Confidential

Vector AI LTD **trading as Raft**
Registered in England & Wales
Company number: 11063616
55 Southwark Street
London SE1 1EU, UK

DATA PROCESSING ADDENDUM

1. Preamble.

This Data Processing Addendum ("DPA"), forms part of the Software as a Service (SaaS) Agreement (the "SaaS Agreement") between Vector AI LTD trading as Raft ("Company", "Raft") and the entity that has engaged Company to provide the Service (as defined below) ("Customer") and shall be effective as of the date of the applicable SaaS Statement of Work (as defined in the SaaS Agreement). The applicable SaaS Statement of Work(s) together with the Service Terms and Conditions and this Data Processing Agreement are referred to collectively herein as the "SaaS Agreement." This DPA is concluded for the duration of the SaaS Agreement between Company and Customer. Terms used and not otherwise defined herein shall have the meanings ascribed to them in the SaaS Agreement.

2. Definitions

In this DPA, the following terms apply:

Term	**Meaning**
Adequate Country	A country or territory that is recognised under Data Protection Laws as providing adequate protection for processing Personal Data.
Controller, data subject, personal data, personal data breach, process/processing, processor and supervisory authority	Have the same meaning as in the applicable Data Protection Laws

Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data, as amended from time to time, under this DPA, including as applicable: ● The Data Protection Act 2018 ● The United Kingdom General Data Protection Regulation (UK GDPR) ● The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) ● European Union Regulation (EU) 2016/679 (GDPR)
Service	The services provided to Customer by the Company in accordance with the terms of the SaaS Agreement.
Sub-processor	Another processor engaged by the Company to carry out specific processing activities with Personal Data
Transfer Mechanism	The Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), for the transfer of personal data from the EEA or Adequate Country to a third country (Exhibit C), and when applicable, the International Data Transfer Addendum issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022 (Exhibit D).

3. Subject Matter, Nature, Purpose and Duration

3.1 Sections 2 through 6 of this DPA apply to the processing of personal data relating to data subjects located in the European Economic Area or the United Kingdom, or that is otherwise regulated by Data Protection Laws, by the Company solely on behalf of Customer for the purpose of providing the Service ("Personal Data").

3.2 The relationship of the parties is:

(i) Customer is a controller and the Company is a processor on behalf of Customer with regard to Personal Data; or

(ii) Customer is a processor and the Company is a sub-processor on behalf of Customer with regard to EU Personal Data.

3.3 The subject matter and purposes of Personal Data processing, type of Personal Data, categories of data subjects, nature of the Personal Data processing, and Customer's data processing instructions for the Company, are set forth on Exhibit A to this DPA and as otherwise as provided in reasonable written instructions by Customer to the Company from time to time.

3.4 The Customer is responsible for complying with its applicable data protection laws and for assessing whether the use of the Raft Services meets its compliance and contractual obligations.

3.5 This DPA shall remain in effect, and the duration of the processing under this DPA shall continue, as long as the Company carries out Personal Data processing operations on behalf of Customer or until the termination of the SaaS Agreement (and all Personal Data has been returned or deleted in accordance with Section 4(g)).

4. Company Obligations.

4.1 In processing Personal Data hereunder, the Company shall:

(a) process Personal Data only on documented instructions from Customer, unless otherwise required to do so by applicable law, in which case the Company will inform Customer of that legal requirement before processing, unless applicable law prohibits the Company from informing Customer. For the avoidance of doubt, this DPA, along with the SaaS Agreement, shall constitute Customer's documented instructions to the Company to process Personal Data in connection with the Company's provision of the Service to the Customer;

(b) inform the Customer immediately if (in its opinion) any instructions infringe Data Protection Laws;

(c) use commercially reasonable efforts intended to ensure that persons authorized to process Personal Data hereunder have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality or are subject to ethical rules of responsibility that include confidentiality;

(d) taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement commercially reasonable technical and organizational measures when processing Personal Data to ensure a level of security appropriate to the risk involved. This does not limit the Customer's responsibility to safeguard its credential information and any components it has control over, as well as to assess whether its privacy and security obligations are met when using the Raft Services;

(e) taking into account the nature of the processing, use commercially reasonable efforts to assist Customer, at Customer's expense, by appropriate technical and organizational measures, insofar as this is possible, with:

(i) in carrying out any assessment of the consequences or impact of Processing of Personal Data;

(ii) the fulfilment of Customer's obligation to respond to requests for exercising the data subjects' rights with respect to their Personal Data under Data Protection Law; and

(iii) any engagement with the Supervisory Authority

(f) notify the Customer promptly, and provide assistance as required by Data Protection Law, if the Company becomes actually aware of a Personal Data Breach, provided that the provision of such notice by the Company shall not be construed as an acknowledgement of fault or liability with respect to any such Personal Data Breach. In the event the Customer suspects that a potential incident occurred, the Customer shall without undue delay notify the Company;

(g) at the choice of Customer, delete or return all Personal Data to Customer within ninety (90) days after the end of the provision of the Service to Customer and delete existing copies unless applicable law requires retention of Personal Data or the Data has been archived on back-up systems due to Service functionalities, which the Company shall securely protect;

(h) if requested, provide Customer with information necessary to demonstrate its compliance with obligations under Data Protection Law and this DPA;

(i) allow for and contribute to audits (each, an "Audit"), at Customer's expense, including inspections of processing facilities under the Company's control, conducted by Customer or another auditor chosen by Customer (an "Auditor"), provided:

(i) they are conducted during normal business hours;

(ii) are no more frequent than once during any twelve (12) month period;

(ii) the Company is given reasonable prior notice at least eight (8) weeks in advance of the proposed audit date;

(iv) that no Auditor shall be a competitor of the Company;

(v) that in no event shall the Customer have access to the information of any other Customer of the Company;

(vi) the disclosures made pursuant to this Section 4.1(i) ("Audit Information") shall be held in confidence as the Company's Confidential Information and subject to any confidentiality obligations in the SaaS Agreement;

(vii) that no Audit shall be undertaken unless or until Customer has requested, and the Company has provided, documentation pursuant to this Section 4.1(h) and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations laid down in this DPA; and

(viii) that without limiting the generality of any provision in the SaaS Agreement, Customer shall employ the same degree of care to safeguard Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer shall be liable for any improper disclosure or use of Audit Information by Customer or its agents.

(j) The Company will notify the Customer without delay if a Supervisory Authority contacts the Company directly with respect to the processing activities that fall within this DPA.

5. Sub-processors.

5.1 Customer hereby grants the Company general authorisation to engage another processor to process Personal Data on behalf of the Company (each a "sub-processor") to assist the Company in processing Personal Data as set out in this DPA.

5.2 The Company shall enter into contractual arrangements with such sub-processors requiring the same level of data protection compliance and information security as that provided for herein.

5.3 Customer hereby approves to the processing of Personal Data by, and the disclosure and transfer of Personal Data to, the sub-processors listed in Exhibit B to this DPA.

5.4 The Company shall inform Customer of any intended changes concerning the addition or replacement of sub-processors at least ten (10) calendar days before the new sub-processor processes Personal Data.

5.5 Customer may object to such changes in writing within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection (an "Objection"). In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution.

5.6 If the parties are not able to achieve a resolution as described in Section 5.5, the Customer, at its sole and exclusive remedy, may terminate the SaaS Agreement for convenience, on the condition that Customer provides written notice to the Company within five (5) calendar days of being informed of the engagement of the sub-processor.

5.6 Customer shall not be entitled to any refund of fees paid prior to the date of any termination pursuant to this Section 5.

6. Customer Obligations.

Customer represents, warrants, and covenants that:

(a) it shall comply with its obligations as a controller under Data Protection Law in respect of its processing of Personal Data and any processing instructions it issues to the Company as referred to in Section 4.1(a);

(b) it has provided notice and obtained all consents and rights required by the Data Protection Laws to transfer the Personal Data outside the European Economic Area or United Kingdom and for the Company to process Personal Data pursuant to the SaaS Agreement and this DPA; and

(c) the processing of Personal Data by the Company upon the documented instructions of Customer under Section 4.1(a) shall have a lawful basis of processing pursuant to Data Protection Law.

(d) If Customer is a processor, Customer represents and warrants to the Company that Customer's instructions and actions with respect to Personal Data, including its appointment of the Company as another processor, have been duly authorised by the relevant controller.

(e) Customer shall indemnify, defend and hold the Company harmless against any claims, actions, proceedings, expenses, damages and liabilities (including without limitation any governmental investigations, complaints and actions) and reasonable fees arising out of Customer's violation of this Section 6.

(f) Notwithstanding anything to the contrary in the SaaS Agreement, Customer's indemnification obligations under this Section 6 shall not be subject to any limitations of liability set forth in the SaaS Agreement.

7. Data Transfer.

7.1 The Company will only transfer Personal Data to a party outside the UK, the EEA or an adequate country on the documented instructions of the Customer, unless otherwise required to do so by law.

7.2 Where the party is located outside the UK, the EEA or an adequate country and receives Personal Data:

(a) that party will act as the data importer;

(b) the other party is the data exporter; and

(c) the relevant Transfer Mechanism will apply.

7.3 If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Law.

7.4 For avoidance of doubt, the Customer hereby approves to the transfer of Personal Data by the Company to, and the processing of Personal Data in, the United States of America and/or in any other jurisdiction in which Company or its sub-processors have operations as stated in Exhibit B.

7.5 Subject to the terms of the relevant Transfer Mechanism, if the Company receives a request from a public authority to access Personal Data, it will (if legally allowed):

(a) challenge the request and promptly notify the Customer; and

(b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

8. Other Personal Data

8.1 Notwithstanding anything to the contrary in the SaaS Agreement (including this DPA), Customer acknowledges that the Company shall have a right to use and disclose data relating to the operation, support and/or use of the Service for its legitimate business purposes, such as product development and sales and marketing.

8.2 To the extent any such data is considered Personal Data, the Company is the controller of such data and accordingly shall process such data in accordance with Data Protection Law.

9. Integration.

9.1 This DPA, including the relevant Transfer Mechanism and the SaaS Agreement, constitute the parties' entire agreement and understanding with respect to the subject matter hereof.

9.2 Except as set forth in Section 6, the obligations contained in this DPA are:

(a) subject to any limitations of liability set forth in the SaaS Agreement; and

(b) in addition to the other obligations contained in the SaaS Agreement.

9.3 In the event of a conflict between this DPA, the Transfer Mechanism, and any other terms in the SaaS Agreement, they will take priority in this order:

(a) Transfer Mechanism;

(b) DPA;

(c) SaaS Agreement.

9.4 For the avoidance of doubt, to the extent that the SaaS Agreement excludes any types of information from confidentiality obligations, those exclusions shall not apply to information relating to any identified or identifiable natural person.

9.5 This DPA shall be interpreted and construed in accordance with the governing laws and jurisdictions specified in the SaaS Agreement between the parties, unless otherwise provisioned in the applicable data protection laws.

Exhibit A

Subject Matter, Nature, Purpose and Duration of the Processing

1. Type of Personal Data:

Representatives of Customer: Personal data including, but not limited to: First name, last name, title, job title, workplace address, billing address, email address, telephone number(s), password, transaction data, internet protocol address, analytics/audit logging features (logins, file views, modifying data); browser type and version, time zone setting and location, username, account ID, browser plug-in types and versions, operating system and platform and other technology on the devices used to access Raft's software; and

Individuals whose Personal Data is included in files uploaded to the Service by Customer: Any Personal Data included in files uploaded to the Service by Customer and/or its representatives, the extent of which is determined and controlled by Customer in its sole discretion, including but not limited to: First name, last name, contact information, email address.

2. Categories of Data Subject:

Representatives of Customer; Individuals whose Personal Data is included in files uploaded to Company's platform by Customer.

3. Subject Matter and Purposes ofPersonal Data Processing:

Company's provision of the Service to Customer in accordance with the SaaS Agreement.

4. Nature of the Processing:

The Personal Data will be subject to basic processing, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Service by the Company to Customer in accordance with the terms of the SaaS Agreement.

5. Special Categories of Data:

The parties do not anticipate the transfer of special categories of data.

Exhibit B

Sub-processors

1. Name: Atlassian Pty Ltd (Jira, Confluence, Trello)
Service description: software development and project management tools
Address: Atlassian Pty Ltd c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104, United States
Contact person's name, position and contact details: Kelly Gertridge, Head of Privacy, dataprotection@atlassian.com
Signature and accession date: 12th October 2020

2. Name: Data Studio (Google Cloud)
Service description: Data visualisation
Address: Google Ireland Limited, with offices at Gordon House, Barrow Street, Dublin 4, Ireland
Contact person's name, position and contact details: Google Cloud Platform Data Protection Team, https://support.google.com/cloud/contact/dpo, legal-notices@google.com
Signature and accession date: 11th October 2022

3. Name: Functional Software, Inc. d/b/a Sentry
Service description: Application monitoring
Address: 45 Fremont Street, 8th Floor, San Francisco, CA 94105
Contact person's name, position and contact details: legal@sentry.io or https://sentry.io/contact/gdpr/
Signature and accession date: 12th March 2021

4. Name: Google Cloud Provider
Service description: cloud hosting services
Address: Google Ireland Limited, with offices at Gordon House, Barrow Street, Dublin 4, Ireland
Contact person's name, position and contact details: Google Cloud Platform Data Protection Team, https://support.google.com/cloud/contact/dpo, legal-notices@google.com
Signature and accession date: 11th October 2022

5. Name: Holistics Software Pte Ltd
Service description: Business data intelligence
Address: 14 Robinson Road, Far East Finance Building, #08-01A, Singapore 048545
Contact person's name, position and contact details: Thanh Dinh Khac, Chief Engineer, Holistics Software Pte Ltd Email: security@holistics.io, https://www.holistics.io/contact-us/
Signature and accession date: 2nd September 2022

6. Name: SendGrid, Inc.
Service description: email delivery service
Address: 1801 California St., Suite 500, Denver, CO 80202, U.S.A.
Contact person's name, position and contact details: Data processing Officer, dpo@sendgrid.com
Signature and accession date: 1st August 2021

7. Name: UserPilot, Inc.
Service description: product experience platform
Address: 2035 Sunset Lake Road, Newark, Delaware 19702
Contact person's name, position and contact details: Yazan Sehwail, security@userpilot.co
Signature and accession date: October 8th, 2022

Exhibit C

STANDARD CONTRACTUAL CLAUSES

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

On standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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) Clauses 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clauses 9(a), (c), (d) and (e);

(iv) Clauses 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clauses 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 within a reasonable timeframe 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) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

(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 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 [insert EU member state].

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 EU Member State in which the data exporter is established.

(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

to the Standard Contractual Clauses

This Annex I form part of the Clauses and must be completed and signed by the parties. By signing the signature page to the applicable SaaS Agreement, the parties will be deemed to have signed this Annex I.

A. List of Parties

Data exporter	The data exporter is the Service recipient of the data importer, the Customer or its affiliated entities. The contact details are as stated in the SaaS Agreement. The data exporter will act as Controller, and activities relevant to the transfer are as stated in Exhibit A.3 of the DPA.
Data importer	The data importer is the Service provider for data exporter, Raft or Raft's affiliated entities or Sub-processors. The contact details are as that stated in the SaaS Agreement. The data importer will act as Processor, and activities relevant to the transfer are as stated in Exhibit A.3 of the DPA.

B. Description of Transfer

Data subjects. Categories of data subjects whose personal data is transferred	As stated in Exhibit A.2 of the DPA
Personal data. Categories of personal data transferred	As stated in Exhibit A.1 of the DPA
Sensitive data. 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	As stated in Exhibit A.5 of the DPA
Transfer frequency. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	For the duration of the SaaS Agreement OR

	[insert reference to Exhibit A if we add this detail there?]
Nature of the processing	As stated in Exhibit A.4 of the DPA
Purpose of the data transfer and further processing	As stated in Exhibit A.3 of the DPA
Retention period. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	As stated in Section 4(g) of the DPA
Sub-processor transfers.	As stated in Exhibit B of the DPA

C. Competent Supervisory Authority

Supervisory authority. Identify the competent supervisory authority/ies in accordance with Clause 13	[insert agreed supervisory authority]

Annex II

Technical and Organisational Measures

Measures. Technical and organisational measures to ensure the security of the data	As stated in Exhibit E of the DPA

Exhibit D

International Data Transfer Addendum

This Exhibit supplements the Data Processing Addendum entered into between the parties (the DPA) to govern the international transfer of personal data. By signing the SaaS Agreement, to which the DPA is appended, the parties agree to the terms of this Schedule.

PART 1: TABLES

Table 1 - Parties

Start date		
The Parties	**Exporter**	**Importer**
Parties details	As described in Annex I.A of Exhibit C	As described in Annex I.A of Exhibit C
Key contact	As described in Annex I.A of Exhibit C	As described in Annex I.A of Exhibit C

Table 2 - Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed in Exhibit C of the DPA, including the Appendix Information

Table 3 - Appendix Information

Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex I.A	List of Parties: As described in Annex I.A of Exhibit C
Annex I.B	Description of Transfer: As described in Annex I of Exhibit C

Annex II	Technical and organisational measures, including technical and organisational measures to ensure the security of the data: As described in Annex II of Exhibit C
Annex III	List of Sub-processors: As described in Exhibit B of the DPA

Table 4 - Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party

PART 2: MANDATORY CLAUSES

Mandatory Clauses	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.