UPSCOPE

Data Processing Addendum

This Data Processing Addendum (this **“DPA”**) is entered into by and between the Upscope Entity (**“Upscope”**, or **“we”**) and the Customer listed on the Master Services Agreement this DPA is incorporated into (the **“Customer”**, or **“you”**).

Customer has entered into one or more agreements with Upscope (each, as amended from time to time, an **“Agreement”**) governing the provision of Upscope’s software (the **“Services”**). This DPA will amend the terms of the Agreement to reflect the parties’ rights and responsibilities with respect to the processing and security of Customer Data (as defined below) under the Agreement.

Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. **Definitions.**

    1.1. **“CCPA”** means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq.) and its regulations; as may be amended, superseded or replaced from time to time.

1.2. **“Customer Data”** means data Customer submits to, stores on, or sends to Upscope via the Service.

1.3. **“Data Incident”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on systems that are managed and controlled by Upscope. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including, without limitation, pings, port scans, denial of service attacks, network attacks on firewall or networked systems, or unsuccessful login attempts.

1.4. **“Europe”** means, for the purposes of this DPA, the member states of the European Economic Area, Switzerland and the United Kingdom.

1.5. **“European Data Protection Legislation”** means the data protection and privacy laws and regulations enacted in Europe and applicable to the Personal Data in question, including as applicable: (a) the GDPR; (b) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and/or (c) in respect of the United Kingdom, the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (**“UK GDPR”**) and the Data Protection Act 2018; in each case as may be amended, superseded or replaced from time to time.

1.6. **“GDPR”** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.7. **“Notification Email Address”** means the email address(es) that Customer designates to receive notifications when Customer creates an account to use the Service. Customer agrees to be

solely responsible for ensuring that their Notification Email Address is current and valid at all times.

1.8. **"Personal Data"** means any personal data or personal information (as those terms are defined by European Data Protection Legislation and the CCPA, as applicable) contained within Customer Data.

1.9. **"Privacy Laws"** means: (a) the CCPA; and (b) European Data Protection Legislation.

1.10. **"Standard Contractual Clauses"** or **"SCCs"** means (a) where the GDPR applies, the standard contractual clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021 (**"EU SCCs"**); and (ii) where the UK GDPR applies, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (**"UK SCCs"**).

1.11. **"Subprocessor"** means a third party that we use to process Customer Data in order to provide parts of the Service and/or related technical support. For the avoidance of doubt, the term Subprocessor shall not include Upscope employees or contractors.

1.12. **"Term"** means the term of the Agreement.

1.13. The terms **"personal data"**, **"special categories of personal data"**, **"data subject"**, **"process"**, **"processing"**, **"controller"**, **"processor"** and **"supervisory authority"** have the meanings given in European Data Protection Legislation or, if not defined therein, the GDPR

2. **Data Processing.**

2.1. **Roles and Regulatory Compliance.**

2.1.1. Scope of this DPA. This DPA applies where and only to the extent Upscope processes Personal Data as a processor (for

the purposes of European Data Protection Legislation) or service provider (for the purposes of and as defined by the CCPA).

2.1.2. **Roles and Responsibilities.** The Parties acknowledge and agree as follows: (i) that Upscope will process the Personal Data as described in Annex I; (ii) that for the purposes of European Data Protection Legislation, Upscope is a processor of Personal Data and Customer is the controller (or a processor acting on behalf of a third party controller); (iii) if the CCPA applies to processing of Personal Data, Upscope shall act solely as a service provider (as that term is defined under the CCPA) on behalf of Customer; (iv) Upscope shall not retain, use or disclose Personal Data for any purpose other than the purposes described in this DPA, and shall not "sell" Personal Data (within the meaning under the CCPA); and (iv) that each party will comply with their obligations under Privacy Laws with respect to the processing of Personal Data.

2.1.3. **Authorization by Third Party Controller.** If Customer is a processor of Personal Data acting on behalf of a third party controller:

2.1.3.1. Customer warrant to Upscope that Customer's instructions and actions with respect to that Personal Data, including Customer's appointment of Upscope as another processor, have been authorized by the relevant controller; and

2.1.3.2. Customer will serve as Upscope's sole point of contact and where Upscope would otherwise be required (including for the purposes of the Standard Contractual Clauses) to provide information, assistance or cooperation to or seek authorization

from any such third party controllers, Upsocpe may provide such information, assistance or cooperation to or seek such authorization from Customer.

2.2. **Customer Responsibilities.**

2.2.1. **Customer Authorization.** Upscope shall process Personal Data in accordance with Customer's documented lawful instructions. By entering into this DPA, Customer hereby authorizes and instructs us to process Personal Data: (i) to provide the Service, and related technical support; (ii) as otherwise permitted or required by Customer's use of the Service and/or Customer's requests for technical support; (iii) as otherwise permitted or required by the Agreement, including this DPA; and (iv) as further documented in any other written instructions that are agreed by the parties. Upscope will not process Personal Data for any other purpose, unless required to do so by applicable law or regulation. The parties agree that the Agreement (including this DPA), and Customer's use of the Service in accordance with the Agreement, set out Customer's complete and final processing instructions and any processing outside the scope of these instructions (if any) shall require prior written agreement between the parties. Customer shall ensure its instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate Privacy Laws. Notwithstanding the foregoing, if Customer is a processor of Personal Data acting on behalf of a third party controller then where legally required Upscope is entitled to follow the instructions of such third party controllers with respect to their Personal Data.

2.2.2. **Prohibition on Sensitive Data.** Customer will not submit, store, or send any sensitive data or special categories of personal data (collectively, **"Sensitive Data"**) to Upscope for

processing, and Customer will not permit nor authorize any of Customer's employees, agents, contractors, or data subjects to submit, store, or send any Sensitive Data to Upscope for processing. Customer acknowledges that Upscope does not request or require Sensitive Data as part of providing the Service, that Upscope does not wish to receive or store Sensitive Data, and that Upscope's obligations in this DPA will not apply with respect to Sensitive Data. Customer shall ensure that they correctly configure the Software (specifically the Masking functionality) to comply with this DPA.

3. **Deletion.**

3.1. **During the Subscription Term.** Upscope will enable Customer to delete Personal Data during the Subscription Term in a manner that is consistent with the Documentation. If Customer uses the Software to delete any Personal Data in a manner that would prevent Customer from recovering Personal Data at a future time, Customer agrees that this will constitute an instruction to Upscope to delete Personal Data from the Upscope Cloud in accordance with Upscope's standard processes and applicable law. Upscope will comply with this instruction as soon as reasonably practicable, but in all events in accordance with applicable law.

3.2. **Deletion when the Subscription Term expires.** When the Subscription Term expires, Upscope will destroy any Personal Data in our possession or control. This requirement will not apply to the extent that we are required by applicable law to retain some or all of the Personal Data, in which event we will isolate and protect the Personal Data from further processing and delete in accordance with Upscope's deletion practices, except to the extent required by law. You acknowledge that you will be responsible for exporting, before the Subscription Term expires,

any Personal Data you want to retain after the Subscription Term expires.

4. **Data Security.**

4.1. **Security Measures.** Upscope will implement and maintain appropriate technical and organizational measures to protect Personal Data against Data Incidents and to preserve the security and confidentiality of Personal Data, as described on the Upscope Website (collectively, the **"Security Measures"**). Upscope shall ensure that any person who is authorized by Upscope to process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). Customer acknowledges that Security Measures are subject to technical progress and development and that accordingly we 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 Service.

4.2. **Data Incidents.** Upon becoming aware of a Data Incident, we will notify you promptly and without undue delay, and will take reasonable steps to minimize harm and secure Personal Data. Any notifications that we send you pursuant to this Section 4.2 will be sent to your Notification Email Address and will describe, to the extent possible and/or known to Upscope, the details of the Data Incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for you to minimize the impact of the Data Incident. We will not assess the contents of any Personal Data in order to identify information that may be subject to specific legal requirements. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third-party notification obligations related to any Data Incident(s). Our notification of or response to a Data Incident under this Section will not constitute an

acknowledgement of fault or liability with respect to the Data Incident.

4.3. **Customer's Security Responsibilities.** Customer agrees that, without prejudice to our obligations under Sections 4.1 or 4.2: (i) you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Data, securing any account authentication credentials, systems, and devices you use to use the Service, and backing up your Customer Data. You understand and agree that we have no obligation to protect Customer Data that you elect to store or transfer outside of our or our Subprocessors' systems (e.g., offline or on-premise storage). You are solely responsible for evaluating whether the Service and our commitments under this Section 4 meet your needs, including with respect to your compliance with any of your security obligations under Privacy Laws, as applicable.

4.4. **Audit Rights.**

4.4.1. **Audit Reports.** You acknowledge that Upscope is regularly audited against various information security standards by independent third-party auditors and internal auditors, respectively. Upon request, we shall supply (on a confidential basis) a summary copy of our audit report(s), so that you can verify our compliance with the audit standards against which it has been assessed, and this DPA. Further, we will provide written responses (on a confidential basis) to all reasonable requests for information necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year.

4.4.2. **Independent Audits.** While it is the parties' intention to rely ordinarily on the provision of the above audit report(s) to verify our compliance with this DPA, we will allow an

internationally-recognized independent auditor that you select to conduct audits to verify our compliance with our obligations under this DPA. You must send any requests for audits under this Section 4.4.2 to legal@upscope.com. Following our receipt of your request, the parties will discuss and agree in advance on the reasonable start date, scope, duration, and security and confidentiality controls applicable to the audit. You will be responsible for any costs associated with the audit. You agree not to exercise your audit rights under this Section 4.4.2 more than once in any twelve (12) calendar month period, except (i) if and when required by a competent data protection authority; or (ii) an audit is necessary due to a Data Incident. You agree that (to the extent applicable), you shall exercise any audit rights under Privacy Laws and the Standard Contractual Clauses by instructing us to comply with the measures described in this Section 4.4.

5. **Data Subject Rights.**

5.1. You acknowledge that the Software may, depending on the functionality of the Software, enable you to: (i) access the Customer Data; (ii) rectify inaccurate Customer Data; (iii) restrict the processing of Customer Data; (iv) delete Customer Data; and (v) export Customer Data.

5.2. To the extent that you cannot access the relevant Personal Data within the Service, we will provide you, at your expense, with all reasonable and timely assistance to enable you to respond to: (i) requests from data subjects who wish to exercise any of their rights under applicable Privacy Laws; and (ii) any other correspondence, enquiry or complaint received from a data subject, supervisory authority or other third party in connection with the processing of the Customer Data. In the event that any such request, correspondence, enquiry or complaint is made

directly to us, we will promptly inform you of it, and provide you with as much detail as reasonably possible.

6. **Data Transfers.**

6.1. **Data Storage and Processing Facilities.** You agree that, unless you configure your Account to only use our European or UK datacenter, we will, subject to Section 6.2, store and process Customer Data in the United States and any other countries we operate datacenters in. Upscope shall ensure that such transfers are made in compliance with applicable Privacy Laws and this DPA.

6.2. **Transfers of Data out of Europe.** If the storage and/or processing of Personal Data as described in Section 6.1 involves a transfer of Personal Data to Upscope outside of Europe, and European Data Protection Legislation applies to the transfer (collectively, **"Transferred Personal Data"**), then (i) the Standard Contractual Clauses shall be incorporated into and form a part of this DPA in accordance with Section 6.3. With respect to Transferred Personal Data, you agree that if we adopt an alternative data transfer mechanism (including any new version of, or successor to, the Standard Contractual Clauses adopted pursuant to applicable European Data Protection Legislation) for Transferred Personal Data not described in this DPA (**"Alternative Transfer Solution"**), the Alternative Transfer Solution shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Solution complies with applicable European Data Protection Legislation and extends to the territories to which Transferred Personal Data is transferred), and if we request that you take any action (including, without limitation, execution of documents) reasonably required to give full effect to that solution, you will promptly do so.

6.3. **Standard Contractual Clauses.** For the purposes of the Standard Contractual Clauses, the parties agree that (i) Upscope is the "data importer" and Customer is the "data exporter"; (ii) the EU SCCs shall be incorporated in the form attached hereto and the UK SCCs shall be incorporated by reference; (iii) the Annexes or Appendices of the EU SCCs and UK SCCs (as applicable) shall be populated with the information from Annexes I, II and III of this DPA; and (iv) the EU SCCs shall be governed by the laws of the Republic of Ireland and the UK SCCs shall be governed by the laws of England and Wales. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses shall prevail to the extent of such conflict. In particular, nothing in the DPA shall exclude the rights of third-party beneficiaries granted under the Standard Contractual Clauses. You agree that in the event we cannot ensure compliance with the Standard Contractual Clauses, we will inform you promptly and you will provide us with a reasonable period of time to cure any non-compliance. You will reasonably cooperate with us to agree what additional safeguards or measures, if any, may be reasonably required to cure the non-compliance and will only be entitled to suspend the transfer of Personal Data and/or terminate the affected parts of the Service if we have not or cannot cure the non-compliance before the end of the cure period.

7. **Subprocessors.**

7.1. **Consent to Engagement.** You authorize us to engage third parties as Subprocessors. Whenever we engage a Subprocessor, we will enter into a contract with that Subprocessor which imposes data protection terms that require the Subprocessor to

protect Personal Data to an equivalent standard required under this DPA, and we shall remain responsible for the Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause us to breach any of our obligations under this DPA.

7.2. **List of Subprocessors.** A list of our current Subprocessors is set out in Annex III. We may update the list of Subprocessors upon thirty (30) days' prior written notice to you, during which period you will have the opportunity to object as described in Section 7.3 below.

7.3. **Objections; Sole Remedy.** During the thirty (30) day period beginning on the date we notify you of any new or replacement Subprocessor, you have the right to object to the appointment of that Subprocessor on reasonable grounds that the Subprocessor does not or cannot comply with the requirements set forth in this DPA (each, an **"Objection"**). If we do not remedy or provide a reasonable workaround for your Objection within a reasonable time, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party. Upscope will not owe Customer a refund of any fees Customer has paid in the event Customer decides to terminate the Agreement pursuant to this Section.

7.4. **Disclosure of Subprocessor agreements.** You agree that by complying with this Section 7, we fulfil our obligations under Clause 9(a) and 9(b) of the Standard Contractual Clauses. You further acknowledge that, for the purposes of Clause 9(c) of the Standard Contractual Clauses, we may be restricted from disclosing Subprocessor agreements to you (or the relevant third party controller) due to confidentiality restrictions. Notwithstanding this, we shall use reasonable efforts to require Subprocessors to permit us to disclose Subprocessor agreements

to you and, in any event, will provide (upon request and on a confidential basis) all information we reasonably can in connection with such Subprocessor agreement.

8. **Additional information.**

8.1. You acknowledge that we are required under European Data Protection Legislation (i) to collect and maintain records of certain information, including, among other things, the name and contact detail of each processor and/or controller on whose behalf we are acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (ii) to make such information available to the supervisory authorities. Accordingly, if European Data Protection Legislation applies to the processing of Personal Data, you will, when requested, provide this additional information to us, and ensure that the information is kept accurate and up-to-date.

9. **Data Protection Impact Assessment.**

9.1. We will provide you with reasonable and timely assistance as you may require in order to conduct a data protection impact assessment and, if necessary, consult with the relevant data protection authority

10. **Miscellaneous.**

10.1. With the exception of the third-party beneficiary rights granted (where applicable) under the Standard Contractual Clauses, there are no third-party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to Upscope's limitations of liability, which will remain in full force and effect. Notwithstanding the foregoing, in no event shall

either party exclude or limit its liability with respect to any data subject's rights under European Data Protection Legislation or the Standard Contractual Clauses. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail. This DPA amends and supersedes any prior data processing addendum or similar agreement regarding its subject matter.

11. **Change in Privacy Laws.**

11.1. Notwithstanding anything to the contrary in the Agreement (including this DPA), in the event of a change in Privacy Laws or a determination or order by a supervisory authority or competent court affecting this DPA or the lawfulness of any processing activities under this DPA, we reserve the right to make any amendments to this DPA as are reasonably necessary to ensure continued compliance with European Data Protection Legislation or compliance with any such orders.

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, 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")

(c) have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

(e) 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 - Clause 12(a), (d) and (f);

(v) Clause 13;

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

(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, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6: Description of the transfers

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 (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:

(a) 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;
(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
(c) 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
(d) 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) OPTION 2: 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 thirty (30) 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) OPTION 2: 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.

(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

(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) 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.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III — LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14: Local laws and practices affecting compliance with the Clauses

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

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

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

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

(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.

MODULE TWO: Transfer Controller to Processor

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

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

MODULE THREE: Transfer processor to processor

(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). 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, 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 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

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.

(Module 3: 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 authorities, whether requests have been challenged and the outcome of such challenges, etc.). (module 3: 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 suspensory 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. (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 (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

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 the Republic of Ireland.

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 Republic 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.

Annex I

List of Parties

A. List of Parties

Data exporter(s):

Name: Customer (as defined in the DPA)

Address: Customer's address (as provided by Customer in the Order Form)

Contact person's name, position and contact details: Customer's contact details (as provided by Customer in the Order Form or in their Account Settings)

Role (controller/processor): Controller/processor

Data importer(s):

Name: Upscope (as defined in the DPA)

Address: Upscope's address (as provided in the Master Services Agreement)

Contact person's name, position and contact details: Pardeep Kullar, DPO, legal@upscope.com

Role (controller/processor): Processor

B. Data Processing Description

Subject Matter: Upscope's provision of the Software to Customer, and related technical support.

Purpose of the Processing: Upscope will process personal data submitted to, stored on, or sent via the Software for the purpose of providing the Service and related technical support in accordance with this DPA.

Categories of Data Subjects: The personal data transferred concern the following categories of data subjects:

- End users of the Service
- Individuals whose personal data is supplied by end users of the Service.

Categories of Personal Data: The personal data transferred concern the following categories of data:

- Direct identifying information (e.g. name, email address, telephone)
- Indirect identifying information (e.g. job title, gender, date of birth)
- Device identification data and traffic data (e.g. IP addresses, MAC addresses, web logs, browser agents)
- Any personal data supplied by end users of the Service

Sensitive Data: The personal data transferred to Upscope through the Service is determined and controlled by Customer. As such, Customer controls the content of the personal data transferred to Upscope and is solely responsible for ensuring the legality of the categories of data it may choose to transfer to Upscope. The DPA includes an express prohibition on the transfer of special categories of personal data to Upscope.

Frequency of the Transfer: Continuous

Nature of the Processing: Upscope will perform the following basic processing activities: processing to provide the Service in accordance with the Agreement; processing to perform any steps necessary for the performance of the Agreement; and processing to comply with other reasonable instructions provided by Customer (e.g. via email) that are consistent with the terms of the Agreement.

Period for which the personal data will be retained: Throughout the Subscription Term plus the period from expiry of the Subscription Term until deletion of Personal Data by Upscope in accordance with the Agreement.

C. Competent Supervisory Authority

The Irish Data Protection Commissioner.

Annex II

Security Measures

Summary

We host our servers in highly secure, SOC 2 certified data centers and use the latest security practices to protect our customers' data. 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.

Upscope security

- All our offices are equipped with CCTV and 24/7 security personnel and access control.
- All actions performed by our employees on your account (such as updating information, viewing your users when you request it for testing, etc.) are monitored and logged.
- All our employees are background checked to the PCI DSS standard.
- Before our employees can perform any action on Upscope they need to authenticate with two factor authentication.
- Our offices are fully ISO 27001 compliant and all our employees are trained on data security regularly.
- Upscope undergoes regular audits and penetration testing.

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 support SAML-based SSO.

Annex III

Subprocessors

Name	Address	Description
Amazon Web Services	410 Terry Avenue North Seattle, WA 98109 United States	Cloud infrastructure services
MongoDB, Inc	100 Forest Avenue Palo Alto, CA 94301 United States	Data storage services
Sentry, Inc	45 Fremont Street, 8th Floor, San Francisco, CA 94105	Cloud monitoring
NewRelic, Inc	188 Spear Street, Suite 1000, San Francisco, CA 94105, United States.	Cloud monitoring
Wildbit, LLC (Postmark)	12 Penns Trail, #521, Newtown, PA 18940	Email delivery