Data Processing Addendum (Provider as Processor)

Last Updated: January 27, 2025

This Data Processing Addendum ("**DPA**") between Provider, acting on its own behalf and as agent for each Provider affiliate as may be applicable (collectively, "**Provider**") and Client, is incorporated into and forms part of the Terms of Service ("**Terms**") and Order Form ("**OF**") between the parties, and reflects the parties' agreement with regard to the Processing of Personal Data.

Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Provider processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "**Client**" shall include Client and Authorized Affiliates.

In the course of providing the Services to Client pursuant to the Agreements, Provider may Process Personal Data on behalf of Client and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

This DPA shall be effective as of the effective date of the OF(s) into which it is incorporated or attached ("**Effective Date**").

Data Processing Terms

1. Definitions

Each capitalized term not defined herein shall have the meaning set forth in the Agreements or the applicable Data Protection Laws.

"**Agreements**" means the Terms, OF(s), this DPA and any other written agreements between the parties.

"**Authorized Affiliate**" means any of Client's affiliate(s) which (a) is subject to applicable Data Protection Laws, and (b) is permitted to use the Services pursuant to the Terms and OF(s) between Client and Provider, and has signed its own OF(s) with Provider.

"**CCPA and US State Privacy Laws**" means the US State data privacy laws, including the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq.*, as amended, and its implementing regulations ("**CCPA**").

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data, and in the case of the Services provided under the Terms and the OF(s), the Client is the Controller.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreements, which may include without limitation, the GDPR, UK GDPR, CCPA and US State Privacy Laws, and the data protection laws and regulations of any other country, state, or territory which apply to such Processing.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**EEA SCCs**" means the standard contractual clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as updated, amended, replaced or superseded from time to time by the European Commission.

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

"**Personal Data**" means any information provided by or on behalf of Client for the purpose of performing the Services relating to (i) an identified or identifiable natural person or household, and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws).

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, and in the case of the Services provided under the Terms and the OF(s), "Processor" means "Provider."

"**Provider Standard Business** Hours" means 9:00 am-5:00 pm EDT, Monday through Friday, excluding holiday hours (which may vary based on time zone and geographic location).

"**Restricted Transfer**" means a transfer of Personal Data from Client to Provider, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses.

"**Standard Contractual Clauses**" means either the EEA SCCs or the UK IDTA, as applicable to a Restricted Transfer.

"**Sub-processor**" means any sub-processor engaged by Provider or its affiliates, who receives Personal Data from Processor in connection with the Services.

"**UK GDPR**" means the GDPR as transposed into United Kingdom national law by operation 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 IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under Section 119A(1) Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the UK Government.

2. Processing of Personal Data

2.1 Client's Processing of Personal Data. With regard to the Processing of Personal Data under the Agreements, Client is the Controller and Provider is the Processor. Each of Provider and Controller shall comply, in the performance of its respective obligations under the Agreements, with applicable Data Privacy Laws. Client's instructions to Provider for the Processing of Personal Data shall comply with Data Protection Laws. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

2.2 Provider's Processing of Personal Data. Provider shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Client's written instructions for the following purposes: (i) Processing in accordance with the Agreements; and (ii) Processing to comply with other written reasonable instructions provided by Client personnel (e.g., via email) where such instructions are consistent with the Agreements. Provider will promptly inform Client if Provider has actual knowledge that a Client instruction infringes Data Protection Laws, provided that Provider's will not incur any liability for its failure to provide such notice to Client.

2.3 Data Protection Impact Assessment. Upon Client's request and only during Provider's Standard Business Hours, Provider shall provide Client with reasonable cooperation and assistance needed to fulfill Client's obligation under Data Protection Laws to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to Provider. Client shall be responsible for any costs arising from Provider's provision of such assistance.

2.4 Audits. Upon Client's written request, and subject to the confidentiality obligations set forth in the Agreements, Provider shall make available to Client (or Client's independent, third-party auditor) information as may be reasonably requested by Client from time to time regarding Provider's compliance with the obligations set forth in this DPA, and will allow for audits conducted by Client (or by Client's independent, third-party auditor), by completing a data protection questionnaire of reasonable length not more than once annually during Provider Standard Business Hours. To the extent permitted by Data Protection Laws, the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with this Section 2.4.

2.5 Limits to DPIAs and Audits. No assessment described in Section 2.3 or audit described in Section 2.4 above (or in Clause 8.9 of the Standard Contractual Clauses): will (i) be conducted by a competitor of Provider, or in a manner that unreasonably interferes with Provider's business or provision of the Services; (ii) require Provider to disclose information that in Provider's reasonable determination would compromise its security measures or that constitutes information that Provider is obligated to keep confidential pursuant to contractual or fiduciary obligations to third parties or applicable legal obligations; or (iii) include networks, systems, or storage facilities, or other records or information, other than those that are reasonably related to the provision of the Services. Such assessments and audits do not include any rights to come on-site to any of Provider's premises or to access any of Provider's systems.

2.6 Representations and Responsibilities of Client. Client confirms that it (i) has all necessary rights or consents to collect the Personal Data from the applicable Data Subjects and transfer such Personal Data to Provider for all Processing to be performed under the Agreements; and (ii) will not transfer to Provider any Personal Data that is not required for Provider to perform the Services for Client. Client agrees that it will not use the Services in a manner that violates the rights of any Data Subject that has opted-out from disclosures of Personal Data under applicable Data Protection Laws.

3. Rights of Data Subjects

Provider shall promptly notify Client if Provider receives a request from a Data Subject to exercise the Data Subject's rights under Data Protection Laws ("**Data Subject Request**"). Client shall then respond to such Data Subject Request in compliance with Data Protection Laws. To the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Provider shall provide reasonable assistance to Client to help Client fulfill such Data Subject Request. Such assistance is subject to Client's ability to identify the applicable Personal Data in a manner that is sufficiently specific given the technical constraints of the Services. Client shall be responsible for any costs arising from Provider's provision of such assistance. Client acknowledges that any Data Subject Request that results in deletions, modifications or restrictions on the Processing of Personal Data may adversely impact Provider's ability to accurately provide the Services relating to such Personal Data, and Client agrees to hold Provider harmless from any such failure of the Services (the "**Modification Result**").

4. Provider Personnel

Provider will inform its personnel engaged in the Processing of Personal Data ("**Personnel**") of the confidential nature of the Personal Data, provide training to such Personnel on their responsibilities, and require such Personnel to be subject to a contractual or fiduciary duty of confidentiality. Provider will limit access to Personal Data to those Personnel performing Services or exercising rights or fulfilling obligations under the Agreements.

5. Sub-processors

5.1 Appointment of Sub-processors. Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services. Provider has entered into a written agreement with each Sub-processor containing data protection obligations no less protective, in the aggregate, than those in this DPA with respect to the protection of Personal Data.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Provider may use Sub-processors to fulfil its contractual obligations to Client under the Agreements or to provide certain Services or components thereof. Client hereby confirms its general written authorization for Provider's use of the Subprocessors listed at https://www.rithum.com/terms/dpa/subprocessors. Provider shall maintain an up-to-date list of the names and locations of all Sub-Processors used for the Processing of Personal Data under this DPA at such URL or a successor thereto.

5.3 Objection Right for New Sub-processors. Client may object to Provider's use of a new Sub-processor added to Processors list after the Effective Date, by notifying Provider promptly in writing within ten (10) business days after Provider's Sub-processor list has been updated as set out in Section 5.2. If Client timely objects to a new Sub-processor, Provider will use reasonable efforts to make available to Client a change in the Services

or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the applicable new Sub-processor without unreasonably burdening the Client. If the parties are unable to implement such change within a reasonable period of time, which shall not exceed thirty (30) days, Client may terminate the applicable OF(s) or portion thereof with respect only to those Services which cannot be provided by Provider without the use of the applicable new Sub-processor, by providing written notice to Provider. Provider will refund Client any prepaid unused fees covering the remainder of the term of OF(s), following the effective date of termination with respect to such terminated Services.

5.4 Liability. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreements.

6. Security

Provider shall maintain technical and organizational measures ("**TOMs**") designed to protect the security (including protection against unauthorized Processing of Personal Data), confidentiality and integrity of Personal Data, that are consistent with the current TOMs documented in Annex II of Schedule 3 of this DPA. Provider regularly monitors compliance with the TOMs. While Provider may update its TOMs from time to time, Provider will not materially decrease the overall security of the Services during the then-current term.

7. Data Incident Management and Notification

Provider maintains security incident management policies and procedures and shall notify Client without undue delay after becoming aware of the material unauthorized access, use, loss, disclosure or destruction of Personal Data then in the possession, or under the control, of Processor (a "**Data Incident**"). Provider shall make reasonable efforts to identify the cause of and remediate such Data Incident (to the extent remediation is within Provider's reasonable control). The obligations herein shall not apply to Data Incidents that are caused by Client or Client personnel; Client shall bear full responsibility for any such Data Incident.

8. Deletion of Data

Following termination or expiration of the OF(s) and receipt of Client's written election, Provider shall delete all Personal Data then in Provider's possession or control, subject in all cases subject to Provider's data retention policies and the Modification Result. This requirement will not apply to the extent that Provider is required by any applicable contractual or fiduciary obligations, laws (including, without limitation, Data Protection Laws), or financial or tax audit obligations, to retain some or all of the Personal Data, in which case, all Personal Data so retained will remain subject to the protection of this DPA.

9. Authorized Affiliates

9.1 Contractual Relationship. The Client that is the contracting party to the Terms shall remain responsible for coordinating all communication with Provider under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.2 Rights of Authorized Affiliates. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA directly by itself, the parties agree that (i) solely the Client that is the contracting party to the Terms shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Client that is the contracting party to the Terms shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together.

10. Certain Limitations

Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Provider, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Terms, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the

Agreements, together. Notwithstanding the foregoing in this Section 10, nothing in this Section 10 is intended to limit the parties' obligations under Clause 12 of Schedule 3 of this DPA. Notwithstanding anything in the Agreements to the contrary: (i) Provider shall not be prohibited from complying with applicable laws and regulations, including, without limitation, Data Protection Laws; and (ii) the parties understand that the Services require data exchange among Client and the third parties with whom Client is connected through the Services and such activity will not violate this DPA.

11. California-Specific Provisions

In cases where the CCPA governs Processor's Processing of Personal Data in connection with the Services, the following terms will apply: (i) Provider at all times under the Agreements is acting as Client's Service Provider and has been engaged by Client for the Business Purpose of providing the Services detailed in the Terms and OF(s); (ii) Provider will not Sell or Share Personal Data it handles in connection with the Services; (iii) Provider will not retain, use or disclose Personal Data for any purpose other than for the specific Business Purposes authorized by Client. All capitalized terms in the immediately preceding sentence not otherwise defined in this DPA shall have the meaning given such term in the CCPA.

Schedule 1 – Transfer Mechanisms for European Data Transfers

1. Additional Terms

The additional terms in this Section 1 of Schedule 1 shall apply to the Processing of Personal Data of a Client established in (i) European Economic Area member states whose Processing activities for the relevant data are governed by the EU Data Protection Directive 95/46/EC or the GDPR ("**EU Data Protection Legislation**") and/or implementing national legislation; (ii) non-European Economic Area member states for which Client has contractually specified that the EU Data Protection Legislation and implementing national legislation shall apply; and (iii) Switzerland and the United Kingdom.

2. Additional Services Terms

2.1 Clients covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 2 of this Schedule 1 apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Authorized Affiliates of Client established within the European Economic Area, Switzerland and the United Kingdom, which have signed an SOW for the Services. For the purpose of the Standard Contractual Clauses and this Section 2, the aforementioned entities shall be deemed "data exporters".

2.2 Instructions. The Agreements are Client's complete and final documented instructions at the time of signature of the Agreements, to Provider for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Client to process Personal Data: (i) Processing in accordance with the Agreements; (ii) Processing initiated by Client in its use of the Services; and (iii) Processing to comply with other reasonable documented instructions provided by Client or Client personnel (e.g., via email) where such instructions are consistent with the Agreements.

2.3 Mitigation. The measures Provider is required to take under Schedule 3, Clause 8.6(3) will only cover Provider's impacted systems.

2.4 Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (excluding the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

2.5 Swiss Federal Act. In respect to any Restricted Transfer subject to FADP, the terms of Schedule 3 – Standard Contractual Clauses below will apply, with the following modifications:

2.5.1 References to the GDPR shall be interpreted as references to the Swiss Federal Act on Data Protection of June 19, 1992 ("**FADP**") or by any subsequent act, including the relevant amendments and implementing ordinances (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established).

2.5.2 "personal data", "special categories of data/sensitive data", "personality profiles", "profiling" "profiling with high risk", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the meaning assigned to them by the FADP or by any subsequent act, including the relevant amendments and implementing ordinances (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established).

2.5.3 The data importer acknowledges and agrees that the personal data transferred to data importer by data exporter may include personal data of legal persons and personality profiles of natural persons. The data importer shall process personal data of legal persons in the same manner as other personal data and personality profiles in the same manner as special categories of data (the special protection of data from legal persons and from personality profiles will be abolished upon entering into force of the revised Swiss Federal Data Protection Act of September 25, 2020).

2.5.4 "Member State" shall be interpreted as including Switzerland.

2.5.5 The term "Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their habitual place of residence (Switzerland) in accordance with Clause 18c of the FADP or by any subsequent act, including the

relevant amendments and implementing ordinances (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established).

In the event Client transfers Client Personal Data that relates to data subjects in Switzerland to Provider, this Section 2.5 shall modify the corresponding references in this DPA. For clarity and avoidance of doubt, this Section 2.5 will amend this DPA to the extent necessary for compliance with the Swiss Federal Act on Data Protection. This Section 2.5 shall only apply to personal data subject to the Swiss Federal Act on Data Protection.

2.6 In respect of any Restricted Transfer subject to the UK GDPR, the Parties hereby enter into the UK IDTA (with Client as data exporter and Provider as data importer), which is incorporated by reference into this DPA and which shall come into effect upon the commencement of a Restricted Transfer. The Parties make the following selections for the purpose of the UK IDTA:

Part 1: Tables

i. Table 1
   1. The Start Date is the Effective Date of the Terms.
   2. The Exporter is the Client and the Importer is Provider.
   3. The Exporter's details are found in the Terms and OF(s). The Importer is Provider, with principal address at: 1201 Peachtree St NE, Suite 600, Atlanta, GA 30361-3510, USA.
   4. The Exporter's Key Contact is found in the Terms and OF(s). The Importer's Key Contact is Provider's Data Protection Officer, legal@rithum.com.

ii. Table 2: The Parties choose the EEA SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the EEA SCCs brought into effect for the purposes of this IDTA:
   1. Clause 7 – See Schedule 3, Clause 7, below.
   2. Clause 9 – See Schedule 3, Clause 9, below.
   3. Clause 11 – See Schedule 3, Clause 11, below.

iii. Table 3
   1. Annex IA: See Schedule 2 below.
   2. Annex IB: See Schedule 2 below.
   3. Annex II: See Schedule 3, Annex II below.
   4. Annex III: See Schedule 3, Annex III below.

iv. Table 4
   1. The Importer may end this IDTA.

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Schedule 2 – Details of Processing

1. Nature and Purpose of Processing

Provider will Process Personal Data as necessary to perform the Services pursuant to the Agreements and as further instructed by Client in its use of the Services as follows:

1.1 Type of Personal Data Processed. Client may submit (or direct Provider to submit, on Client's behalf) Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First name and surname, phone number, physical or mailing address, email address of buyers of Client's products, and, to the extent applicable, IP addresses of consumers that interact with Client advertising.
- Business contact information (company, first name and surname, phone number, physical or mailing address, email address) of Client's business partners, Client's vendors, and Client's customers.
- Business contact information (company, first name and surname, phone number, physical or mailing address, email address) of (a) Client personnel who are users of this solution; (b) Client personnel who support users of this solution; and (c) agents and advisors of Client.

1.2 Purpose of Processing. Purpose of the Processing:

Personal Data will be processed in order to perform and support the Services in accordance with the Agreement, the OF(s), any statements of work, and this DPA.

1.3 Categories of Data Subjects. Client may submit (or direct Provider to submit, on Client's behalf) Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Client (who are natural persons)
- Employees or contact persons of Client's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Client (who are natural persons)
- Individuals authorized by Client to use the Services
- Buyers of Client's products

2. Duration of Processing

Subject to Section 8 of the DPA, Provider will Process Personal Data for the duration of the Agreements, unless otherwise agreed upon in writing.

Schedule 3 – Standard Contractual Clauses
Controller to Processor Module 2

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') 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 8.1(b), 8.9(a), (c), (d) and (e);
   (iii) Clause 9(a), (c), (d) and (e);
   (iv) Clause 12(a), (d) and (f);
   (v) Clause 13;
   (vi) Clause 15.1(c), (d) and (e);
   (vii) Clause 16(e);
   (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6
Description of the transfer(s)
The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
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.
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 benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

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

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

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

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

8.9 Documentation and compliance

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

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

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

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors
(a) 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. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights
(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress
(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    (ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability
(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision
(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES
Clause 14
Local laws and practices affecting compliance with the Clauses
(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and

proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ();
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

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

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of 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

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as "Client" in the OF(s) to which the DPA is incorporated into or attached or as otherwise specified in the DPA.

Address: The address for Client in the OF(s) to which the DPA is incorporated into or attached or as otherwise specified in the DPA.

Contact person's name, position and contact details: The contact details associated with Client's account in the OF(s) to which the DPA is incorporated into or attached or as otherwise specified in the DPA.

Activities relevant to the data transferred under these Clauses: The activities specified in Schedule 2 to the DPA.

Signature and date: By using the Provider Services to transfer personal data to the data importer in the United States or other Third Country, and by executing the OF(s) with Provider, data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: Provider

Address: 1201 Peachtree Street, NE Building 400, Suite #600, Atlanta, GA 30361, US

Contact person's name, position and contact details: Jason Rodriguez, Deputy General Counsel, legal@rithum.com

Activities relevant to the data transferred under these Clauses: The activities specified in Schedule 2 to the DPA.

Signature and date: By receiving Personal Data from or on behalf of Client in the United States or another Third Country on Clients' instructions, the data importer will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: The categories of data subjects are specified in Schedule 2 to the DPA.

Categories of personal data transferred: The categories of personal data transferred are described in Schedule 2 to the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): The personal data is transferred in accordance with Client's instructions as described in Section 2.3 of the DPA.

Nature of the processing: The nature of the processing is described in Schedule 2 to the DPA:
Purpose(s) of the data transfer and further processing: The purpose of the data transfer and further processing is described in Schedule 2 to the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: All personal data processed for Client may be transferred to Provider's sub-processors for the purpose of performing the Services for Client. These transfers take place on a continuous basis to support Client.

C. COMPETENT SUPERVISORY AUTHORITY

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

Where Client is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Client with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where Client 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 shall act as competent supervisory authority.

Where Client 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 Irish Data Protection Commission shall act as competent supervisory authority.

ANNEX II

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

Provider Technical and Organizational Measures

This document describes the measures taken and implemented by Provider to protect and secure the personal information that we process.

Physical Access Control

Web applications, backend processing systems and database servers (information systems) of Provider are located in secure data centers, distributed across a hosted colocation and Amazon Web Services (AWS) in US and EU Regions. Provider has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where personal data are processed or stored.

This is accomplished by:

- An access control policy that works in coordination with our data center provider policy and procedures;
- Protection of secured cages and cabinets where systems and storage are housed;
- Establishing, approving and maintaining a list of individuals with authorized access to the facility where the information systems resides;
- Under the AWS Shared Responsibility model, AWS inherits all physical and environmental controls for our information systems running in Amazon EC2; and
- Annual review of Data Center SOC reports.

Logical Access Control

Provider has implemented measures to prevent unauthorized access to data processing systems, data in transit and data at rest.

This is accomplished by:

- Established policy and procedures for authorizing and granting access to the network and systems used to process data;
- Multifactor authentication is enforced for access to systems and storage;
- Implementing and maintaining monitoring systems that detect malicious, unauthorized activities within the network and information systems;
- Prohibiting the use of insecure protocols over the management plane;
  Client personal data is encrypted in transit and at rest in the database;
- All data on storage disk arrays is encrypted at rest;
- Periodic review of user permissions and access control lists; and
- Restricting access to information systems based upon the principle of least privilege.

ANNEX III

LIST OF SUB-PROCESSORS
See the list of Provider Sub-processors at:
https://www.rithum.com/terms/dpa/subprocessors