ON24 DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") is entered into by and between ON24 Inc., on behalf of itself and its Affiliates ("ON24"), and Client, on behalf of itself and its Affiliates ("Client", Client and ON24 each a "Party" and together the "Parties") and is effective as of the date on which Client signs this Addendum (the "Effective Date").

1. Background

1.1 ON24 operates a content delivery platform that enables its business customers to create, manage, host and deliver webcasts and other content, as well as virtual events and environments, to send emails and communications to registrants, attendees and other end users, and to collect registration and other information from registrants, attendees and other end users (the "Platform"). In operating and providing the Platform, ON24 will provide services to its business customers relating to their use of the Platform (the "Services"). This Addendum applies to the Processing (defined below) of Client Personal Data (defined below), pursuant to the Services, including Personal Data received from the European Economic Area ("EEA"), the United Kingdom and Switzerland.

1.2 This Addendum forms a part of the ON24 Universal Terms and Conditions, and any Master Services Agreement, Subscription Agreement, Services Agreement, Work Order, and other written or electronic agreement between ON24 and Client related to Client's purchase of Services and ON24's provision of the same, and any amendments thereto (collectively, the "Agreement," which also includes any amendments hereto).

1.3 This Addendum supersedes any prior data processing agreements, data processing addenda or similar terms between the Parties. In the event of any conflict or inconsistencies between the terms of this Addendum and any other terms in the Agreement, this Addendum will control.

2. Execution

2.1 To make this Addendum a part of the Agreement, Client must enter the Client-related information in the signature box below, have an authorized representative of Client sign this Addendum, and email it to ON24.

2.2 This Addendum will be considered a legally binding addendum to the Agreement once it has been signed by both ON24 and an authorized representative of Client, and such fully executed version is emailed to ON24. This Addendum is not valid or enforceable where signed by a Client or other entity that is not a party to an unexpired, valid and enforceable Agreement directly with ON24.

3. Certain Definitions

3.1. In this Addendum, the following terms will have the meanings set out below:

(a) "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

(b) "CCPA" means, where applicable, the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended or superseded from time to time;

(c) "CPRA" means, where applicable, the California Privacy Rights Act of 2020, as amended or superseded from time to time;

(d) "Client Affiliate" means any Affiliate of Client that is authorized and/or permitted to use the Platform or Services pursuant to the Agreement;

(e) "Client Event" means the webcasts, webinars, virtual environments, and other content offered or made available through the Platform by Client or Client Affiliate;

(f) "Client Materials" means any materials or data Client enters into, collects, manages or creates using the Platform, including, but not limited to, slides, audio files, video files, photographs, and recordings generated from a Client Event;

(g) "Client Personal Data" means any Personal Data Processed by ON24 or a Subprocessor in the provision of the Services to Client or a Client Affiliate, including (but not limited to) any contact information or other personally identifiable information of End Users of Client Events or contained in Client Materials;

(h) "Data Breach" means accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored or otherwise Processed by ON24 or its Subprocessors;

(i) "Data Center" means the physical location containing ON24's computer servers which house ON24's Platform and store Client Personal Data;

(j) "Data Protection Laws" means any local, national or international laws, rules and regulations related to privacy, security, data protection, and/or the Processing of Personal Data, as amended, replaced or superseded from time to time, including: (i) the GDPR and laws of EEA Member States implementing or supplementing the GDPR; and (ii) any data protection laws of the United Kingdom including the UK Data Protection Act 2018 and the UK General Data Protection Regulation; "Data Privacy Frameworks" means together the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework;

(k) "Data Privacy Frameworks" means together the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework;

(l) "End User" means an actual and prospective attendee, visitor and other user who has registered for or attended one or more Client Events;

(m) "GDPR" means EU General Data Protection Regulation 2016/679;

(n) "International Data Transfer Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner on 21 March 2022, attached hereto as Appendix A to Annex 3;

(o) "Personal Data" is any information defined as "personal data", "personal information", or other similar terms under applicable Data Protection Laws;

(p) "Process" means any operation or set of operations that is performed upon Client Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and "processed," or "processing" will be construed accordingly;

(q) "Restricted Transfer" means a transfer of Client Personal Data to, between or by ON24, its Affiliates and/or a Subprocessor, to the extent such transfer would be prohibited by applicable Data Protection Laws in the absence of the Standard Contractual Clauses, the International Data Transfer Addendum or the Data Privacy Framework;

(r) "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection of data subjects, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers (other than from the UK), attached hereto as Annex 3;

(s) "Subprocessor" means any person or entity (including any third party and any ON24 Affiliate, but excluding an employee of ON24) appointed by or on behalf of ON24 who may Process Client Personal Data;

(t) "Supervisory Authority" means (a) an independent public authority established by a Member State pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws, including the UK Information Commissioner Office ("ICO"); and

(u) The terms "Controller," "Processor," "Data Subject," and "Member State," will have the same meaning as in the GDPR.

(v) The term "Consumer" will have the same meaning as in the CCPA.

3.2. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

4. Processing of Personal Data

4.1. The Parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Controller, and ON24 is the Processor.

4.2. ON24 will and will ensure that Subprocessors will Process Client Personal Data only on Client's documented instructions, or where Processing is required by applicable laws to which ON24 or Subprocessors are subject; in the latter case, ON24 will notify the Client of the legal requirement before Processing, unless the law prohibits such notification.

4.3. Client on its own behalf and as agent for each relevant Client Affiliate instructs ON24 (and authorizes ON24 to instruct each Subprocessor) to, as reasonably necessary for the provision of the Services (including any additional services used by Client or Client Affiliate, which may subject to supplemental terms): (a) Process Client Personal Data; (b) transfer Client Personal Data to any country or territory provided such complies with Section 12 (Cross-border Transfers) below; and (c) engage any Subprocessors, provided such complies with Section 11 (Subprocessing) below. If requested by Client and set forth in an Agreement, ON24 will store Client Personal Data in a Data Center located in the European Union.

4.4. As may be required by CCPA, CRPA and Data Protection Laws, ON24 will process Client Personal Data to the extent necessary to provide the Services described in the Agreement and only for the purposes as instructed by Client in a manner consistent with this Addendum. ON24 will not retain, use, or disclose such Client Personal Data for any purpose other than to perform the Services, which for the avoidance of doubt prohibits ON24 from retaining, using, or disclosing Client Personal Data outside of the direct business relationship with Client or for any other commercial purpose. ON24 will not sell, share (as defined under CPRA), rent, release, disclose, disseminate, make available, transfer or otherwise communicate such Client Personal Data to any third party for monetary or other consideration. ON24 certifies that that it understands the restrictions set out in this Section 4 and will comply with them. Client agrees that ON24 may de-identify or aggregate Client Personal Data and other data related to the Services to render it Anonymous Data, which may then be used for the purposes of operating and improving ON24's services and operations, and other research, analytics and related purposes. ON24 may maintain Anonymous Data as part of its own records and information, and such data shall no longer be subject to the Agreement or this Addendum. "Anonymous Data" means data that has been de-identified and/or aggregated with other data to such an extent that Client and Client Affiliates are no longer identifiable, and individuals are no longer identified, identifiable, linked or linkable, or otherwise ascertainable by reference to or combination with other datasets.

4.5. Client agrees that (a) Client's submission of Client Personal Data and instructions for the Processing of Personal Data will comply with Data Protection Laws and Client will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section (Processing of Personal Data) on behalf of each relevant Client Affiliate; (b) Client and any Client Affiliate will, in the use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws; and (c) Client will provide any required notices to and obtain any required consents from Data Subjects related to the Processing of Client

Personal Data as contemplated in this Addendum and the Agreement, or as otherwise instructed by Client.

4.6. Annex 1 to this Addendum sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, and the categories of Personal Data and Data Subjects, as required by Article 28(3) of the GDPR; Annex 1 does not confer and rights or obligations on either Party. Either of the Parties may make reasonable amendments to Annex 1 as they reasonably consider necessary to meet the requirements of the Data Protection Laws by providing the other Party with an updated or an additional Annex 1.

5. ON24 Personnel

ON24 will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Client Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

6. Security

ON24 will implement appropriate technical and organizational measures, as set forth in Annex 2 (Technical and Organizational Measures), that are designed to provide a level of security appropriate to the risks presented by the Processing of Client Personal Data. In assessing the appropriate level of security, ON24 will take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7. Personal Data Breach

ON24 will notify Client without undue delay, from when it discovers a Data Breach involving Client Personal Data and will provide information (as available) to assist Client to meet any obligations to report a Data Breach under the Data Protection Laws. ON24 will co-operate with Client and take such reasonable steps as are agreed in good faith by the parties to assist in the investigation, mitigation and remediation of each Data Breach. To the extent that Client is responsible for a Personal Data Breach Client will reimburse ON24 for all costs reasonably and properly incurred by ON24 performing its obligations under this Section (including internal costs and third party costs including legal fees).

8. Data Subject and Consumer Rights

ON24 will promptly notify Client if it receives a request from a Data Subject or Consumer entitled to exercise a request under applicable law regarding Client Personal Data as it pertains to that Data Subject or Consumer. Upon request, ON24 will provide Client with reasonable assistance as necessary to Client's fulfilment of its obligations under applicable laws to respond to such requests relating to their Personal Data. Taking into account the nature of the Processing, such assistance will include, where practicable, implementation of reasonable and appropriate technical and organizational measures to allow Client to respond effectively to such requests.

9. Data Protection Impact Assessment and Prior Consultation

Upon request and subject to the nature of the relevant Processing by and information available to ON24, ON24 will provide reasonable assistance to Client with any data protection impact assessments and any prior consultations to any Supervisory Authority, which are required under applicable Data Protection Laws.

10. Audit Rights

10.1 Upon Client's written request, ON24 will make available to Client information reasonably necessary to demonstrate ON24's compliance with this Addendum and will allow for and contribute to inspections by a qualified, independent third-party auditor appointed by Client, in relation to the Processing of Client Personal Data by ON24 or its Subprocessors.

10.2 Client will give ON24 reasonable notice of any audit or inspection to be conducted under this Section and will (and ensure that each of its mandated auditors will) take all reasonable steps to avoid causing any damage, injury or disruption to the premises, equipment, personnel and business of ON24 or any Subprocessor during the course of such an audit. Except as otherwise required by applicable law or a relevant Supervisory Authority, any audit or inspection will be conducted within normal business hours no more than once in any calendar year. Client will reimburse ON24 in full for all costs reasonably and properly incurred by ON24 performing its obligations under this Section (including internal costs, third party costs including legal fees, and costs incurred by ON24 with respect to audits of other Subprocessors). Any information obtained under this Section will be kept confidential and not disclosed to any person without the express consent of ON24, and Client will ensure that any auditor, agent, personnel or other person or entity that participates in such audit is subject to appropriate written confidentiality obligations.

11. Subprocessing

11.1 Client authorizes ON24 to appoint (and permit each Subprocessor appointed in accordance with this Section to appoint) Subprocessors subject to satisfying the requirements listed in Section 11.3 below. Client expressly agrees that ON24 Affiliates may be engaged as Subprocessors, and that ON24 may continue to use those other Subprocessors already engaged by ON24 as of the date of this Addendum. ON24 will make available a current list of ON24 Subprocessors at www.on24.com/about-us/gdpr/subprocessors, including the names and a description of the Processing to be undertaken by the Subprocessor, and will update the list prior to adding any additional Subprocessors. Client may subscribe to email notifications of new Subprocessors at www.on24.com/about-us/gdpr/subprocessors. ON24 will provide notice of new Subprocessors prior to authorizing new Subprocessors to Process Personal Data in connection with the Services by updating the Subprocessor list at www.on24.com/about-us/gdpr/subprocessors via email notification if Client has subscribed to email notifications about new Subprocessors. Client may object to the appointment of a new Subprocessor by sending written notice to ON24 at privacy@on24.com within ten (10) business days of the notice of new Subprocessors; Client's notice of objection should state the basis for Client's objection. Client agrees that it will not unreasonably object to the use of a Subprocessor. If Client does not object to the appointment of the Subprocessor within ten (10) business days, the Client shall be deemed to have approved and agreed to such appointment.

11.2 The Parties will work in good faith to resolve Client's objections to the appointment of any Subprocessors. During this time, there may be an impact to the provision of the Services; Client agrees that ON24 is not liable for any such impact. If the parties are unable to resolve Client's objection within 90 days, Client may terminate without penalty the portion of the Agreement pertaining to the Services that ON24 states it cannot provide without the use of the objected-to Subprocessor, and ON24 will refund Client any prepaid but unused amounts for such portion; otherwise, the Agreement shall remain in full force and effect.

11.3 With respect to each Subprocessor, ON24 will: (a) exercise commercially reasonable care in the assessment, appointment and oversight of the relevant Processing activities of Subprocessors; (b) include terms in the contract between ON24 and each Subprocessor which offer an equivalent level of protection for Client Personal Data as those set out in this Addendum, taking into account the nature of the services performed by the Subprocessor; (c) if the arrangement involves a Restricted Transfer of Client Personal Data, ON24 will ensure that the Standard Contractual Clauses and the International Data Transfer Addendum are at all relevant times incorporated into the agreement between ON24 and the Subprocessor; and (d) remain liable to the Client for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of Client Personal Data.

12. Cross-border Transfers

Client (for itself and its relevant Affiliates), as data exporter, and ON24 and its relevant Affiliates, each as a data importer, as evidenced by execution of this DPA, hereby execute the Standard Contractual Clauses attached hereto as Annex 3, including the International Data Transfer Agreement, which shall apply to the Client Personal Data and take effect in the event of a Restricted Transfer of Client Personal Data. With respect to the Client Personal Data subject to Data Protection Laws other than those of the EEA, the United Kingdom or Switzerland, in the Standard Contractual Clauses, the terms "Member State" and "State" are replaced throughout by the word "jurisdiction," "supervisory authority" will mean the relevant data protection regulator or other government body with authority to enforce Data Protection Laws, and references to "applicable data protection laws" and "Regulation (EU) 2016/679" shall be replaced with the "applicable Data Protection Laws" as defined herein. In addition, ON24 participates in the Data Privacy Frameworks and obeys the commitments they entail. ON24 agrees to notify as required by applicable law or the Data Privacy Frameworks Client if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the principles of the Data Privacy Frameworks or if the Data Privacy Frameworks are declared invalid or superseded.

13. Deletion or Return of Personal Data

Upon the termination or expiration of the Agreement (unless continued Processing is subject to a new or amended agreement) and to the extent not prohibited by applicable law, ON24 will within 90 days (the "Cessation Date") cease Processing and delete or return the Client Personal Data. If Client does not inform ON24 of its choice of either return or deletion of such Client Personal Data at least 30 days prior to the Cessation Date, then Client will be deemed to have chosen deletion. The parties agree that ON24 is not required to return or delete any Anonymous Data at the conclusion of the Agreement.

14. Limitation of Liability

The aggregate liability of ON24 and the Client arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability in the Agreement.

15. General Terms

15.1 No Legal Advice. Notwithstanding anything to the contrary in this Addendum, ON24 will not be required to provide legal advice to Client and nothing provided by ON24 will be construed by Client as legal advice.

15.2 Termination. The parties agree that this Addendum and the Standard Contractual Clauses and the International Data Transfer Addendum will terminate automatically upon: (a) termination of the Agreement; or (b) expiry or termination of all service contracts entered into by ON24 with Client pursuant to the Agreement; or (iii) termination or completion of statements of work, work orders or similar documents, thereunder, whichever is later.

15.3 Third Party Rights. A person who is not a Party to this Addendum will have no right to enforce any term of this Addendum; the rights to rescind or vary this Addendum are not subject to the consent of any other person.

15.4 Business Interest Cloud. Client hereby elects, and expressly requests and consents, to participate in the ON24 Business Interest Cloud feature, as part of the Services, and agrees to the Business Interest Cloud Terms and Conditions set forth at http://www.on24.com/bic-terms.

15.5 Changes in Data Protection Laws. If any variation is required to this Addendum as a result of a change in Data Protection Law, either Party may provide written notice to the other party of that change in law. The Parties will discuss and negotiate in good faith any necessary variations to this Addendum to address such changes. Notwithstanding the foregoing, to the extent the Standard Contractual Clauses or the International Data Transfer Addendum are superseded by new or amended standard contractual clauses ("Amended SCCs") or a new International Data Transfer Agreement ("Amended International Data Transfer Addendum"), Client agrees that ON24 may amend the terms of this Addendum as necessary in order to incorporate the Amended SCCs or Amended International Data Transfer Addendum, by providing written notice to Client at least 30 days prior to the effective date of such amendment or such shorter notice period as may be necessitated by applicable Data Protection Laws. The Parties agree that any such amendment to the Agreement shall take effect and be binding upon the Parties as of the effective date set forth therein, unless Client notifies ON24 in writing of its objection to such amendment within 15 days of ON24's amendment notice.

15.6 Severance. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum will remain valid and in force. The invalid or unenforceable provision will be either (a) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement as of the Effective Date.

Client:	**ON24, Inc.**
Signature	Signature DocuSigned by: Amit Khetan 4F60C0C51F02487...
Name	Name Amit Khetan, CAO
Title	Title VP Finance, Chief Account Officer
Date Signed	Date Signed 02/21/2024

ANNEX 1: DETAILS OF PROCESSING OF CLIENT PERSONAL DATA

This Annex 1 includes certain details of the Processing of Client Personal Data as required by Article 28(3) of GDPR.

Subject matter and duration of the Processing of Client Personal Data:

The subject matter and duration of the Processing of Client Personal Data are set out in the Agreement and this Addendum.

The categories of Data Subjects to whom Client Personal Data relates:

- Actual and prospective attendees, visitors and other users (i.e., End Users) of Client Events and users of other Client Materials via the Platform, which may include:
  - Prospects, customers, business partners and vendors of data exporter (who are natural persons)
  - Employees or contact persons of data exporters' prospects, customers, business partners and vendors
  - Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Client personnel, agents, affiliates, subsidiaries and others who have been authorized to access, manage and use the Platform on Client's behalf ("Authorized Users"), and other Client personnel

The nature and purpose of the Processing of Client Personal Data:

- Collection, storage and management of registration and other information from End Users of Client Events and Client Materials
- Facilitate Client's creation, management, hosting, delivery, sharing and distribution of Client Events and Client Materials
- Facilitate reminders, notices, and other email and other communications (including by email) to End Users, and to permit Client to personalize Client Materials, Client Events and communications to End Users
- Manage Platform access by Authorized Users and prevent unauthorized access
- Track attendance by End Users and prevent unauthorized access
- Generate and provide reporting and analytics to Client related to Client Events and other Services
- Support, maintenance and managed services related to Client's Use of the Platform and Services

The types of Client Personal Data to be Processed:

- Name, email and other contact details
- Company, position/title, company contact details, and other business information
- Other information Client chooses to or requests ON24 to collect as part of Client Event registration or attendance
- Video, images, audio and other content
- Name, title, company email, and other information requested of Authorized Users
- Client Event analytics and usage statistics

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organizational 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.

- **Security of data center locations**

  ON24 utilizes top tier data center collocation, IAAS, and hosting facilities located in North America and Europe*. These facilities incorporate physical security protections 24 hours a day, seven days a week, including on-site guards, CCTV and active fire monitoring/suppression. Industry-standard security access controls, including badge/picture IDs, mantraps, and biometric access screening. ON24 servers and all related equipment are housed in locked cages within the collocation facilities. *Data center collocation facility location is determined pursuant to relevant Agreement.

- **Back Ups**

  Incremental backups are performed daily. Full backups are performed weekly. Additionally, data and critical backups are replicated between primary and secondary data centers using an encrypted highly redundant storage layer with erasure coding. Both utilize AES-256 bit encryption.

- **System Access**

  Access to systems is provisioned following the least privilege principle. System access is via individual named accounts with strong password requirements and all system access is logged. Privileged access is controlled centrally using LDAP and role-based access groups with integrated 2FA. Access control groups are reviewed regularly as part of internal audit function.

- **Business Continuity**

  ON24 facilities are connected to multiple diverse Tier 1 internet backbones with high availability architecture and redundancy designed into each service layer. For business continuity and disaster recovery purposes data is actively replicated from ON24 primary facility to secondary sites in near real-time. ON24 operations team maintains internal runbooks, server orchestration & automation tools, and other documentation to facilitate rapid response to system and network events.

- **Security Certification**

  ON24 is SOC2 Type II audited on an annual basis. ON24 reviews the security certifications of subservices providers and Subprocessors to ensure adequate technical and organizational measures are in place.

- **Penetration Testing**

  ON24 undergoes annual penetration testing performed by a qualified third party. Summary reports of the most recent assessment are available upon request.

- **User identification and authorization**

  Platform access is permitted via unique credentials for each user. Clients may also enable SSO via SAML/2. SSO federated access can control Admin (backend), Presenter, and also Attendee access. User permissions are configured via roles managed by the Client administrator. Clients have access to additional controls to increase access security, including but not limited to passwords, CAPTCHAs, domain restrictions.

- **Protection of data during transmission and during storage**

  ON24 supports TLS 1.2 for protection of data during transmission while interacting with the platform. Certificates are at least 2048-bit and renewed biannually. All data backups are encrypted using AES-256.

- **Event logging**

  All network, system, and platform access is logged. Logs are retained for an appropriate amount of time to support correlation, investigation and auditing of events.

- **System configuration, including default configuration**

  Hardened images and configurations are maintained based on vendor guidance and CIS benchmarks; this includes changing default configurations to block common attack vectors. Various orchestration and automation tools are utilized to ensure consistent configurations are in place.

- **Internal IT and IT security governance and management**

  In addition to an internal security team, ON24 maintains a cross-functional security group and information security oversight committee in order to ensure appropriate governance and risk management processes are in place.

- **Data minimization**

  Contact details may be captured from Attendees during registration as needed to attend and use the Services. Captured data typically consists of what is considered “business card info”, including name, phone, title, company name and email address. ON24 stores Client data during the relevant subscription term only. Upon expiration of the relevant subscription term, or upon request, Client may export, remove or delete Client data via an administration interface in their Platform account. Client, as the Data Controller, determines the type, frequency, and storage length of all data collected and may minimize as appropriate.

- **Limited data retention**

  Client data is retained during the relevant subscription term. Client may delete Client Data via the administrative interface which renders them unavailable until the database updates (24 hours) and deletes the Webinar permanently. Client may also submit a ticket to request Webinars to be removed, and such Webinars shall be expunged from the database and permanently deleted.

- **Data destruction**

  Upon disposal of physical assets, storage media, e.g. hard drives, are removed and physically destroyed on site by data destruction specialists.

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferringthe 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 theydo not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3
Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

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

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b);

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

Clause 4 Interpretation

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

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

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

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existingat 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 Clausesand have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part ofthe 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 applicableto 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 requiredunder 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 thatit 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 dueaccount 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 forattributing the personal data to a specific data subject shall, where possible, remain under the exclusive controlof 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 anappropriate 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 shallcontain 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') 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 auditsof the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9
Use of sub-processors

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer 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.

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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module.

(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 theright 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 oron its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informedabout 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) If 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.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of applicationof 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.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of applicationof 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 authorityin any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respondto 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 oneof 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];

[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

(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 processingof personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 **Notification**

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

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

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

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, witha 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 onthe 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.

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.

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 laws of the Netherlands.

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 Netherlands.

(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.

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 officerand/or representative in the European Union]*

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Receiving Services pursuant to the relevant Agreement.

Signature and date:

Role (controller/processor): Controller.

Data importer(s):

1. Name: ON24, Inc.
Address: 50 Beale Street, Eighth Floor, San Francisco, CA 94105
Tel.:415-369-8000; e-mail: privacy@on24.com

Activities relevant to the data transferred under these Clauses: Delivery of Services pursuant to the relevant Agreement.

Signature and date: DocuSigned by: Amit Khetan 02/21/2024
4F60C0C51F02487...

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Those set forth in Annex 1 to Annex 3 to the ON24 Data Processing Addendum.

Categories of personal data transferred

Those set forth in Annex 1 to Annex 3 to the ON24 Data Processing Addendum.

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.

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

During the relevant term of the Agreement.

Nature of the processing

Delivery of Services purchased.

Purpose(s) of the data transfer and further processing

The purposes of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement, as set forth in Annex 1 to Annex 3 to the ON24 Data Processing Addendum.

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

During the relevant term of the Agreement.

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

Subprocessors shall process Personal Data on instructions from ON24 as needed to deliver the Services during the relevant Agreement term.

C. COMPETENT SUPERVISORY AUTHORITY

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

As defined in Clause 13.

———

ANNEX II

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

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.

Those security measures set forth in Annex 2 to the ON24 Data Processing Addendum.

APPENDIX A

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Table 1: Parties

Start date	*See Effective Date of the ON24 Data Processing Addendum*	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	*See at Annex I.A of Annex 3 to the ON24 Data Processing Addendum*	*See at Annex I.A of Annex 3 to the ON24 Data Processing Addendum*
Key Contact	*See at Annex I.A of Annex 3 of the ON24 Data Processing Addendum*	*See at Annex I.A of Annex 3 to the ON24 Data Processing Addendum*

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

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: *See Annex I.A of Annex 3 to the ON24 Data Processing Addendum*
Annex 1B: Description of Transfer: *See Annex I.B of Annex 3 to the ON24 Data Processing Addendum*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *See Annex II of Annex 3 to the ON24 Data Processing Addendum*
Annex III: List of Sub processors: *See Section 11.1 of the ON24 Data Processing Addendum*

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 19: ☐ Importer ☐ Exporter ☒ neither Party

By entering into this Addendum

1. 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.

2. 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.

3. 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 2 February 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 UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. 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.

5. 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.

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

7. 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.

8. 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.

Hiearchy

9. 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.

10. 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.

Incorporation of and changes to the EU SCCs

11. 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.

12. 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.

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

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

15. 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

16. 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.

17. 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.

18. 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.

19. If the ICO issues a revised Approved Addendum under Section, 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:

a. its direct costs of performing its obligations under the Addendum; and/or

b. 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.

20. 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.