Note to copy:

The Retrium Data Processing Agreement is made available at https://www.retrium.com/gdpr. No changes made to this copy are agreed to by Retrium, Inc. or its affiliates.

If you have questions please contact Retrium at support@retrium.com.

Last Modified: January 2023

Retrium Data Processing Agreement

Retrium, Inc. ("**Retrium**") takes the security and privacy of data subjects seriously and wishes to comply with relevant Data Protection Laws.

We update these terms from time to time. If you have an active Retrium subscription, we will let you know when we do via email (if you have subscribed to receive email notifications via the link in our Master Terms) or via in-app notification.This Data Processing Addendum ("**Addendum**") forms part of the Subscription Agreement or other agreement ("**Agreement**") between Retrium and the customer ("**Customer**") (each a "**party**" and collectively the "**parties**") and reflects each party's agreement with regard to the processing of personal data in accordance with the requirements of the applicable Data Protection Laws.

Retrium leverages the Standard Contractual Clauses (including Appendix 1, Appendix 2 and Appendix 3) for data transfers outside the European Economic Area and the United Kingdom.

1. Definitions Final

a. "**Customer Personal Data**" means any personal data that Retrium processes on behalf of Customer via the Service, as more particularly described in this Addendum.

b. "**Data Protection Law**" means all applicable laws and regulations, including (without limitation) of the European Union, the European Economic Area, their Member States and the United Kingdom, which are applicable to the processing of Customer Personal Data under this Addendum including (without limitation) the GDPR and the Irish Data Protection Acts, as amended from time to time. All references to Directive 95/46/EC shall be read as inclusive of their meaning under the GDPR.

c. "**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 regards to the processing of data and on the free movement of such data, and repealing Directive 95/46/EC. "GDPR" shall be construed as also referring to the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**") (in this Addendum, any references to specific articles of the GDPR shall be construed as also referring to the equivalent sections of the UK GDPR, where applicable).

d. "**Services**" means those services and other activities to be provided to Customer by or on behalf of Retrium pursuant to the Agreement;

e. "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in decision 2010/87/EU, or any set of clauses approved by the European Commission or a supervisory authority which subsequently amends, replaces or supersedes the same.

f. "**Sub-processor**" means any processor engaged by Retrium to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this Addendum. Sub-processors may include third parties or affiliates of Retrium but shall exclude Retrium employees, contractors, or consultants.

The terms "**personal data**", "**controller**", "**data subject**", "**processor**", "**processing**", "**supervisory authority**" shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and "**process**", "**processes**" and "**processed**", with respect to any Customer Personal Data, shall be interpreted accordingly.

2. Roles and Responsibilities

a. Roles of Parties. The parties acknowledge that in relation to any Customer Personal Data, Customer is a controller and Retrium is a processor.

b. Appointment. Customer appoints Retrium to process Customer Personal Data on Customer's behalf only as is necessary to provide the Services and as may subsequently be agreed to by the parties in writing.

c. Legitimacy of Processing. Customer is responsible for ensuring a valid legal basis for processing the Customer Personal Data as well as any transfer of Customer Personal Data to Retrium or a third party.

d. Details of Processing. The subject matter and details of processing are described in Annex 1 of this Addendum.

e. Compliance with Law. Each party agrees it will comply with its obligations under the Data Protection Laws relating to any Customer Personal Data it processes under or in relation to this Addendum.

3. Retrium Obligations

a. Processing Obligations. Where Retrium processes Customer Personal Data under or in connection with the Agreement, Retrium shall:

I. Unless otherwise required by applicable law, only process such Customer Personal Data as may be necessary to perform its obligations under the Agreement, and only in accordance with Customer's instructions.

II. Put in place appropriate technical and organizational security measures to protect against unauthorized or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data ("**Personal Data Breach**").

III. Provide reasonable co-operation to Customer in the event of an inquiry by a supervisory authority relating to Retrium's processing of Customer Personal Data.

IV. Keep Customer Personal Data confidential and ensure that Retrium staff who have access to Customer Personal Data are subject to appropriate confidentiality obligations.

V. Notify Customer without undue delay after becoming aware of any Personal Data Breach involving Customer Personal Data.

VI. Taking into account the nature of the processing, provide reasonable cooperation and assistance to Customer as Customer may reasonably require to allow Customer to comply with its obligations under Articles 32 - 36 of the GDPR, as applicable, including in relation to data security, data breach notification, data protection impact assessments, prior

consultation with supervisory authorities, the fullfilment of data subjects' rights, and any enquiry, notice or investigation by a supervisory authority.

VII. Save as may be required or permitted by applicable law, delete or return all Customer Personal Data on termination of the Agreement at the written direction of Customer.

VIII. Inform Customer immediately if, in its opinion, the Customer's processing instructions infringe Data Protection Laws.

4. Sub-processing

a. Authorized Sub-processors. Customer agrees that Retrium may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Retrium and authorized by Customer are available here (https://www.retrium.com/retrium-subprocessor-list). Retrium shall notify Customer if it adds or removes Sub-processors at least thirty (30) days prior to any such changes if Customer opts in to receive such notifications by registering here (https://www.retrium.com/retrium-subprocessor-list). If Customer has a reasonable objection to a proposed Sub-processor, Retrium shall work with Customer to make available a commercially reasonable change to avoid the use of that proposed Sub-processor and, if such change cannot be made, Customer may by written notice to Retrium terminate those Services which cannot be provided by Retrium without the use of the objected-to Sub-processor.

b. Sub-processor Obligations. Retrium shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Personal Data as those in this Addendum, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this Addendum and for any acts or omissions of such Sub-processor that cause Retrium to breach any of its obligations under this Addendum.

5. Security Reports and Audits

a. Audit Rights. Retrium shall make available to Customer all information reasonably necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this Addendum. Customer acknowledges and agrees that it shall exercise its audit rights under this Addendum (including this Section 5a and where applicable, the Standard Contractual Clauses) and any audit rights granted by Data Protection Laws, by instructing Retrium to comply with the audit measures described in Sections 5b – 5d below.

b. Security Reports. Upon Customer's request, Retrium shall make available for Customer's review copies of certifications or reports demonstrating Retrium's compliance with this Addendum and the prevailing data security standards applicable to the processing of Customer Personal Data.

c. Security Due Diligence. In addition, Retrium shall respond to all reasonable requests for information made by Customer to confirm Retrium's compliance with this Addendum, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written reasonable request, provided that Customer shall not exercise this right more than once per calendar year.

d. Inspections. Where Customer reasonably believes the information provided under Section 5b and 5c above is not sufficient to demonstrate Retrium's compliance with this Addendum, at Customer's expense, Retrium shall permit Customer, or its appointed third-party auditors (collectively, "**Auditor**"), to audit the architecture, systems and procedures relevant to Retrium's compliance with this Addendum and shall make available to the Auditor all information, systems and staff necessary for the Auditor to conduct such audit. To the extent any such audit incurs in excess of 10 hours of Retrium personnel time, Retrium may charge Customer on a time and materials basis for any such

excess hours. Before the commencement of an audit described in this Section 5d, Retrium and Customer will mutually agree upon the reasonable scope, start date, duration of and security and confidentiality controls applicable to the audit. Customer agrees that:

I. audits will be conducted during Retrium's normal business hours;

II. it will not exercise its on-site audit rights more than once per calendar year, (unless required more frequently by Data Protection Law, an order of a supervisory authority or court, or in the event of a Personal Data Breach);

III. it will be responsible for any fees charged by any third party auditor appointed by Customer to execute any such audit;

IV. Retrium may object to any third-party auditor appointed by Customer to conduct an audit if the auditor is, in Retrium's opinion, not suitably qualified or independent, a competitor of Retrium or otherwise manifestly unsuitable. Any such objection by Retrium will require Customer to appoint another auditor or conduct the audit itself;

V. nothing in this Section 5 will require Retrium either to disclose to the Auditor, or to allow the Auditor access to (a) any data processed by the Retrium on behalf of any other organisation, (b) any Retrium internal accounting or financial information, (c) any trade secret of Retrium, (d) any information that, in Retrium's opinion, could (i) compromise the security of any Retrium systems or premises, or (ii) cause Retrium to breach its obligations to Customer or any third party, or (e) any information that Customer seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Data Protection Law; and

VI. shall provide Retrium with copies of any audit reports completed by the Auditors.

6. International Transfers

a. Data Center Locations. Customer acknowledges that Retrium may transfer and process Customer Personal Data to and in the United States and anywhere else in the world where Retrium, its affiliates or its Sub-processors maintain data processing operations. Retrium shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this Addendum.

b. European Transfers. To the extent that Retrium processes Customer Personal Data to which the GDPR or UK GDPR applies in a territory outside of the European Economic Area and/or the United Kingdom that does not provide adequate protection for Personal Data (as determined by applicable Data Protection Laws), Retrium and Customer hereby enter into the Standard Contractual Clauses in respect of any transfer of Customer Personal Data from Customer (as "data exporter") to Retrium (as "data importer") where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses.

c. Additional terms for Standard Contractual Clauses:

I. For the purposes of Clause 15(a)(i) of the Standard Contractual Clauses, Retrium agrees that (i) it will not disclose Customer Personal Data to a law enforcement authority unless it is ordered to do so by a court of competent jurisdiction and in compliance with this Addendum; (ii) it will promptly without undue delay, and in any event no more than five (5) days after it becomes aware of the obligation to provide notice, notify Customer about any legally binding request or court order for disclosure of Customer Personal Data to a law enforcement authority, thereby giving Customer an opportunity to challenge or object to the request or court order, unless such notice is otherwise prohibited by applicable law; and (iii) where Retrium notifies Customer of a law enforcement request or court order and Customer agrees

that it is legally binding, it shall agree with Customer which specific and limited categories of Customer Personal Data may be shared with law enforcement, and will share only those categories which are deemed necessary to satisfy the request in question.

II. Customer agrees that the audits described in Clause 8 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with Section 5 of this Addendum.

III. Customer agrees that Retrium shall provide the certification of deletion of Personal Data that is described in Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses to Customer upon Customer's request.

IV. The Appendices of the Standard Contractual Clauses shall contain the information set forth in Appendix 2 (Appendices to Standard Contractual Clauses) to this Addendum.

V. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

7. General

a. Variations. Retrium may propose variations to this Addendum and the Standard Contractual Clauses which Retrium reasonably considers to be necessary to address the requirements of any Data Protection Laws, and the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Retrium's notice as soon as is reasonably practicable.

b. Termination. The parties agree that this Addendum shall terminate automatically upon termination of the Agreement. Notwithstanding the foregoing, any obligation imposed on Retrium under this Addendum in relation to the processing of Customer Personal Data shall survive any termination or expiration of this Addendum.

c. Governing Law. This Addendum shall be governed by the governing law of the Agreement.

d. Choice of Jurisdiction. The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum.

e. Order of Precedence. Nothing in this Addendum reduces Retrium's obligations under the Agreement in relation to the protection of Customer Personal Data or permits Retrium to process (or permit the processing of) Customer Personal Data in a manner which is prohibited by the Agreement. In the event of any inconsistency between this Addendum and any other agreements between the parties, including but not limited to the Agreement, the Addendum shall prevail.

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

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date it is signed by both parties.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

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

b. The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data

exporter and/or data importer, with the following exceptions:

I. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

II. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

IV. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

V. Clause 13;

VI. Clause 15.1(c), (d) and (e);

VII. Clause 16(e);

VIII. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

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 (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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 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. (8) 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 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. (9) 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 fulfill 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

MODULE ONE: Transfer controller to controller

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. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

c. 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.

d. The Parties agree that if one Party is held liable under paragraph (c), 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.

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

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

   [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

   [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

II. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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 fulfill 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

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. [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

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.

Appendices to the Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

Data exporter(s): (Identity and contact details of the data exporter(s) and, where applicable of its/their data protection officer and/or representative in the European Union)

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role: Controller

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

Name: Retrium, Inc.

Address: 8705B Colesville Road Suite 219 Silver Spring, MD 20910 USA

Contact person's name, position and contact details:

Niki Kohari, COO, privacy@retrium.com

Activities relevant to the data transferred under these Clauses:

Retrium is a collaboration platform which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Signature and date:

Role: Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's Users authorized by Customer to use the Services
- Any other categories of data subjects whose personal data is processed

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Customer's Users authorized by Customer to use the Services
- First and last name
- Contact information (company, email, phone, physical business address)
- Employment-related data (position, job title, employer)

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.

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

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

Continuous

Nature of the processing

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

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

Upon contract termination if the importer receives a written request within sixty (60) days after such termination, data will be returned or destroyed.

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

The objective of Processing of Personal Data by subprocessors is the performance of the Services and to fulfill business related objectives.

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Customer's Users authorized by Customer to use the Services
- First and last name
- Contact information (company, email, phone, physical business address)
- Employment-related data (position, job title, employer)

Upon contract termination and upon written request within sixty (60) days after such termination, data will be returned or destroyed.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority/ies will be selected in accordance with Clause 13. Retrium uses the following directory for assessment:
https://docs.google.com/document/d/1vczOKNZTC_gY87qfM20eZxs0Yjn383KnDR52iBECguU/edit

ANNEX II

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by data exporter, and accessible via https://www.retrium.com or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

Technical and organisational measures taken may include and are not limited to:

- Third-party assessments (such as pentest, vulnerability scans and SOC audits)
- SLAs
- Retrium uses trusted suppliers, such as Amazon AWS, for data storage and takes precautions to ensure data is protected both in transit and at rest
- IDS, IPS, firewalls, and logging are all utilized for prevention and protection.
- Username and passwords (encrypted) are enabled for users; certain subscriptions are eligible for SSO
- Data can be returned or destroyed, upon contract termination and at the customer's written request
- We have evaluated our subprocessors and verified their SCC compliance.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

The controller has authorised the use of the following sub-processors:
https://www.retrium.com/retrium-subprocessor-list