x

DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) **INSELLIGENCE, LLC**, a Florida limited liability company with its principal business address at 3822 Leafy Way Miami, Florida 33133 ("**Inselligence**"); and (2) the entity or other person who is a counterparty to the Agreement (as defined below) into which this DPA is incorporated and forms a part ("**Client**"), 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 Agreement.

(b) "**Agreement**" means the 'SaaS Subscription Terms of Use Agreement' entered into by and between the Parties.

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

(d) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(e) "**Client Personal Data**" means any Personal Data Processed by Inselligence or its Sub-Processor on behalf of Client to perform the Services under the Agreement.

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

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

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

(j) "**Personal Data Breach**" means a breach of Inselligence's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data

in Inselligence's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Client Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

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

(l) "**Process**" and inflections 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.

(m) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

(n) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Client Personal Data to any person located in: (i) in the context of the EU GDPR, any country or territory outside the European Economic Area ("**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 GDPR, 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.

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

(p) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Inselligence for Client pursuant to the Agreement.

(q) "**Sub-Processor**" means any third party appointed by or on behalf of Inselligence to Process Client Personal Data.

(r) "**Supervisory Authority**": (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.

(s) "**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 UK Mandatory Clauses included in Part 2 thereof (the "**UK 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 Agreement.

x

2. **SCOPE OF THIS DATA PROCESSING ADDENDUM**

2.1 The front-end of this DPA applies generally to Inselligence's Processing of Client Personal Data under the Agreement.

2.2 Annex 1 (European Annex) to this DPA applies only if and to the extent Inselligence's Processing of Client Personal Data under the Agreement is subject to the GDPR.

3. **PROCESSING OF CLIENT PERSONAL DATA**

3.1 Inselligence shall not Process Client Personal Data other than on Client's written instructions or as required by applicable laws.

3.2 Client instructs Inselligence to Process Client Personal Data as necessary to provide the Services to Client under and in accordance with the Agreement. The Agreement is a complete expression of such instructions, and Client's additional instructions will be binding on Inselligence only pursuant to any written amendment to the Agreement and/or this DPA signed by both Parties.

4. **INSELLIGENCE PERSONNEL**

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

5. **SECURITY**

5.1 Inselligence shall implement and maintain those technical and organisational measures in relation to Client Personal Data designed to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access, which are described in Annex 2 (Security Measures) (the "**Security Measures**").

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

6. **DATA SUBJECT RIGHTS**

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

6.2 Inselligence shall:

(a) promptly notify Client 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 Client, except on the written instructions of Client or as required by Applicable Data Protection Laws.

6.3 Operational clarifications:

(a) When complying with its transparency obligations under Clause 8.3 of the SCCs, Client agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, Inselligence's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

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

(c) 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, Client agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

(d) Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Inselligence (at Inselligence's then-current professional services rates) in Inselligence's cooperation and assistance provided to Client under this Section 6, and shall on demand reimburse Inselligence any such costs incurred by Inselligence.

7. **PERSONAL DATA BREACH**

Breach notification and assistance

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

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

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

7.4 Operational clarification: Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Inselligence (at Inselligence's then-current professional services rates) in Inselligence's cooperation and assistance provided to Client under Section 7.2, and shall on demand reimburse Inselligence any such costs incurred by Inselligence.

Notification to Inselligence

7.5 If Client 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 Inselligence, where permitted by applicable laws, Client agrees to:

(a) notify Inselligence in advance; and

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

8. **CLIENT'S RESPONSIBILITIES**

8.1 Client agrees that, without limiting Inselligence's obligations under Section 5 (Security), Client 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 Client Personal Data; (b) securing the account authentication credentials, systems and devices Client uses to access the Services; (c) securing Client's systems and devices that Inselligence uses to provide the Services; and (d) backing up Client Personal Data.

8.2 Client shall ensure:

(a) that there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Inselligence of Client Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Client 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 Inselligence of Client Personal Data.

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

8.4 Client shall not provide or otherwise make available to Inselligence any Client 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**").

9. **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 Agreement; **provided that**, nothing in this Section 9 will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the SCCs (if and as they apply).

10. **CHANGE IN LAWS**

Inselligence 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 6.3 of Annex 1 (European Annex).

11. **INCORPORATION AND PRECEDENCE**

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

11.2 In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Paragraph 6 of Annex 1 (European Annex) and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1

European Annex

1. **PROCESSING OF CLIENT PERSONAL DATA**

1.1 The Parties acknowledge and agree that the details of Inselligence's Processing of Personal Data under this DPA and the Agreement (including the respective roles of the Parties relating to such Processing) are as set out in Attachment 1 to Annex 1 (European Annex) to the DPA.

1.2 Where Inselligence receives an instruction from Client that, in its reasonable opinion, infringes the GDPR, Inselligence shall inform Client.

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

2. **SUB-PROCESSING**

2.1 Client generally authorises Inselligence to appoint Sub-Processors in accordance with this Paragraph 2.

2.2 Inselligence may continue to use those Sub-Processors already engaged by Inselligence as at the date of this DPA (as those Sub-Processors are shown, together with their respective functions and locations, in Annex 3 (Authorised Sub-Processors) (the "**Sub-Processor List**").

2.3 Inselligence shall give Client prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor. If, within fourteen (14) days of receipt of that notice, Client notifies Inselligence in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Inselligence 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 fourteen (14) days from Inselligence's receipt of Client's notice; (ii) no commercially reasonable change is available; and/or (iii) Client 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 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.

2.4 If Client does not object to Inselligence's appointment of a Sub-Processor during the objection period referred to in Paragraph 2.3, Client shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

2.5 With respect to each Sub-Processor, Inselligence shall maintain a written contract between Inselligence and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Client Personal Data as those set out in this DPA (including the Security Measures). Inselligence shall remain liable for any breach of this DPA caused by a Sub-Processor.

2.6 Operational clarifications:

(a) The terms and conditions of this Paragraph 2 apply in relation to Inselligence's appointment and use of Sub-Processors under the SCCs.

(b) Any approval by Client of Inselligence's appointment of a Sub-Processor that is given expressly or deemed given pursuant to this Paragraph 2 constitutes Client'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. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**

3.1 Inselligence, taking into account the nature of the Processing and the information available to Inselligence, shall provide reasonable assistance to Client, at Client's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Client 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 Client Personal Data by Inselligence.

3.2 Operational clarification: Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Inselligence (at Inselligence's then-current professional services rates) in Inselligence's provision of any cooperation and assistance provided to Client under Paragraph 3.1, and shall on demand reimburse Inselligence any such costs incurred by Inselligence.

4. **RETURN AND DELETION**

4.1 Subject to Paragraph 4.2 and 4.3, upon the date of cessation of any Services involving the Processing of Client Personal Data (the "**Cessation Date**"), Inselligence shall promptly cease all Processing of Client Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA.

4.2 Subject to Paragraph 4.4, to the extent technically possible in the circumstances (as determined in Inselligence's sole discretion), on written request to Inselligence (to be made no later than fourteen (14) days after the Cessation Date ("**Post-cessation Storage Period**")), Inselligence shall within thirty (30) days of such request:

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

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

4.3 In the event that during the Post-cessation Storage Period, Client does not instruct Inselligence in writing to either delete or return Client Personal Data pursuant to Paragraph 4.2, Inselligence shall promptly after the expiry of the Post-cessation Storage Period either (at its option) delete; or irreversibly render anonymous, all Client Personal Data then within Inselligence possession to the fullest extent technically possible in the circumstances.

4.4 Inselligence may retain Client Personal Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Inselligence shall:

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

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

4.5 Operational clarification: Certification of deletion of Client Personal Data as described in Clauses 8.5 and 16(d) of the SCCs, shall be provided only upon Client's written request.

5. **AUDIT RIGHTS**

5.1 Inselligence shall make available to Client on request, such information as Inselligence (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

5.2 Subject to Paragraphs 5.3 to 5.8, in the event that Client (acting reasonably) is able to provide documentary evidence that the information made available by Inselligence pursuant to Paragraph 5.1 is not sufficient in the circumstances to demonstrate Inselligence's compliance with this DPA, Inselligence shall allow for and contribute to audits, including on-premise inspections, by Client or an auditor mandated by Client in relation to the Processing of Client Personal Data by Inselligence.

5.3 Client shall give Inselligence reasonable notice of any audit or inspection to be conducted under Paragraph 5.2 (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 Inselligence's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Inselligence's other customers or the availability of Inselligence's services to such other customers).

5.4 Prior to conducting any audit, Client 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. Inselligence will review the proposed audit plan and provide Client with any concerns or questions (for example, any request for information that could compromise Inselligence security, privacy, employment or other relevant policies). Inselligence will work cooperatively with Client to agree on a final audit plan.

5.5 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 Client's audit request ("**Audit Report**") and Inselligence has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Client agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

5.6 Inselligence 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 Paragraph 5.5; (b)to any individual unless they produce reasonable evidence of their identity; (c) to any auditor whom Inselligence has not approved in advance (acting reasonably); (d) to any individual who has not entered into a non-

disclosure agreement with Inselligence on terms acceptable to Inselligence; (e) outside normal business hours at those premises; or (f) on more than one occasion in any calendar year during the term of the Agreement, except for any audits or inspections which Client is required to carry out under the GDPR or by a Supervisory Authority.

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

5.8 Operational clarifications:

(a) Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Inselligence (at Inselligence's then-current professional services rates) in Inselligence's provision of any cooperation and assistance provided to Client under this Paragraph 5 (excluding any costs incurred in the procurement, preparation or delivery of Audit Reports to Client pursuant to Paragraph 5.5), and shall on demand reimburse Inselligence any such costs incurred by Inselligence.

(b) 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 this Paragraph 5.

6. **RESTRICTED TRANSFERS**

EU Restricted Transfers

6.1 To the extent that any Processing of Client Personal Data under this DPA involves an EU Restricted Transfer from Client to Inselligence, 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 2 to Annex 1 (European Annex); and

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

UK Restricted Transfers

6.2 To the extent that any Processing of Client Personal Data under this DPA involves a UK Restricted Transfer from Client to Inselligence, 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 2 to Annex 1 (European Annex); and

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

Adoption of new transfer mechanism

6.3 Inselligence 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; or

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

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

Provision of full-form SCCs

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

[REMAINDER OF PAGE INTENTIONALLY BLANK]

ATTACHMENT 1 TO EUROPEAN ANNEX

Data Processing Details

Note: This Attachment 1 to Annex 1 (European Annex) to the DPA includes certain details of the Processing of Personal Data as required: • by Article 28(3) GDPR; and • to populate the Appendix to the SCCs in the manner described in Attachment 2 to Annex 1 (European Annex) to the DPA.

INSELLIGENCE / 'DATA IMPORTER' DETAILS

Name:	INSELLIGENCE, LLC, a Florida limited liability company
Address:	1644 Tigertail Avenue Miami, Florida 33133
Contact Details for Data Protection:	Name: Juan DeAngulo Role: Co-Founder, Manager and Member Email: jdeangulo@inselligence.io
Inselligence Activities:	Inselligence is a provider of a software-as-a-service solution that can be utilised by Client and its users (under and subject to the Agreement) to manage sales based on forecasts, perform associated data analysis and generate associated insights.
Role:	Processor

CLIENT / 'DATA EXPORTER' DETAILS

Name:	The entity or other person who is a counterparty to the Agreement
Address:	Client's address is: • the address shown in the Agreement; or • if no such address is contained within the Agreement, the Client's principal business trading address – unless otherwise notified to Inselligence's contact point noted above.
Contact Details for Data Protection:	Client's contact details are: • the contact details shown in the Agreement; or • if no such contact details are contained within the Agreement, Client's contact details submitted by Client and associated with Client's account for the Services – unless otherwise notified to Inselligence's contact point noted above.
Client Activities:	Client'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 Agreement as part of its ongoing business operations.
Role:	• Controller – in respect of any Processing of Client Personal Data in respect of which Client is a Controller in its own right; and • Processor – in respect of any Processing of Client Personal Data in respect of which Client 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:	Any individuals whose Personal Data is comprised within data submitted to the Services by or on behalf of Client under the Agreement, which shall depend on the Services selected and used by Client and the nature of any such Service(s). Sales Forecasting and Analytics: This will depend on the 'customer relationship management tooling' with which Client integrates the Services and the configuration of such integration – but may include: • actual and prospective customers, collaborators, licensees, and partners of Client (themselves being natural persons); and • employees, independent contractors, workers, agents and consultants of actual and prospective customers, collaborators, licensees, and partners of Client, (together, "**Client Prospects and Counterparties**"). Continuous Sales Improvement • Client's users authorised by Client to use the Services. • Client's employees, independent contractors, workers, agents and consultants. • Client Prospects and Counterparties. • Any other relevant Data Subjects whose data is included in text fields associated with this Service (e.g., associated with task allocation, action planning and/or status tracking). Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Any Personal Data comprised within data submitted to Services by or on behalf of Client under the Agreement, which shall depend on the Services selected and used by Client and the nature of any such Service(s). Sales Forecasting and Analytics: This will depend on the 'customer relationship management tooling' with which Client integrates the Services and the configuration of such integration – but may include: • **Employment-/engagement-related details** – for example, employer, position, function, job title and primary location for role.

	• **Business Contact details** – for example, business address, business email address, telephone details and other business contact information such as professional social media identifiers/handles. • **Commercial details** – for example, Personal Data relating to goods, services or other intellectual property provided, licensed or sold whether by Client or other parties. <u>Continuous Sales Improvement</u> • **Employment-/engagement-related details** – for example, employer, position, function, job title, primary location for role and performance – together with any other employment-/engagement-related details contained in task allocation, action planning and/or status tracking. • **Business Contact details** – for example, business address, business email address, telephone details and other business contact information such as professional social media identifiers/handles. • **Any other details** – for example, any Personal Data relating to relevant Data Subjects included in text fields (e.g., in task allocation, action planning and/or status tracking).
Sensitive Categories of Data, and associated additional restrictions/safeguards:	<u>Categories of sensitive data:</u> None – as noted in Section 8.4 of the DPA, Client agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the SCCs), must **<u>not</u>** be submitted to the Services. <u>Additional safeguards for sensitive data</u>: N/A.
Frequency of transfer:	Ongoing – as initiated by Client 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 Agreement.
Purpose of the Processing:	Client Personal Data will be processed: (i) as necessary to provide the Services as initiated by Client in its use thereof, and (ii) to comply with any other reasonable instructions provided by Client in accordance with the terms of this DPA.
Duration of Processing / Retention Period:	For the period determined in accordance with the Agreement and DPA, including Paragraph 4 of Annex 1 (European Annex) to the DPA.

Transfers to (sub-)processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with Paragraph 2 of Annex 1 (European Annex) to the DPA).

ATTACHMENT 2 TO 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 2 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 6.1 of Annex 1 (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 2 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 6.2 of Annex 1 (European Annex) to the DPA).

PART 1: POPULATION OF THE SCCs

1. **SIGNATURE OF THE SCCs**

Where the SCCs apply in accordance with Paragraph 6.1 of Annex 1 (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 Client set out in Attachment 1 to Annex 1 (European Annex) to the DPA):

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

(b) Module Three of the SCCs applies to any EU Restricted Transfer involving Processing of Client Personal Data in respect of which Client 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 Paragraph 2.3 of Annex 1 (European Annex) to 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: 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 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**

Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Attachment 1 to Annex 1 (European Annex) to the DPA, with: Client being 'data exporter'; and Inselligence being 'data importer'.

4.1 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 Client is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which Client is established.
- Where Client is not established in an EU Member State, Article 3(2) of the GDPR applies and Client 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 Client's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where Client is not established in an EU Member State, Article 3(2) of the GDPR applies, but Client 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 Inselligence's contact point for data protection identified in Attachment 1 to Annex 1 (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.

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

General:

- Please refer to Section 5 of the DPA and Annex 2 (Security Measures) to the DPA.
- In the event that Client receives a Data Subject Request under the EU GDPR and requires assistance from Inselligence, Client should email Inselligence's contact point for data protection identified in Attachment 1 to Annex 1 (European Annex) to the DPA.

Sub-Processors: When Inselligence engages a Sub-Processor under these Clauses, Inselligence 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 Inselligence;
- return or deletion of Client 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 6.2 of Annex 1 (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*. The Parties agree:

(i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Attachment 1 to Annex 1 (European Annex) to the DPA and the foregoing provisions of this Attachment 2 (subject to the variations effected by the UK 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 agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum.

1.2 As permitted by Section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner set out in Paragraph 1.1 of this Part 2; **provided that** the Parties further agree that nothing in the manner of that presentation shall

operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of the UK Mandatory Clauses).

1.3 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 2

Security Measures

As from the Addendum Effective Date, Inselligence will implement and maintain the Security Measures as set out in this Annex 2.

1. Organisational management and dedicated staff responsible for the development, implementation and maintenance of Inselligence's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Inselligence's organisation, monitoring and maintaining compliance with Inselligence's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Client Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of production resources relevant to the Services is maintained by the relevant Sub-Processor(s) (and their vendors) engaged from time-to-time by Inselligence to host those resources. Inselligence takes steps to ensure that such Sub-Processors provide appropriate assurances and certifications that evidence such physical and environmental security – including security of data center, server room facilities and other areas containing Client Personal Data.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Inselligence's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Inselligence's technology and information assets.

10. Incident management procedures designed to allow Inselligence to investigate, respond to, mitigate and notify of events related to Inselligence's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Inselligence may freely update or modify these Security Measures from time to time **provided that** such updates and modifications do not decrease the overall security of Client Personal Data.

Annex 3

Authorised Sub-Processors

Sub-Processor	Function	Location
Amazon Web Services, Inc.	Hosting services provider for all core functionalities of any platform-based elements of the Services	United States