raft

CONFIDENTIAL

Last modified: December 2024

Raft

Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) **Vector AI Ltd (trading as Raft)**, a company registered in England and Wales with its principal business address at Level 3, 22 Southwark Bridge Road, London SE1 9HB ("**Raft**"); and (2) the entity or other person who is a counterparty to the SaaS Agreement (as defined below) into which this DPA is incorporated and forms a part ("**Customer**"), together the "**Parties**" and each a "**Party**".

1. **INTERPRETATION**

1.1 In this DPA the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Addendum Effective Date**" means the effective date of the first Order Form under the SaaS Agreement.

(b) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data under the SaaS Agreement, including, without limitation, the GDPR (as and where applicable).

(c) "**Controller**" means the entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(d) "**Customer Personal Data**" means any Personal Data Processed by Raft or its Sub-Processor on behalf of Customer to perform the Services under the SaaS Agreement.

(e) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Customer Personal Data and the Processing thereof.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(g) "**EEA**" means the European Economic Area.

(h) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union

(Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(i) "**Order Form**" means any order form (or statement of work, as applicable) entered into between Raft (as service provider) and the Customer (as customer) for the provision of software-as-a-service products for, or relating to, the processing of shipment transactions, or other associated professional services.

(j) "**Personal Data**" means "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws.

(k) "**Personal Data Breach**" means a breach of Raft's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data in Raft's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(l) "**Personnel**" means a person's employees, agents, consultants, contractors, or other staff.

(m) "**Process**" and inflection thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(n) "**Processor**" means the entity that Processes Personal Data on behalf of the Controller.

(o) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Customer Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision

from the European Commission (an "**EU Restricted Transfer**"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(p) "**SaaS Agreement**" means the "Agreement" as defined in the Service Terms and Conditions.

(q) "**Service Terms and Conditions**" means the service terms and conditions identified in the relevant Order Form and applicable to the provision by Raft (as service provider) to the Customer (as customer) of software-as-a-service products for, or relating to, the processing of shipment transactions, or other associated professional services.

(r) "**SCCs**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(s) "**Service Data**" means any data relating to the use, support and/or operation of the Services, which is collected directly by Raft from and/or about users of the Services and/or Customer's use of the Service for use for its own purposes (certain of which may constitute Personal Data).

(t) "**Services**" means those services and activities to be supplied or to be carried out by (or on behalf of) Raft to or for Customer pursuant to the SaaS Agreement.

(u) "**Sub-Processor**" means any third party appointed by or on behalf of Raft to Process Customer Personal Data.

(v) "**Supervisory Authority**" means any entity with the authority to enforce Applicable Data Protection Laws, including, (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office.

(w) "**UK Transfer Addendum**" means 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 the Mandatory Clauses included in Part 2 thereof (the "**Mandatory Clauses**").

1.2 Unless otherwise defined in this DPA, all capitalised terms in this DPA shall have the meaning given to them in the SaaS Agreement.

2. SCOPE OF THIS DATA PROCESSING ADDENDUM

2.1 The body of this DPA applies generally to Raft's Processing of Customer Personal Data under the SaaS Agreement.

2.2 Annex 2 (European Annex) to this DPA applies only if and to the extent Raft's Processing of Customer Personal Data under the SaaS Agreement is subject to the GDPR.

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 Raft shall not Process Customer Personal Data other than on Customer's instructions or as required by applicable laws.

3.2 Customer instructs Raft to Process Customer Personal Data as necessary to provide the Services to Customer under and in accordance with the SaaS Agreement. For the avoidance of doubt, this DPA does not apply to Raft's Processing of Personal Data that does not constitute Customer Personal Data, and/or any other Processing of Personal Data with respect to Customer conducted by Raft as a Controller, including business relationship administration and system security.

3.3 The Parties acknowledge and agree that the details of Raft's Processing of Customer Personal Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 (Data Processing Details) to the DPA.

4. RAFT PERSONNEL

Raft shall take commercially reasonable steps to ascertain the reliability of any Raft Personnel who Process Customer Personal Data, and shall enter into written confidentiality agreements with all Raft Personnel who Process Customer Personal Data that are not subject to professional or statutory obligations of confidentiality.

5. SECURITY

5.1 Raft shall implement and maintain appropriate technical and organisational measures in relation to Customer Personal Data designed to protect Customer Personal Data against Personal Data Breaches as described in Annex 3 (Security Measures) (the "**Security Measures**").

5.2 Raft may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Customer Personal Data.

6. SUB-PROCESSING

6.1 Customer generally authorises Raft to appoint Sub-Processors in accordance with this Section 6. Without limitation to the foregoing, Customer authorises the engagement of the Sub-Processors listed as of the Addendum Effective Date at the URL specified in Section 6.2.

6.2 Information about Raft's Sub-Processors, including their functions and locations, is available at: https://www.raft.ai/raft-documentation-portal in the Data Processing Agreement section (as may be updated by Raft from time-to-time) or such other website address as Raft may provide to Customer from time to time (the "**Sub-Processor Site**").

6.3 When Raft engages any Sub-Processor after the Addendum Effective Date, Raft will notify Customer of the engagement (including the name and location of the relevant Sub-Processor and the activities it will perform) by updating the Sub-Processor Site or by other written means at least thirty (30) days before such Sub-Processor Processes Customer Personal Data. If, within ten (10) days of being notified of such engagement, Customer notifies Raft in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Raft shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and

(b) where: (i) such a change cannot be made within thirty (30) days from Raft's receipt of Customer's notice; (ii) no commercially reasonable change is available; and/or (iii) Customer declines to bear the cost of the proposed change, then either Party may by written notice to the other Party with immediate effect terminate the SaaS Agreement, either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-Processor, as its sole and exclusive remedy.

6.4 If Customer does not object to Raft's appointment of a Sub-Processor during the objection period referred to in Section 6.3, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

6.5 With respect to each Sub-Processor, Raft shall maintain a written contract between Raft and the Sub-Processor that includes terms which offer a level of protection for Customer Personal Data substantially similar to those set out in this DPA (including the Security Measures). Raft shall remain liable for any breach of this DPA caused by a Sub-Processor to the same extent as Raft would have been had Raft performed the Processing itself.

7. DATA SUBJECT RIGHTS

7.1 Raft, taking into account the nature of the Processing of Customer Personal Data, shall provide Customer with such assistance as may be reasonably necessary and technically feasible to assist Customer in fulfilling its obligations to respond to Data Subject Requests. If Raft receives a Data Subject Request, Customer will be responsible for responding to any such request.

7.2 Raft shall:

(a) promptly notify Customer if it receives a Data Subject Request; and

(b) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except on the written instructions of Customer or as required by Applicable Data Protection Laws.

7.3 Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Raft (at Raft's then-current professional services rates) in Raft's cooperation and assistance provided to Customer under this Section 7, and shall on demand reimburse Raft any such costs incurred by Raft.

8. PERSONAL DATA BREACH

Breach notification and assistance

8.1 Raft shall notify Customer without undue delay upon Raft's discovering a Personal Data Breach affecting Customer Personal Data. Raft shall provide Customer with information (insofar as such information is within Raft's possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Raft) to allow Customer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. Raft's notification of or response to a Personal Data Breach shall not be construed as Raft's acknowledgement of any fault or liability with respect to the Personal Data Breach.

8.2 Raft shall reasonably co-operate with Customer and take such commercially reasonable steps as may be directed by Customer to assist in the investigation of any such Personal Data Breach.

8.3 Customer is solely responsible for complying with notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breaches.

Notification to Raft

8.4 If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to

the extent such notice directly or indirectly refers to or identifies Raft, where permitted by applicable laws, Customer agrees to:

(a) notify Raft in advance; and

(b) in good faith, consult with Raft and consider any clarifications or corrections Raft may reasonably recommend or request to any such notification, which: (i) relate to Raft's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

9. **RETURN AND DELETION**

9.1 Subject to Sections 9.2 and 9.3, upon the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), Raft shall promptly cease all Processing of Customer Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA.

9.2 Subject to Sections 9.4 and 9.5, to the extent technically possible in the circumstances (as determined in Raft's sole discretion), on written request to Raft (to be made no later than fourteen (14) days after the Cessation Date ("**Post-cessation Storage Period**")), Raft shall within fourteen (14) days of such request:

(a) return a complete copy of all Customer Personal Data within Raft's possession to Customer by secure file transfer, promptly following which Raft shall delete or irreversibly anonymise all other copies of such Customer Personal Data; or

(b) either (at its option) delete or irreversibly anonymise all Customer Personal Data within Raft's possession.

9.3 In the event that during the Post-cessation Storage Period, Customer does not instruct Raft in writing to either delete or return Customer Personal Data pursuant to Section 9.2, Raft shall promptly after the expiry of the Post-cessation Storage Period either (at its option) delete; or irreversibly render anonymous, all Customer Personal Data then within Raft possession to the fullest extent technically possible in the circumstances.

9.4 To the extent that deletion of any Customer Personal Data contained in any back-ups' maintained by or on behalf of Raft is not technically feasible within the timeframe set out in Customer's instructions, Raft shall:

(a) securely delete such Customer Personal Data in accordance with any relevant scheduled back-up deletion routines (e.g., those contained within Raft's relevant business continuity and disaster recovery procedures); and

(b) pending such deletion, put such Customer Personal Data beyond use.

9.5 Raft may retain Customer Personal Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Raft shall:

(a) maintain the confidentiality of all such Customer Personal Data; and

(b) Process the Customer Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.

10. AUDIT RIGHTS

10.1 Raft shall make available to Customer on request, such information as Raft (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA and Applicable Data Protection Laws.

10.2 Subject to Sections 10.3 to 10.8, in the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Raft pursuant to Section 10.1 is not sufficient in the circumstances to demonstrate Raft's compliance with this DPA, Raft shall allow for and contribute to audits, including on-premise inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by Raft.

10.3 Customer shall give Raft reasonable notice of any audit or inspection to be conducted under Section 10.2 (which shall in no event be less than fourteen (14) days' notice) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Raft's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Raft's other customers or the availability of Raft's services to such other customers).

10.4 Prior to conducting any audit, Customer must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Raft will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information

that could compromise Raft security, privacy, employment or other relevant policies). Raft will work cooperatively with Customer to agree on a final audit plan.

10.5 If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request ("**Audit Report**") and Raft has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

10.6 Raft need not give access to its premises for the purposes of such an audit or inspection:

(a) where an Audit Report is accepted in lieu of such controls or measures in accordance with Section 10.5;

(b) to any individual unless they produce reasonable evidence of their identity;

(c) to any auditor whom Raft has not approved in advance (acting reasonably);

(d) to any individual who has not entered into a non-disclosure agreement with Raft on terms acceptable to Raft;

(e) outside normal business hours at those premises; or

(f) on more than one occasion in any calendar year during the term of the SaaS Agreement, except for any audits or inspections which Customer is required to carry out under Applicable Data Protection Laws or by a Supervisory Authority.

10.7 Nothing in this DPA shall require Raft to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers.

10.8 Nothing in this Section 10 shall be construed to obligate Raft to breach any duty of confidentiality.

10.9 Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Raft (at Raft's then-current professional services rates) in Raft's provision of any cooperation and assistance provided to Customer under this Section 10 (excluding any costs incurred in the procurement, preparation or delivery of Audit Reports to Customer pursuant to Section 10.5), and shall on demand reimburse Raft any such costs incurred by Raft.

11. CUSTOMER'S RESPONSIBILITIES

11.1 Customer agrees that, without limiting Raft's obligations under Section 5 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Raft uses to provide the Services; and (d) backing up Customer Personal Data.

11.2 Customer shall ensure:

(a) that there is, and will be throughout the term of the SaaS Agreement, a valid legal basis for the Processing by Raft of Customer Personal Data in accordance with this DPA and the SaaS Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable)); and

(b) that all Data Subjects have (i) been presented with all required notices and statements (including as required by Article 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Raft of Customer Personal Data.

11.3 Customer agrees that the Service, the Security Measures, and Raft's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Customer Personal Data.

11.4 Customer shall not provide or otherwise make available to Raft any Customer Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) biometric information; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) any payment card information subject to the Payment Card Industry Data Security Standard; (i) Personal Data of children under 13 years of age; or (j) any other information that falls within any special

categories of personal data (as defined in GDPR) and/or data relating to criminal convictions and offences or related security measures (together, "**Restricted Data**").

12. **LIABILITY**

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA and the SCCs (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the SaaS Agreement; **provided that**, nothing in this Section 12 will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the SCCs (if and as they apply).

13. **SERVICE DATA**

13.1 Customer acknowledges that Raft may collect, use and disclose Service Data for its own business purposes, such as:

(a) for accounting, tax, billing, audit, and compliance purposes;

(b) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or

(c) as otherwise permitted or required by applicable law.

13.2 In respect of any such Processing described in Section 13.1, Raft:

(a) independently determines the purposes and means of such Processing;

(b) shall comply with Applicable Data Protection Laws (if and as applicable in the context);

(c) shall Process such Service Data as described in Raft's relevant privacy notices/policies, as updated from time to time; and

(d) where possible, shall apply technical and organisational safeguards to any relevant Personal Data that are no less protective than the Security Measures.

13.3 For the avoidance of doubt, this DPA shall not apply to Raft collection, use, disclosure or other Processing of Service Data, and Service Data does not constitute Customer Personal Data.

14. **CHANGE IN LAWS**

Raft may on notice vary this DPA to the extent that (acting reasonably) it considers necessary to address the requirements of Applicable Data Protection Laws from time to time, including by varying or replacing the SCCs in the manner described in Paragraph 3.3 of Annex 2 (European Annex).

15. **INCORPORATION AND PRECEDENCE**

15.1 This DPA shall be incorporated into and form part of the SaaS Agreement with effect from the Addendum Effective Date.

15.2 In the event of any conflict or inconsistency between:

(a) this DPA and the other terms of the SaaS Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Paragraph 3 of Annex 2 (European Annex) and this DPA and/or the other terms of the SaaS Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1

Data Processing Details

RAFT / 'DATA IMPORTER' DETAILS

Name:	Vector AI Ltd
Address:	As set out in the SaaS Agreement
Contact Details for Data Protection:	The contact person as notified to Customer by Raft from time-to-time
Raft Activities:	Raft provides a Software-as-a-Service platform and connected web-based software applications for the processing of shipment transactions and associated professional services.
Role:	Processor (including sub-processing)

CUSTOMER / 'DATA EXPORTER' DETAILS

Name:	The entity or other person who is a counterparty to the SaaS Agreement
Address:	Customer's address is: ● the address shown in the SaaS Agreement ; or ● if the SaaS Agreement does not include the address, the Customer's principal business trading address
Contact Details for Data Protection:	Customer's contact details are: ● the contact details shown in the SaaS Agreement; or ● if the SaaS Agreement does not include the contact details, Customer's contact details submitted by Customer and associated with Customers account for the Services
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Services under and in accordance with, and for the purposes

	anticipated and permitted in, the SaaS Agreement as part of its ongoing business operations
Role:	● *Controller* – in respect of any Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and ● *Processor* – in respect of any Processing of Customer Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including its affiliates if and where applicable).

DETAILS OF PROCESSING

Categories of Data Subjects:	Relevant Data Subjects include any Data Subjects Customer causes Raft to process as part of the provisions of the Service, including: ● Customer's Personnel ● Customer's own customers Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Relevant Personal Data includes any Categories of Data Customer causes Raft to process as part of the provisions of the Service, including: ● **Personal details** – for example, any information that identifies the Data Subject and their personal characteristics, name, age, date of birth, sex, and physical description. ● **Contact details** – for example, home and/or business address, email address, telephone details and other contact information. ● **Analytics details** - audit logging features (e.g., logins, file views, modifying data); and

	● **Technological details** – for example, internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.
Sensitive Categories of Data, and associated additional restrictions/safeguards:	Categories of sensitive data: None – as noted in Section 11.4 of the DPA, Customer agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the SCCs), must **not** be submitted to the Services. Additional safeguards for sensitive data: N/A
Frequency of transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the SaaS Agreement.
Purpose of the Processing:	Customer Personal Data will be processed: (i) as necessary to provide the Services as initiated by Customer in its use thereof, and (ii) to comply with any other reasonable instructions provided by Customer in accordance with the terms of this DPA.
Duration of Processing / Retention Period:	For the period determined in accordance with the SaaS Agreement and DPA, including Section 9 of the DPA.
Transfers to (sub)processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time on the Sub-Processor Site.

Annex 2

European Annex

1. **PROCESSING OF CUSTOMER PERSONAL DATA**

1.1 Where Raft receives an instruction from Customer that, in its reasonable opinion, infringes the GDPR, Raft shall inform Customer.

1.2 Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing of Customer Personal Data by or on behalf of Raft pursuant to or in connection with the SaaS Agreement shall be in strict compliance with the GDPR and all other applicable laws.

2. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**

2.1 Raft, taking into account the nature of the Processing and the information available to Raft, shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by Raft.

2.2 Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Raft (at Raft's then-current professional services rates) in Raft's provision of any cooperation and assistance provided to Customer under Paragraph 2.1, and shall on demand reimburse Raft any such costs incurred by Raft.

3. **RESTRICTED TRANSFERS**

EU Restricted Transfers

3.1 To the extent that any Processing of Customer Personal Data under this DPA involves an EU Restricted Transfer from Customer to Raft, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be:

(a) populated in accordance with Part 1 of Attachment 1 to Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

UK Restricted Transfers

3.2 To the extent that any Processing of Customer Personal Data under this DPA involves a UK Restricted Transfer from Customer to Raft, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be:

(a) varied to address the requirements of the UK GDPR in accordance with UK Transfer Addendum and populated in accordance with Part 2 of Attachment 1 to Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

Adoption of new transfer mechanism

3.3 Raft may on notice vary this DPA and replace the relevant SCCs with:

(a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or

(b) another transfer mechanism, other than the SCCs,

that enables the lawful transfer of Customer Personal Data to Raft under this DPA in compliance with Chapter V of the GDPR.

Provision of full-form SCCs

3.4 In respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request (made to the contact details set out in Annex 1 (Data Processing Details); accompanied by suitable supporting evidence of the relevant request), Raft shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with Attachment 1 to Annex 2 (European Annex) in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

Operational clarifications

3.5 When complying with its transparency obligations under Clause 8.3 of the SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps

to protect, Raft's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

3.6 Where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Raft to notify any third-party controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

3.7 For the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

3.8 The terms and conditions of Section 6 of the DPA apply in relation to Raft's appointment and use of Sub-Processors under the SCCs. Any approval by Customer of Raft's appointment of a Sub-Processor that is given expressly or deemed given pursuant to that Section 6 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the SCCs.

3.9 The audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in Section 10 of the DPA.

3.10 Certification of deletion of Personal Data as described in Clauses 8.5 and 16(d) of the SCCs shall be provided only upon Customer's written request.

Attachment 1

To Annex 2 (European Annex)

POPULATION OF SCCs

Notes:

- In the context of any EU Restricted Transfer, the SCCs populated in accordance with Part 1 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 3.1 of Annex 2 (European Annex) to the DPA).
- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 3.2 of Annex 2 (European Annex) to the DPA).

PART 1: POPULATION OF THE SCCs

1. **SIGNATURE OF THE SCCs:**

Where the SCCs apply in accordance with Paragraph 3.1 of Annex 2 (European Annex) to the DPA each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. **MODULES**

The following modules of the SCCs apply in the manner set out below (having regard to the role(s) of Customer set out in Attachment 1 to Annex 2 (European Annex) to the DPA):

(a) Module Two of the SCCs applies to any EU Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and/or

(b) Module Three of the SCCs applies to any EU Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person.

3. **POPULATION OF THE BODY OF THE SCCs**

3.1 For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Section 6.3 of the DPA; and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed and all text therein is retained.

(e) In Clause 17:

i. OPTION 1 applies, and the Parties agree that the SCCs shall be governed by the law of Ireland in relation to any EU Restricted Transfer; and

ii. OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the SCCs in relation to any EU Restricted Transfer shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

3.2 In this Paragraph 3, references to "**Clauses**" are references to the Clauses of the SCCs.

4. **POPULATION OF ANNEXES TO THE APPENDIX TO THE SCCs**

4.1 Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 (Data Processing Details) to the DPA, with:

(a) Customer being 'data exporter'; and

(b) Raft being 'data importer'.

4.2 Part C of Annex I to the Appendix to the SCCs is populated as below:

The competent supervisory authority shall be determined as follows:

- Where Customer is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which Customer is established.
- Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which Customer's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies, but Customer has not appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to Raft's contact point for data protection identified in Attachment 1 to Annex 2 (European Annex) to the DPA, which must be an EU Member State 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.

4.3 Annex II to the Appendix to the SCCs is populated as below:

General:

- Please refer to Section 5 of the DPA and Annex 3 (Security Measures) to the DPA.
- In the event that Customer receives a Data Subject Request under the EU GDPR and requires assistance from Raft, Customer should email Raft's contact point for data protection identified in Annex 1 (Data Processing Details) to the DPA.

Sub-Processors: When Raft engages a Sub-Processor under these Clauses, Raft shall enter into a binding contractual arrangement with such Sub-Processor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the DPA – including in respect of:

- applicable information security measures;
- notification of Personal Data Breaches to Raft;
- return or deletion of Customer Personal Data as and where required; and

engagement of further Sub-Processors.

PART 2: UK RESTRICTED TRANSFERS

1. **UK TRANSFER ADDENDUM**

1.1 Where relevant in accordance with Paragraph 3.2 of Annex 2 (European Annex) to the DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below –

(a) *Part 1 to the UK Transfer Addendum*. As permitted by Section 17 of the UK Transfer Addendum, the Parties agree:

(i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Data Processing Details) and the foregoing provisions of this Attachment 1 (subject to the variations effected by the Mandatory Clauses described in (b) below); and

(ii) Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

(b) *Part 2 to the UK Transfer Addendum*. The Parties agreed to be bound by the Mandatory Clauses of the UK Transfer Addendum.

1.2 In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in Paragraph 1.1 of this Part 2.

Annex 3

Security Measures

A description of the technical and organisational security measures implemented by Raft (including any relevant certifications) is located to the following URL: https://raft.ai/raft-documentation-portal (accessed using password: GDPREuropeanParliament1995!).

Raft may update these Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Customer Personal Data.