WebinarNinja EU Data Processing Addendum

Updated October 18, 2021

Effective October 18, 2021

This Data Processing Addendum, including the Standard Contractual Clauses (as defined below), is made and entered into as of the effective date (the "Effective Date") of the applicable customer's ("Customer") acceptance of the Terms of Service between WebinarNinja- a Team ON PTY LTD product ("WebinarNinja") and Customer to which this DPA is attached (the "Agreement"). All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. Under the Agreement, WebinarNinja provides certain Services to Customer that may involve WebinarNinja processing Customer's data, which may include Personal Information (as defined below).

This DPA forms part of the Agreement and contains certain terms and conditions relating to data protection, privacy and security to include certain requirements of the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and the California Consumer Privacy Act of 2018 (Cal. Civ. Code, Title 1.81.5 comprising §§ 1798.100 – 1798.198 (as amended) (the "CCPA"), where applicable. In the event (and to the extent only) that there is a conflict between the GDPR and the CCPA, the parties agree to comply with the higher standard.

1. Definitions

All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement. Terms used but not defined in this DPA, such as “controller,” “data subject,” “personal data,” “processing,” and “processor” will have the same meaning as set forth in the EU Data Protection Law.

"Affiliate" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity.

"Agreement" means WebinarNinja.com’s Terms of Service, which govern the provision of the Services to Subscriber, as such terms may be updated by WebinarNinja.com from time to time.

"Data Protection Laws" means all data protection and privacy laws applicable to the processing of personal data under the Agreement, including, where applicable, EU Data Protection Law.

"EU Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR");

and (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"EEA" means the European Economic Area, United Kingdom and Switzerland.

"Privacy Shield" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Subscriber Data.

"Services" means any product or service provided by WebinarNinja.com to Subscriber pursuant to the Agreement.

“Subprocessors” means the other processors that are used by WebinarNinja.com to process Personal Data.

"Subscriber Data" means any personal data that WebinarNinja.com processes on behalf of Subscriber as a processor in the course of providing Services, as more particularly described in this DPA.

2. Relationship with the Agreement

2.1 The parties agree that the DPA shall replace any existing data processing addendum the parties may have previously entered into in connection with the Services.

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

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

2.4 Subscriber further agrees that any regulatory penalties incurred by WebinarNinja.com in relation to the Subscriber Data that arise as a result of, or in connection with, Subscriber's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce WebinarNinja.com's liability under the Agreement as if it were liability to the Subscriber under the Agreement.

2.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that WebinarNinja.com processes Subscriber Data that originates from the EEA or that is otherwise subject to EU Data Protection Law on behalf of Subscriber as a processor in the course of providing Services pursuant to the Agreement.

3.2 Part A and Exhibit A of this DPA shall apply to the processing of Subscriber Data within the scope of this DPA from the Effective Date.

3.3 Part B shall apply to the processing of Subscriber Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Protection Obligations 4. Roles and Scope of Processing

4.1 Role of the Parties. As between WebinarNinja.com and Subscriber, Subscriber is controller of Subscriber Data, and WebinarNinja.com shall process Subscriber Data only as a processor acting on behalf of Subscribers.

4.2 Subscriber Processing of Subscriber Data. Subscriber agrees that (i) it shall comply with its obligations as a controller under Data Protection Laws in respect of its processing of Subscriber Data and any processing instructions it issues to WebinarNinja.com; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for WebinarNinja.com to process Subscriber Data and provide the Services pursuant to the Agreement and this DPA.

4.3 WebinarNinja.com Processing of Subscriber Data. WebinarNinja.com shall process Subscriber Data only for the purposes described in this DPA. The parties agree the processing of Subscriber Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Subscriber and WebinarNinja.com.

4.4 Details of Data Processing (a) Subject matter: The subject matter of the data processing under this DPA is the Subscriber Data.

(b) Duration: As between WebinarNinja.com and Subscriber, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Subscriber and the performance of WebinarNinja.com's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: WebinarNinja.com provides email messaging, analytics technology and other related services, as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Subscriber's account ("Users"); and any individual: (i) whose email address is included in the Subscriber's Distribution List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "End Users").

(f) Types of Subscriber Data:

(i) Subscriber and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

(ii) End Users: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

4.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Subscriber acknowledges that WebinarNinja.com shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, WebinarNinja.com is the controller of such data and accordingly shall process such data in accordance with the WebinarNinja.com Privacy Policy and Data Protection Laws.

4.6 Tracking Technologies. Subscriber acknowledges that in connection with the performance of the Services, WebinarNinja.com employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Subscriber shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable WebinarNinja.com to deploy Tracking Technologies lawfully on, and collect data

from, the devices of End Users (defined below) in accordance with and as described in the WebinarNinja.com Cookie Policy.

5. Subprocessing

5.1 Authorized Sub-processors. Subscriber agrees that WebinarNinja.com may engage Subprocessors to process Subscriber Data on Subscriber's behalf. The Sub-processors currently engaged by WebinarNinja.com and authorized by Subscriber are listed in Annex III.

5.2 Sub-processor Obligations. WebinarNinja.com shall: (i) enter into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Subscriber Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause WebinarNinja.com to breach any of its obligations under this DPA.

6. Security

6.1 Security Measures. WebinarNinja.com shall implement and maintain appropriate technical and organizational security measures to protect Subscriber Data from Security Incidents and to preserve the security and confidentiality of the Subscriber Data, in accordance with WebinarNinja.com's security standards described in this DPA.

6.2 Updates to Security Measures. Subscriber is responsible for reviewing the information made available by WebinarNinja.com relating to data security and making an independent determination as to whether the Services meet Subscriber’s requirements and legal obligations under Data Protection Laws. Subscriber acknowledges that the Security Measures are subject to technical progress and development and that WebinarNinja.com may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Subscriber.

6.3 Subscriber Responsibilities. Notwithstanding the above, Subscriber agrees that except as provided by this DPA, Subscriber is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Subscriber Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Subscriber Data uploaded to the Services.

7. Compliance Verification

7.1 Upon reasonable request, WebinarNinja.com will verify its compliance with this DPA, provided that Subscriber shall not exercise this right more than once per year.

8. International Transfers

8.1 Data center locations. WebinarNinja.com may transfer and process Subscriber Data anywhere in the world where WebinarNinja.com, its Affiliates or its Subprocessors maintain data processing operations. WebinarNinja.com shall at all times provide an adequate level of

protection for the Subscriber Data collected, transferred, processed, or retained in accordance with the requirements of Data Protection Laws.

8.2 Privacy Shield. WebinarNinja.com is currently in the process of preparing to self-certify its compliance under Privacy Shield. WebinarNinja intends to self-certify under Privacy Shield at the soonest practicable opportunity. Although it has not yet self-certified under Privacy Shield, WebinarNinja agrees to conduct its activates in accordance with the requirements of the Privacy Shield Principles. To the extent that WebinarNinja.com processes any Subscriber Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, to the United States, a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for personal data, the parties acknowledge that WebinarNinja.com shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Subscriber Data as though it has self-certified its compliance with Privacy Shield. WebinarNinja.com agrees to protect such personal data in accordance with the requirements of the Privacy Shield Principles. If WebinarNinja.com is unable to comply with this requirement, WebinarNinja.com shall inform Subscriber.

8.3 Alternative Transfer Mechanism. The parties agree that the data export solution identified in Section 8.2 shall not apply if and to the extent that WebinarNinja.com adopts an alternative data export solution with Subscriber for the lawful transfer of personal data (as recognized under EU Data Protection Laws) outside of the EEA ("Alternative Transfer Mechanism"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which personal data is transferred).

Part B: GDPR Obligations from 25 May 2018

9. Additional Security

9.1 Confidentiality of processing. WebinarNinja.com shall ensure that any person who is authorized by WebinarNinja.com to process Subscriber Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 Security Incident Response. Upon becoming aware of a Security Incident, WebinarNinja.com shall notify Subscriber without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Subscriber.

10. Changes to Subprocessors.

10.1 WebinarNinja.com shall (i) provide an up-to-date list of the Subprocessors it has appointed upon written request from Subscriber; and (ii) notify Subscriber (for which email shall suffice) if it adds Sub-processors at least 10 days prior to any such changes.

10.2 Subscriber may object in writing to WebinarNinja.com's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Subscriber may suspend or terminate the Agreement (without prejudice to any fees incurred by Subscriber prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, WebinarNinja.com shall (at Subscriber's election) delete or return to Subscriber all Subscriber Data (including copies) in its possession or control, save that this requirement shall not apply to the extent WebinarNinja.com is required by applicable law to retain some or all of the Subscriber Data, which Subscriber Data WebinarNinja.com shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Subscriber with a number of controls that Subscriber may use to retrieve, correct, delete or restrict Subscriber Data, which Subscriber may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Subscriber is unable to independently access the relevant Subscriber Data within the Services, WebinarNinja.com shall (at Subscriber's expense) provide reasonable cooperation to assist Subscriber to respond to any requests from individuals or applicable data protection authorities relating to the processing of personal data under the Agreement. In the event that any such request is made directly to WebinarNinja.com, WebinarNinja.com shall not respond to such communication directly without Subscriber's prior authorization, unless legally compelled to do so. If WebinarNinja.com is required to respond to such a request, WebinarNinja.com shall promptly notify Subscriber and provide it with a copy of the request unless legally prohibited from doing so.

12.2 If a law enforcement agency sends WebinarNinja.com a demand for Subscriber Data (for example, through a subpoena or court order), WebinarNinja.com shall attempt to redirect the law enforcement agency to request that data directly from Subscriber. As part of this effort, WebinarNinja.com may provide Subscriber's basic contact information to the law enforcement agency. If compelled to disclose Subscriber Data to a law enforcement agency, then WebinarNinja.com shall give Subscriber reasonable notice of the demand to allow Subscriber to seek a protective order or other appropriate remedy unless WebinarNinja.com is legally prohibited from doing so.

12.3 To the extent WebinarNinja.com is required under EU Data Protection Law, WebinarNinja.com shall (at Subscriber's expense) provide reasonably requested information regarding the Services to enable the Subscriber to carry out data protection impact

assessments or prior consultations with data protection authorities as required by law.

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

SECTION I

Clause 1 - Purpose and scope

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

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, 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 (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.

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 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);

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

iv. Clause 12 - 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 Two and Three: Clause 18(a) and (b).

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

Clause 4 - Interpretation

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

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

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

Clause 5 - Hierarchy

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

Clause 6 - Description of the transfer(s)

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

Clause 7 - 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.

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.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

iii. the onward transfer is necessary for the establishment, exercise or 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

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

b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter

‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

Clause 9 - Use of sub-processors

MODULE TWO: Transfer controller to processor

a. GENERAL WRITTEN 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 fourteen (14) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

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

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

Clause 10 - Data subject rights

MODULE TWO: Transfer controller to processor

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

MODULE THREE: Transfer processor to processor

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

b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11 - Redress

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 12 - Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13 -Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

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

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 [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

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

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

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

[For Module Three: The data exporter shall forward the notification to the controller.]

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

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

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

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

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable

obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

b. The Parties agree that those shall be the courts of Ireland.

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

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

APPENDIX

ANNEX I

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

A. LIST OF PARTIES

Data exporter:

Name: Customer, as defined in the Data Processing Addendum to the Agreement.

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: As described under Section B.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Role: Controller/Processor

Data importer:

Name: Team ON PTY LTD

Address: 333 George Street, Level 13, Sydney, Australia 2000

Contact person's name, position and contact details: Omar Zenhom, Co-founder & CEO, privacy@webinarninja.com.com

Activities relevant to the data transferred under these Clauses: As described under Section B.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects are the recipients of emails the data exporter sends using our Services – typically their customers. Where the data exporter is a processor, data subjects are their customers and end users.

Note: We also transfer the personal data of the (representatives of the) data exporter, those who enter into this agreement with us (our customers) and anyone they allow to access their account (users, for example employees, contractors, collaborators). For this processing and transfer of personal data, we are the Controller and our Privacy Policy applies.

Categories of personal data transferred

The categories of personal data transferred relates to the sending and receiving of email messages (and which constitutes personal data). At a minimum, this includes metadata, email address and message content. Message content may also include name and other information decided and added by the sender, like attachments. The data exporter also has the option to enable open/link tracking and other analytics/tracking of recipient actions, which could include IP address, location, operating system, browser, device, email client and spam complaints.

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.

Not applicable.

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

The frequency of transferring the personal data is continuous, until the agreement comes to an end.

Nature of the processing

Application emails sent through WebinarNinja are categorized as transactional or broadcast electronic messages. Transactional emails are primarily functional, high-priority messages sent to a single recipient, like password resets or receipts/invoices. Broadcast emails are sent to multiple recipients at once, like announcements of product updates or revised terms of service. The nature of the processing relates to facilitate sending and receiving such email messages, including hosting/storage of contact lists and message content, and analytics services.

Purpose(s) of the data transfer and further processing

The purpose of transferring the personal data is to allow the data exporter to reliably deliver application emails to their users/customers.

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

We process personal data on behalf of the data exporter for as long as they remain customers of ours. When the data exporter terminates their use of the Services, we delete their user/customer data within 30 days of the account termination.

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

We rely on some sub-processors when delivering our application email services. The subject matter pertains mainly to infrastructure hosting. The nature of the processing relates to facilitating sending and receiving email messages, including hosting/storage of contact lists and message content, and analytics services. We also use sub-processors for content distribution, logging and similar operations that are strictly necessary for delivering our services. The duration of processing is for as long as the data exporter remains a customer, after which their data is deleted within 30 days.

Current sub-processors are specified in Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Commission of Ireland.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES 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.

Summary

We host our servers in highly secure, SOC 2 certified data centers and use the latest security practices to protect our customers' data. Out of the box, the WebinarNinja service supports opportunistic TLS for all outbound email, ensuring messages are encrypted in transit to remote mail servers and ISPs who support TLS. Combining this with full HTTPS and TLS support on our SMTP and API endpoints provides safe passage for messages flowing through WebinarNinja. Our systems are regularly tested using both automated systems and manual audits from respected security firms.

Amazon Web Services (AWS) details

All personal data is stored in highly secure AWS data centers. AWS regularly achieves third-party validation for thousands of global compliance requirements that they continually monitor to help their customers meet security and compliance standards. AWS supports security standards and compliance certifications like PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS

140-2 and NIST 800-171. For a detailed overview of all security and privacy measures, see the AWS Cloud Security page (https://aws.amazon.com/security)

AWS also has a dedicated Compliance Program which include certifications and accreditations like CSA, ISO, SOC and more, as listed on their website here: https://aws.amazon.com/compliance/programs.

App security

All access to the WebinarNinja interface is secured over SSL (HTTPS), ensuring the information is encrypted. Our SSL configurations are regularly and automatically scanned to ensure we can quickly remediate any vulnerabilities discovered, such as Heartbleed. Additionally, we provide both TLS and HTTPS connections to the WebinarNinja SMTP and API services, ensuring emails sent to the service are encrypted. Account passwords are encrypted in the WebinarNinja database, preventing even our own staff from viewing them. We offer a method to recycle API keys at anytime in the WebinarNinja interface.

Security the controller can implement

Further, our customers (the controllers) can enable 2FA on their account and we allow for detailed user permissions so they can easily and efficiently control who has access to each of their servers. We also fully support and encourage use of email standards like DKIM, SPF, and DMARC, giving them control over their domain's reputation and reducing the risk of email spoofing.

ANNEX III – LIST OF SUB-PROCESSORS

List of WebinarNinja.com Sub-processors:

These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.

Amazon Web Services, Inc.

ConvertKit, LLC

Intercom, Inc. and Intercom R&D Unlimited Company

Sendgrid, Inc.

200 OK, LLC

On behalf of the data importer:

Name (written out in full): Omar Zenhom Position: CEO

Signatories

Address: WebinarNinja - Team ON PTY LTD, 333 George Street, Level 13, Sydney, NSW 2000, Australia

Other Information necessary in order for the contract to be binding (if any):

Signature 

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other Information necessary in order for the contract to be binding (if any):

Signature _____

Date _____