S3. Credentials and names used ensure that an attacker cannot access or alter the logs. Flipnode uses versioning on Amazon S3 to make sure previous content of updated logs are kept. Log files are stored on an Amazon S3 bucket properly configured for encryption-at-rest using the SSE-S3 encryption scheme. The S3 object lock feature is activated precventing any deletion of log data intentionally or by accident during the configured bucket lifecycle policy (90 days).

Log Rotation. All Logs are rotated on the server on 5-days basis, to facilitate support and debugging. Logs stored on Amazon S3 are rotated on a 90-days basis.

Password Policy

Access to all systems, applications and software is password protected. Customer is responsible to use passwords, which comply with password configurations (eg minimum length, expiration, complexity etc.) and to change passwords regularly. Customer is responsible to safeguard security of its passwords and of the users' passwords and comply with the commitments of this paragraph (Password Policy).

Passwords are not written, either physically or electronically, in their actual form. They are retained electronically in a non-readable form, whereas the retrieval of their initial form is not possible. After three attempts of unsuccessful access authorization, access is prohibited to the user.

Passwords are not kept in logs.

Industry standard procedures are implemented to deactivate passwords that have been corrupted or inadvertently disclosed.

Service Continuity and Disaster Recovery

a. Flipnode utilizes facilities (data centers), for Personal Data and their back-ups, providing

adequate emergency and contingency plans and guarantees; b. Flipnode has in place adequate data recovery procedures.

Incident Monitoring and Management

Flipnode monitors, analyses and responds to security incidents in a timely manner, and escalates as necessary. Flipnode implements a specific Incident Management Procedure to guarantee the recovery of normal service operations as soon as possible in case of interruption.

Data Breach Policy

Flipnode has a Data Breach Policy in place to meet the requirements of Clause 8 of this DPA, which includes but is not limited to i) internal reporting of potential Personal Data Breaches, ii) recovery of a Personal Data Breach, iii) risk assessment, iv) notification of Personal Data Breach to the Data Controller, the Supervisory Authority and the affected data subject, as applicable, v) evaluation and response measures to prevent similar breaches. Security Officer is responsible for the implementation and update of the Data Breach Policy.

Design of the Services

Privacy.

Every User, after signing up for the first time, has to accept Flipnode's Privacy Policy. YODECK application enables the Customer to assign specific rights (of view, access, modification, and deletion) based on the tasks and responsibilities of the Authorized Affiliate or the Authorized User. Deletion of Personal Data as well as deletion of the Account is possible by the process described in the Dashboard under section "Personal Data". Following security measures are accommodated: a) authentication of users before access; ii) encryption of passwords iii) activation of secure password policy by Customer in the Enterprise Plan; and iv) prevention of access after suspicious access attempts..

Customer's responsibility. Customer manages each user's access to and use of the Services by assigning to each user a credential and user type that controls the level of access to and use of the Services. Customer is responsible for protecting the confidentiality of its own and each user's login and password and managing each user's access to the Services.

Security.

Exclusively Outbound Traffic. YODECK Application uses only outbound traffic. No inbound listening port (TCP or UDP) is required. YODECK Application does not use port forwarding, DMZ, or UPnP in the network.

Digital Signature Verification for Schedule Files and Configuration Files. Schedule and Configuration files are digitally signed using RSA encryption keys. It is not possible for an attacker to force the Player to play a different schedule file than one generated by the system for this specific device.

HTTPS Certificate checks. Schedule Files, Configuration Files and Media Files are downloaded using HTTPS. SSL certificate check are enforced throughout the system.

Software Upgrading Verification Checks. On each software upgrade, software packages downloaded are verified using GPG RSA-based encryption keys. Upgrading will fail, if verification fails.

Device Firewall. YODECK Players have a standard firewall policy enabled by default, that only allows inboundSSH access. SSH can also be firewall for the LAN interface, leaving nothing accessible from the LAN, withoutany service disruption.

Proxy Authentication Support. YODECK Players support using a Proxy installed and managed. The Proxy is required to support the "CONNECT" method for HTTPS connections. Yodeck supports using authentication credentials for Proxies.

Customization Scripts. Device support customization scripts for altering default behavior are issued remotely as part of the Configuration file, which is digitally signed and secured.

Secure Software Initialization. The whole SD card that holds the Player software can be re-written through USB on boot. You place a zip file on a USB flash drive, attach it on the Player, and boot it. Upon boot, the Player will self-rewrite the whole SD card. Prior to starting this process, the software verifies the integrity and authenticity of the zip file. All images are signed.

Network segmentation. The network on which YODECK Players can be segmented and is totally separate from the rest of the local network. No direct local network access is required for any reason.

Customer's responsibility. Customer is solely responsible for the safe connection of the YODECK Player to internet.

- Audit and Review

Internal and external audit of all systems takes place on yearly basis. Technical and Organizational Security Measures are reviewed annually, and in case of a major change. Audit and Review include capacity planning of IT resources with view to future requirements based on workload and data storage requirements.

- Data subjects rights:

For data subjects rights see online Privacy Policy of Yodeck.

For affiliate sub-processors same as above.
For non-affiliate sub-processors, see online terms of the sub-processors.

CUSTOMER	**FLIPNODE LLC**
Name:	Name: EVANGELOS MICHALOPOULOS
Title:	Title: CEO
Date:	Date: February 21, 2025
Authorised Signature	Authorised Signature: *Evangelos Michalopoulos*

ATTACHMENT 3

The list of Sub-processors is as set forth at the Yodeck sub-processors page (https://www.yodeck.com/subprocessors/).

CUSTOMER	**FLIPNODE LLC**
Name:	Name: EVANGELOS MICHALOPOULOS
Title:	Title: CEO
Date:	Date: February 21, 2025
Authorised Signature	Authorised Signature: *Evangelos Michalopoulos*

ATTACHMENT 4

STANDARD CONTRACTUAL CLAUSES

(based on COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standardcontractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council)

1. Name of the data exporting organisation:

Address:

Tel.:   **e-mail:**

2. ….

(the data exporter(s))

And

Name of the data importing organisation: Flipnode

LLC Address: 505 Montgomery Street, Suite 1100, San

Francisco,   CA   94111,   United   States   Tel.:

+14159926050 ; e- mail: info@yodeck.com

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex I.

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.

---

[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

(b) The Parties:

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – 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);

---

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.

(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

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

<div align="center">

SECTION II – OBLIGATIONS OF THE PARTIES

</div>

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer')

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's

if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9   Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 (thirty) 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

---

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.

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 fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these

---

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

Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13 Supervision
(a) [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.

[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.

[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 behaviour 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

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific

circumstances of the transfer, and the applicable limitations and safeguards[4];

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

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

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

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

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

Clause 15

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

15.1 Notification

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

---

[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.

(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.).

(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.

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

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

Clause   17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of_Greece_ .

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of ___the data exporter____.

(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.

On behalf of the data exporter(s)

Name (written out in full):

Title:

Date:

Authorised Signature:

2. …

On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21, 2025

Authorised Signature:

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

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. CUSTOMER

Name:

Address: ……….

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): CONTROLLER
2. …

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

1. SUPPLIER

Name: Flipnode LLC

Address: 505 Montgomery Street, Suite 1100, San Francisco, CA 94111, United States

Contact person's name, position and contact details: George Dramitinos, Chief Information Officer, dramit@flipnode.net

Activities relevant to the data transferred under these Clauses: Provision of the Services under the SaaS Agreement between Customer and Supplier.

Signature and date: *Evangelos Michalopoulos*   February 21, 2025
Role (controller/processor): PROCESSOR

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customers
- Customer's Agents, Employees, Authorized Users

Categories of personal data transferred
- Identification data:
- name, address, email, phone number and access rights.
- Customer Content:
- Images
- Videos
- Power point
- Pdf files etc

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.

N/A – For the avoidance of doubt, it is clarified that Customer is not allowed to upload sensitive data to the Services.

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

Continuous. See also matrix below.

Nature of the processing

Collection, storage, modification, transmission of personal data, only in automated (not manual) form.

Purpose(s) of the data transfer and further processing

Provision of the Services under the SaaS Agreement between Customer and Supplier, and as further instructed by the Customer in its use of the Services.

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

For the duration of the SaaS agreement

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

See the Yodeck sub-processors page (https://www.yodeck.com/subprocessors/).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

[…]

On behalf of the data exporter(s)

1. Name (written out in full):

Title:

Date:

Authorised Signature:

2.
On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21, 2025

Authorized Signature: Evangelos Michalopoulos

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONALMEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Same as attachment 2 of the DPA

On behalf of the data exporter(s)

1. Name (written out in full):

Title:

Date:

Authorised Signature:

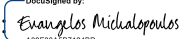2.
On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21, 2025

Authorized Signature: *Evangelos Michalopoulos*

ANNEX III

LIST OF SUB-PROCESSORS

The list of Sub-processors is as set forth at the at the Yodeck sub-processors page (https://www.yodeck.com/subprocessors/).

On behalf of the data exporter(s)

1. Name (written out in full):

Title:

Date:

Authorised Signature:

2.

On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21. 2025

Authorized Signature: *Evangelos Michalopoulos*

ANNEX IV
SUPPLEMENTARY MEASURES
TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

1. In the event the data importer receives a legally binding request for Personal Data from agovernment authority, or a Court authority, including an authority in the US, the data importer shall:

   a) promptly notify Customer, unless prohibited under applicable law; and

   b) to the extent the data importer is prohibited by applicable law from providing such notice:

      a. review each request on a case-by-case basis; and

      b. use best efforts to request that the confidentiality requirement be waived to enable the data importer to notify Customer; and

      c. maintain evidence of any such attempt to have a confidentiality requirement waived.

2. Transfers of Personal Data by the data importer to a government or Court authority, should, to the extent possible, avoid being massive, disproportionate or indiscriminate in a manner that would go beyond what is required by applicable law.

3. The data importer shall regularly review its internal policies to assess the suitability of the implemented supplementary measures and identify and implement additional or alternative solutions, if necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

On behalf of the data exporter(s)

1. Name (written out in full):

Title:

Date:

Authorised Signature:

2.

On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21, 2025

Authorized Signature:
DocuSigned by:
Evangelos Michalopoulos
A09F33A5B7124BD...

Attachment 5

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start Date	This Addendum is effective as of the date of the DPA stated above.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' Details	Full legal name: Trading name (if different):registered address): Official registration number (if any) (company number or similar identifier):	Company name: Flipnode LLC Address: 505 Montgomery Street, Suite 1100, San Francisco, CA 94111, United States Official registration number: 5194759
Key Contact	Contact details including email:	Contact details including email:Evangelos Michalopoulos Tel.: +1 415 992 6050 e-mail: mihalop@yodeck..com
Signature		DocuSigned by: *Evangelos Michalopoulos* A09F33A5B7124BD...

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	x		x	X	
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As identified in Annex 1A of Attachment 4 of the DPA (EU SCCs).
Annex 1B: Description of Transfer: Set forth in Annex 1B Attachment 4 of the DPA (EU SCCs).
Annex II: Technical and organizational measures including technical and organizational measures to ensure the securityof the data: Set forth in Annex II Attachment 4 of the DPA (EU SCCs).
Annex III: List of Sub processors (Modules 2 and 3 only): Set forth in Annex III Attachment 4 of the DPA (EUSCCs)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which parties may end this Addendum as set out in Section IV: [X] Importer [ ] Exporter

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UKGDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

1. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

2. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

4. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

5. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

6. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

7. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

8. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

9. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

   a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

   b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

   c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

10. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

11. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

12. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

   a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

   b. In Clause 2, delete the words: "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";

   c. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

   d. Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

   e. Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

   f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

13. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
its direct costs of performing its obligations under the Addendum;

and/or its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

14. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Attachment 6

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

In its communication of August 27, 2021, the Swiss Federal Data Protection and Information Commissioner ("FDPIC") recognized the new SCCs issued by the European Commission in accordance with Regulation (EU) 2016/679 as a legal basis for personal data transfers to a country without an adequate level of data protection, provided that the necessary adaptations and amendments are made for use under Swiss data protection law. Therefore, this Attachment 6 to the Data Processing Addendum incorporates by reference the Standard Contractual Clauses in Attachment 4 and its Annexes I through IV, except that (i) all references to "GDPR" will be replaced by "FDPA", (ii) "Third Country" will be replaced by "Swiss Third Country", (iv) any reference to a supervisory authority shall refer to the Swiss Federal Data Protection and Information Commissioner; (v) all references to the EEA shall include Switzerland; (vi) where the Clauses refer to Member States, they shall be read to refer to Switzerland; (vii) with regards to Clauses 17 and 18 of the Clauses, these clauses shall be governed by the law of Switzerland and the Parties agree to the jurisdictions of the courts of Switzerland with regard to any disputes that arise from these Clauses.

On behalf of the data exporter(s)

1. Name (written out in full):

Title:

Date:

Authorised Signature:

2.

On behalf of the data importer:

Name (written out in full): EVANGELOS MICHALOPOULOS

Title: CEO

Date: February 21, 2025

Authorized Signature: