DATA PROCESSING ADDENDUM

1. GENERAL

1.1. This Data Processing Addendum (the "**DPA**") forms part of the Agreement, between IHQ and the Client which governs the use of the IHQ Product(s) by the Client and becomes effective on the Effective Date.

1.2. In this DPA, references to an annex in Arabic numerals (for example "Annex 1 to this DPA") are references to the annexes to this DPA. References to an annex in Roman numerals (for example "Annex II of the EU Standard Contractual Clauses") are references to the Appendix to the EU Standard Contractual Clauses. The two are distinct and are not to be read interchangeably.

2. PERSONAL DATA PROCESSING

2.1. The Client and IHQ agree and acknowledge that, with regards to the processing of Personal Data, the Client is the Data Controller and IHQ is the Data Processor. The Data Subject is the natural person whose Personal Data is being processed by IHQ, on behalf and under the instructions of the Client.

2.2. Where the Client enables or configures any agentic AI functionality, such configuration constitutes the Client's documented instructions. Processing carried out autonomously by the AI System within the scope of that configuration shall be deemed Processing on behalf of the Client and IHQ shall remain a Data Processor. The Client retains responsibility for determining the purposes of such Processing; for the avoidance of doubt IHQ does not determine the purposes of agentic processing. Notwithstanding the foregoing, the Parties acknowledge that where the AI System Processes Personal Data for a purpose which was not determined by the Client's configuration and which IHQ has not been instructed to carry out, IHQ may be a controller in respect of that Processing by operation of Article 28(10) of the UK GDPR or the EU GDPR. On becoming aware of any such Processing, IHQ shall (i) notify the Client without undue delay in accordance with Clause 8.4, (ii) cease that Processing as soon as reasonably practicable, and (iii) delete any Personal Data Processed for that purpose unless retention is required by applicable law. Nothing in this Clause 2.2 shall be construed as determining the roles of the Parties otherwise than in accordance with the factual circumstances of the Processing.

2.3. The Personal Data will be processed by IHQ on behalf of the Client, following the Client's written instructions, in accordance with the Agreement and the data protection laws that apply to IHQ and with the provisions of this DPA, unless Processing is required by applicable data protection laws to which IHQ may be subject to, in which case IHQ shall, to the extent permitted by the applicable data protection laws, inform the Client of that legal requirement before Processing that Client Personal Data. The Client's activation, configuration and use of any agentic AI functionality (including setting objectives, parameters, permissions, prompts, integrations, or workflows) shall constitute documented instructions for the purposes of this DPA.

2.4. In its use of the Product, the Client shall comply with the requirements contained in the data protection laws that apply to it, including those contained in the UK GDPR, EU GDPR or, if applicable, CCPA. This includes obtaining the necessary consents from the Data Subjects, as well as providing the necessary notices with regards to the use of the Product. Where the Client uses the Product in connection with automated decision-making, including through agentic AI functionality, the Client shall remain responsible for complying with any applicable obligations relating to such processing, including those arising under Article 22 of the EU GDPR, Articles 22A to 22D of the UK GDPR (as applicable), and any applicable transparency requirements under Regulation (EU) 2024/1689 or equivalent legislation.

2.5. Any action or decision taken by the Client with regards to the Processing of Personal Data shall comply with the applicable data protection regulations, including, if applicable, the CCPA, as well as with the terms contained in this DPA.

2.6 IHQ shall immediately inform the Client if, in IHQ's opinion, an instruction given by the Client infringes the UK GDPR, the EU GDPR or any other applicable data protection law. Where IHQ gives such notice, IHQ may suspend performance of the affected instruction until the Client confirms, amends or withdraws it, and IHQ shall not be liable for any delay in or non-performance of the Product to the extent caused by such suspension.

2.7 The Client shall not submit to the Product, and shall not configure the Product to derive or infer, any special category personal data within the meaning of Article 9 of the UK GDPR or the EU GDPR without IHQ's prior written agreement. Where the Parties agree that the Product may Process special category

personal data, the Client shall confirm to IHQ in writing the condition under Article 9(2) on which it relies and, where such data informs a significant decision based solely on automated processing, the condition under Article 22B of the UK GDPR or Article 22(4) of the EU GDPR (as applicable). IHQ shall disable by default any Product segment, feature or attribute which IHQ has identified as capable of revealing special category personal data, and shall enable it only on the Client's written instruction given in accordance with this Clause 2.7.

3. DATA SUBJECT ACCESS REQUESTS

3.1. In the event that IHQ receives a request from a Data Subject seeking to exercise their data protection rights, IHQ will notify the Client without undue delay, and will provide, when possible and necessary, reasonable assistance to the Client to respond to the Data Subject's request. The Client will be solely responsible for responding to any Data Subject requests or communications involving Personal Data.

4. DISCLOSURE OF PERSONAL DATA

4.1. IHQ will not disclose Personal Data to any third party, unless:

4.1.1. It is requested expressly and in writing by the Client;

4.1.2. it is allowed under this DPA;

4.1.3. it is necessary to provide the Product; or

4.1.4. it is required by applicable laws, subject to Clause 4.2.

4.2. If IHQ receives any legally binding request from a public authority, including a judicial or administrative authority, for the disclosure of Personal Data (an "**Order**"), IHQ shall:

4.2.1. notify the Client of the Order promptly and, where possible, before responding to it, unless IHQ is prohibited from doing so by applicable law; where such notification is prohibited, IHQ shall use reasonable efforts to obtain a waiver of the prohibition and shall document those efforts;

4.2.2. review the legality of the Order and challenge it where, on a reasonable assessment, there are grounds to consider it unlawful under the law of the requesting jurisdiction or under applicable international law, including by pursuing available rights of appeal, and seek interim measures to suspend the effect of the Order pending the outcome of that challenge;

4.2.3. disclose only the minimum amount of Personal Data reasonably necessary to respond to the Order; and

4.2.4. document its assessment and the steps taken under this Clause 4.2 and make that documentation available to the Client on request.

Nothing in this Clause 4.2 requires IHQ to act in breach of applicable law. This Clause 4.2 is without prejudice to Clause 15 of the EU Standard Contractual Clauses, which shall prevail in the event of any conflict

5. INTERNATIONAL TRANSFERS

5.1. The Client acknowledges and consents that Personal Data processed by IHQ may be transferred, stored and processed outside the United Kingdom and/or the European Economic Area. IHQ warrants that it will only undertake international transfers in accordance with applicable data protection laws. For transfers to a country or territory in respect of which an Adequacy Decision is in force, no additional safeguards shall apply, provided that where the relevant Adequacy Decision extends only to entities which are certified or otherwise listed under a designated framework, this sentence shall apply only to transfers to entities which are so certified or listed at the time of the transfer. Where IHQ acts as data exporter under the UK GDPR, IHQ shall have regard to whether the standard of protection for data subjects in the destination country is not materially lower than under the UK GDPR.

5.2. For transfers of Personal Data of data subjects originating in the European Union, the European Economic Area and/or its member states, Switzerland, or the United Kingdom, such transfers will be conducted in accordance with the EU Standard Contractual Clauses set out in Annex 1 to this DPA. The EU Standard Contractual Clauses shall only apply in the absence of an applicable Adequacy Decision.

5.3. For transfers of Personal Data of data subjects originating in the United Kingdom, the International Data Transfer Addendum to the EU Standard

DATA PROCESSING ADDENDUM

Contractual Clauses shall apply in addition to the EU Standard Contractual Clauses.

5.4. For transfers of Personal Data originating from Switzerland exclusively subject to the FADP, the provisions of Annex 3 to this DPA (Swiss FADP Supplement) shall apply.

5.5. For Processing of Personal Data subject to the data protection laws of Latin American jurisdictions other than Brazil, the LATAM Data Protection Supplement set out in Annex 4 to this DPA shall apply.

6. SECURITY

6.1. IHQ has implemented appropriate technical and organisational measures against accidental, unauthorised or unlawful Processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data or other improper use.

6.2. IHQ has implemented such measures to ensure a level of security appropriate to the risk involved, including (i) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (ii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iii) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6.3. Where the Product includes AI or agentic functionality, IHQ shall implement reasonable technical and organisational safeguards appropriate to the risks associated with such processing. Such measures may include controls designed to: (i) restrict agentic processing to the scope and purpose configured by the Client; (ii) detect and interrupt anomalous or unexpected agent behaviour; (iii) maintain logs of autonomous agent operations involving Personal Data; (iv) protect against prompt injection, unauthorised data access, or data exfiltration through agent interactions; and (v) prevent the AI System from autonomously determining new or unauthorised purposes for the Processing of Personal Data.

6.4. IHQ shall ensure that any person authorised by IHQ to Process the Personal Data (including IHQ's employees, contractors and agents) is subject to a duty of confidentiality in respect of that Personal Data, whether by way of a written contractual commitment or an appropriate statutory obligation of confidentiality, and that such duty survives the termination of that person's engagement by IHQ.

6.5. IHQ shall ensure that any person acting under its authority who has access to the Personal Data does not Process it except on the Client's documented instructions as given effect by IHQ under this DPA, unless required to do so by applicable law.

7. MINIMUM TECHNICAL AND ORGANISATIONAL MEASURES

7.1. IHQ has security certifications in place, including ISO/IEC 27001, ISO/IEC 27018 and SOC2 Type II. The list of security measures implemented by IHQ includes, but is not limited to, the following:

7.1.1. limiting access to information and systems to authorised users on a need-to-know basis;

7.1.2. limiting physical access to IHQ's information systems and related equipment to authorised individuals;

7.1.3. regular assessments of information security risks to IHQ's information systems and associated information processing activities and of the effectiveness of information security controls in IHQ's information systems;

7.1.4. training of IHQ's employees on information systems regarding the information security risks associated with their activities and applicable laws and policies; and

7.1.5. imposition of formal sanctions for IHQ's employees failing to comply with information security policies and procedures.

8. PERSONAL DATA BREACH NOTIFICATIONS

8.1. IHQ will notify the Client without undue delay in the event of becoming aware of an incident concerning a Personal Data Breach on the Personal Data that IHQ processes on behalf of the Client.

8.2. After becoming aware of a Personal Data Breach, IHQ will investigate it and, if possible, provide the Client with sufficient information about the Personal Data Breach for the Client to comply with the

notification requirements contained in the data protection laws which are applicable to the Client.

8.3. IHQ will take reasonable steps to minimise the negative impacts from happening as a result of the Personal Data Breach. The obligation of IHQ in reporting or responding to a Personal Data Breach will not be construed as an acceptance by IHQ of any liability or fault with regards to the Personal Data Breach.

8.4. In addition to Personal Data Breaches, IHQ shall notify the Client without undue delay where it becomes aware of a material incident involving agentic AI functionality that results in the Processing of Personal Data outside the scope of the Client's configured instructions or operational parameters, where such incident could reasonably impact the security, confidentiality, or lawful Processing of Personal Data.

9. AUDITS

9.1. The Client may conduct a maximum of one audit per calendar year, unless there is a request to the Client by a Supervisory Authority or any other data protection enforcement authority.

9.2. Before the audit is conducted, IHQ and the Client shall agree on the terms applicable to the audit, including, but not limited to, its scope, timing and duration. If IHQ incurs any costs as a consequence of the audit, the Client shall reimburse IHQ of such costs. The audit shall be performed in a way that does not cause any damage, injury or disruption to IHQ.

9.3. IHQ shall make available to the Client all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and in Article 28 of the UK GDPR and the EU GDPR. The Client shall in the first instance seek to satisfy itself of such compliance by means of (i) IHQ's current security certifications together with the most recent summary audit reports issued under them, and (ii) a security questionnaire, which IHQ shall complete and return within thirty (30) days of a reasonable written request. Where the information provided under (i) and (ii) is not reasonably sufficient to demonstrate compliance, or where an audit is required by a Supervisory Authority, or where an audit is reasonably necessary following a Personal Data Breach affecting the Client's Personal Data, the Client (or an independent auditor mandated by the Client, not being a competitor of IHQ and subject to obligations of confidentiality no less onerous than those in the Agreement) may conduct an audit, including an inspection, of IHQ's Processing of the Personal Data, subject to Clauses 9.1 and 9.2.

9.4. Nothing in this DPA shall be interpreted as limiting or affecting any rights of a Supervisory Authority, of a data subject, or of the data exporter under the EU Standard Contractual Clauses, including the data exporter's rights under Clause 8.9 thereof.

10. PERSONAL DATA RECORDS

10.1. IHQ will keep records of the Processing of Personal Data carried out on behalf of the Client. These records will include:

10.1.1. name and contact details of the Client and where applicable, details of the Client's representative or/and data protection officer;

10.1.2. the categories of processing carried out on behalf of the Client; and

10.1.3. international transfers and the basis on which the international transfers are in conformity with the applicable data protection regulations.

11. SUB-PROCESSORS

11.1. Due to the complex and technical nature of the Product, IHQ may from time to time engage third party sub-processors to process Personal Data on its behalf. IHQ shall (1) maintain a list of its Data Sub-Processors in the IHQ Legal Resource Centre (www.intenthq.com/legal), (2) notify the Client in writing, to the contact address specified in the Order Form or such other address as the Client notifies to IHQ in writing, no less than fourteen (14) days before appointing any new Data Sub-Processor or replacing an existing one, (3) impose data protection terms on such Data Sub-Processors which are no less onerous than those set out in this DPA and (4) be liable for any acts or omissions of those Data Sub-Processors as if they were its own. The Client may nominate additional recipients for such notifications by written notice to subprocessornotifications@intenthq.com. The Client may object to any proposed Data Sub-Processor change on legitimate data protection grounds within fourteen (14) days after IHQ's notification under (2), failing which the Client shall be deemed to have accepted the change.

11.2. In the event that the Client objects to a new Data Sub-Processor on legitimate data protection grounds, and IHQ is unable to make enough changes after receiving the Client's written objection, to avoid processing of the Personal Data by the sub-processor for which the Client is Data Controller, the Client may terminate the specific component of the Product subscribed to which cannot be provided without the Processing of the Personal Data by the objected sub-processor.

11.3. Where a sub-processor provides AI or machine learning services in connection with the Processing of Personal Data, IHQ shall ensure that its contract with such sub-processor includes obligations prohibiting the sub-processor from: (i) retaining or using Client Personal Data for its own purposes; and (ii) using Client Personal Data to train, improve, or develop its own artificial intelligence or machine learning models, except as strictly necessary to provide the Product for the Client.

12. DATA PROTECTION IMPACT ASSESSMENT

12.1. IHQ will provide reasonable assistance to the Client, upon request, in ensuring compliance with the obligations deriving from carrying out a data protection impact assessment, when the Client reasonably considers that it is obliged to perform it, and from prior consultation of the Supervisory Authority.

12.2. Where the Client uses the Product in connection with AI or agentic functionality, the Parties acknowledge that the nature of such Processing may initiate obligations under Article 35 GDPR or equivalent laws which would require the Client to conduct a data protection impact assessment. IHQ shall, upon reasonable request, provide information necessary to assist the Client in carrying out such assessments, which may include standard documentation, risk summaries, or templates relating to the relevant AI functionality. IHQ shall also reasonably cooperate with the Client in connection with any data protection impact assessment undertaken in relation to the Client's use of agentic features of the Product.

13. CCPA PROVISIONS

13.1. IHQ is the "Service Provider" and the Client is the "Business", with IHQ considered to be acting at the direction of the Client. Under no circumstances will IHQ sell or share Client Personal Data, as those terms are defined in the CCPA. IHQ will not retain, disclose or use the data disclosed to it by the Client for any other purpose than to provide the services as contained in the Agreement or as otherwise provided in the CCPA.

13.2. IHQ will only retain, use, or disclose Client Personal Data within the context of the direct business relationship with the Client, except where expressly permitted by the CCPA.

13.3. To the extent the Product uses Automated Decision-Making Technology within the meaning of applicable U.S. privacy laws, including the CCPA, IHQ shall process personal information solely on behalf of and at the direction of the Client. IHQ shall provide reasonable assistance to the Client to enable the Client to comply with any applicable obligations relating to opt-out rights or other requirements concerning automated decision-making that replaces or substantially facilitates human decision-making.

13.4. IHQ shall not retain, use, or disclose Client Personal Data for the purpose of training, improving, or developing its own artificial intelligence or machine learning models, except as necessary to provide the Product in accordance with the Agreement.

13.5. IHQ shall not retain, use or disclose the Personal Data for any purpose other than the specific business purposes set out in the Agreement and the applicable Order Form, and shall not retain, use or disclose it outside the direct business relationship between IHQ and the Client, except as expressly permitted by the CCPA.

13.6. IHQ shall not combine the Personal Data it receives from, or on behalf of, the Client with personal information that it receives from, or on behalf of, any other person, or that it collects from its own interaction with a consumer, except where expressly permitted by the CCPA.

13.7. IHQ shall notify the Client promptly, and in any event within five (5) Business Days, if it determines that it can no longer meet its obligations under the CCPA.

13.8. The Client may take reasonable and appropriate steps to (i) ensure that IHQ uses the Personal Data in a manner consistent with the Client's obligations under the CCPA, and (ii) upon notice, stop and

remediate any unauthorised use of the Personal Data.

13.9. IHQ shall comply with the obligations applicable to it under the CCPA and shall provide the same level of privacy protection in respect of the Personal Data as is required of the Client by the CCPA.

14. AUTOMATED DECISION-MAKING

14.1. Where the Client uses the Product in connection with automated decision-making, including through AI or agentic functionality, the Client remains responsible for complying with any applicable requirements under Article 22 of the EU GDPR, Articles 22A to 22D of the UK GDPR, or equivalent laws. IHQ shall, upon reasonable request, provide reasonable assistance to support the Client's compliance with such obligations, including facilitating requests for human intervention or review, providing relevant information about how the Product carries out autonomous processing operations, and supporting the safeguards required by Article 22C of the UK GDPR, namely the provision of information about decisions taken, the ability to make representations, the ability to obtain human intervention, and the ability to contest such decisions.

15. TERMINATION

15.1. This DPA will remain in full force and effect so long as: (i) the Agreement remains in effect; or (ii) IHQ retains any of the Personal Data related to the Agreement in its possession or control.

15.2. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement whenever necessary to protect the Personal Data will remain in full force and effect.

15.3. The Client may, by written notice given within thirty (30) days after the termination or expiry of the Agreement, elect that IHQ either return the Personal Data to the Client or delete it. IHQ shall give effect to that election, and shall delete any existing copies, within thirty (30) days after receipt of the notice. Where the Client makes no election within the said thirty (30) day period, IHQ shall delete the Personal Data within thirty (30) days after the expiry of that period. IHQ shall not charge the Client for return or deletion under this Clause 15.3, save that IHQ may charge its reasonable and pre-notified costs where the Client requests return in a format or medium not supported as standard by the Product. IHQ may retain the Personal Data only to the extent, and for so long as, required by applicable law, in which case IHQ shall (i) inform the Client of that requirement unless legally prohibited from doing so, (ii) continue to protect the Personal Data in accordance with this DPA, and (iii) Process it only to the extent necessary for that legal requirement. The obligations to return, delete and certify under this Clause 15.3 do not extend to Personal Data that resides on end-user terminal equipment and is not within IHQ's direct operational control. In respect of such data, IHQ shall (a) cease any further collection or Processing through its SDK promptly following the applicable deletion deadline, (b) ensure that the SDK is designed to delete or overwrite any locally stored Personal Data upon the next application update or removal of the SDK, and (c) provide the Client, upon request, with reasonable technical documentation describing the residual data and the mechanism for its removal. IHQ shall certify in writing to the Client that it has complied with this Clause 15.3 upon request. For the avoidance of doubt, nothing in this Clause 15.3 curtails the Client's right to extract Client Data under Clause 15.1.4 of the General Terms during the said thirty (30) day period.

15.4. Where the Client accesses the Product under a free trial period and does not convert to a paid subscription, the Agreement and this DPA shall terminate at the end of the trial period. Following such termination, IHQ shall delete or return Personal Data processed in connection with the trial in accordance with Clause 15.3 above, unless retention is required by law.

16. NOTICES

16.1. Unless otherwise stated in this DPA, any notices given to a Party under or in connection with this DPA shall be given in accordance with the notice provisions set out in the Agreement.

17. MISCELLANEOUS

17.1. If there is a conflict between this DPA and any other document forming part of the Agreement in respect of a data protection matter, this DPA shall prevail. The DPA shall not restrict any applicable data protection laws. If any provision of the present DPA is ineffective or void, the remaining provisions of the DPA shall remain in full force and they shall not be affected. The Parties shall replace the ineffective or void provision with a lawful provision that reflects the

DATA PROCESSING ADDENDUM

business purpose of the ineffective or void provision. If a provision is missing in the DPA, the Parties shall with good faith add an appropriate provision. The Agreement remains unchanged and in full force except for changes made by this DPA. Any liability arising out of this DPA as between the Parties is subject to the provisions relating to limitation of liability set out in the Agreement, save that nothing in this DPA or the Agreement shall limit or exclude (i) either Party's liability to a data subject, including under Article 82 of the UK GDPR or the EU GDPR, or (ii) any liability which may not be limited or excluded under the EU Standard Contractual Clauses, the International Data Transfer Addendum or applicable data protection law. This DPA replaces and supersedes all previous written and oral agreements related to the processing of data.

ANNEX 1 TO THE DPA: EU STANDARD CONTRACTUAL CLAUSES

The Parties agree that, to the extent required by the applicable data protection laws and by this DPA, the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU Standard Contractual Clauses**") shall apply and form an integral part of this DPA. The EU Standard Contractual Clauses are hereby incorporated into this Annex 1 to the DPA by reference, including the specific selections found below.

Clause	**Selection**
Clause 8: Data Protection Safeguards	Module Two
Clause 9: Use of sub-processors	Module Two, OPTION 2: General Written Authorisation. Time period for informing about intended changes of fourteen (14) days
Clause 10: Data subject rights	Module Two
Clause 11: Redress	Module Two
Clause 12: Liability	Module Two
Clause 13: Supervision	Module Two
Clause 14: Local laws and practices affecting compliance with the Clauses	Module Two
Clause 15: Obligations of the data importer in case of access by public authorities	Module Two
Clause 16: Non-compliance with the Clauses and termination	Module Two
Clause 17: Governing law	Module Two, OPTION 1. The Parties agree that this shall be the law of Ireland
Clause 18: Choice of forum and jurisdiction	Module Two. The Parties agree that those shall be the courts of Ireland
Appendix	Same as in the EU Standard Contractual Clauses

With respect to Annex I, Part A (List of Parties) of the EU Standard Contractual Clauses: the details of the Parties are set out in Schedule 1 to this DPA.

With respect to Annex I, Part B (Description of Transfer) of the EU Standard Contractual Clauses: the Description of Transfer is set out in Schedule 2 to this DPA.

With respect to Annex I, Part C (Competent Supervisory Authority) of the EU Standard Contractual Clauses: the competent supervisory authority determined in accordance with Clause 13 of the EU Standard Contractual Clauses, as identified in the Order Form or, in the absence of such identification, as notified by the Client to IHQ in writing. Where the Client is established in a Member State of the European Economic Area, the competent supervisory authority shall be the supervisory authority of that Member State.

With respect to Annex II (Technical and Organisational Measures) of the EU Standard Contractual Clauses: the technical and organisational security measures set out in Clauses 6 and 7 of this DPA.

DATA PROCESSING ADDENDUM

With respect to Annex III (List of Sub-Processors) of the EU Standard Contractual Clauses: not applicable, the Parties having selected Option 2 (General Written Authorisation) under Clause 9(a) of the EU Standard Contractual Clauses. For transparency, the agreed list of Data Sub-Processors forming the basis of that general authorisation is maintained at www.intenthq.com/legal in accordance with Clause 11.1 of this DPA.

ANNEX 2 TO THE DPA: INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

The International Data Transfer Addendum to the EU Standard Contractual Clauses is hereby incorporated into this Annex 2 to the DPA by reference, including the specific selections found below.

With respect to Part 1 Tables 1 to 3:

Table 1: the details of the Parties are set out in Schedule 1 of the DPA with the start date being the Effective Date of the Agreement.

Table 2: the version of the EU Standard Contractual Clauses appended to the DPA as Annex 1 to the DPA.

Table 3: the details set out in Schedule 1 and 2 of the DPA and Clauses 6 and 7 and Clause 11 of the DPA.

Table 4: shall be deemed to be completed by selecting neither party.

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

ANNEX 3 TO THE DPA: SUPPLEMENT TO THE EU STANDARD CONTRACTUAL CLAUSES FOR DATA TRANSMISSIONS EXCLUSIVELY SUBJECT TO FADP

The Parties agree that, when the data transmissions are exclusively subject to FADP, the following provisions shall apply in connection to the EU Standard Contractual Clauses:

(a) The term "Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

(b) References to the GDPR are to be understood as references to the FADP.

(c) The Competent Supervisory Authority in Annex I Part C is the Federal Data Protection and Information Commissioner of Switzerland.

ANNEX 4 TO THE DPA: SUPPLEMENT FOR PROCESSING SUBJECT TO LATAM DATA PROTECTION LAWS (EXCLUDING BRAZIL)

This Annex applies where the Processing of Personal Data under the Agreement is subject to the data protection laws of one or more Latin American jurisdictions other than Brazil, including without limitation, Mexico (LFPDPPP), Colombia (Law 1581/2012), Chile (Law 19.628 as amended or replaced from time to time), Argentina (Law 25.326), Uruguay (Law 18.331) and any other applicable Latin American data protection law (collectively "**LATAM Data Protection Laws**"). Processing subject to Brazil's LGPD remains governed exclusively by Annex 5 of this DPA.

(d) Roles of the Parties. The Client shall be deemed the Controller, Responsible Party, or equivalent role under the applicable LATAM Data Protection Law, and IHQ shall act as Processor, Operator, Encargado, or equivalent role. IHQ shall process Personal Data only on documented instructions from the Client.

(e) International Transfers. Where LATAM Data Protection Laws impose restrictions on international transfers, the Parties agree that the EU Standard Contractual Clauses, the UK Addendum, or equivalent contractual safeguards used under this DPA shall be deemed appropriate transfer mechanisms to the extent permitted by the relevant LATAM jurisdiction.

(f) Data Subject Rights. IHQ shall provide reasonable assistance to the Client to enable the Client to respond to Data Subject requests under applicable LATAM Data Protection Laws, including rights of access, rectification, cancellation/deletion, opposition, portability (where applicable), and review of automated decisions.

(g) Automated Decision Making and AI. Where the Client uses the Product in connection with automated decision making or AI functionality, the

DATA PROCESSING ADDENDUM

Client remains responsible for compliance with any obligations relating to such processing under LATAM Data Protection Laws. IHQ shall provide reasonable assistance upon request.

(h) Sub-Processors. IHQ shall ensure that sub-processors engaged in Processing subject to LATAM Data Protection Laws are bound by obligations consistent with this Annex and shall prohibit sub-processors from using Client Personal Data for their own purposes, including training independent AI or machine-learning models.

(i) Precedence. In the event of conflict between this Annex and the DPA, this Annex shall prevail solely for Processing subject to LATAM Data Protection Laws other than Brazil, which remains governed by Clause 15.

ANNEX 5 TO THE DPA: SUPPLEMENT FOR PROCESSING SUBJECT TO THE BRAZILIAN LGPD

This Annex applies where the Processing of Personal Data under the Agreement is subject to Brazilian Federal Law No. 13,709/2018 (the "**LGPD**").

(a) Roles. The Client is the controller (controlador) and IHQ is the operator (operador) within the meaning of Article 5 of the LGPD. IHQ shall Process Personal Data only on the documented instructions of the Client, in accordance with Article 39 of the LGPD.

(b) International transfers. Where Personal Data subject to the LGPD is transferred outside Brazil, such transfer shall be made on the basis of the standard contractual clauses approved by the Autoridade Nacional de Proteção de Dados under Resolution CD/ANPD No. 19 of 23 August 2024 (the "ANPD SCCs"), which are incorporated into this Annex 5 by reference and shall prevail over the EU Standard Contractual Clauses in respect of such transfer. The Parties agree that the ANPD SCCs shall be completed as set out in the Order Form.

(c) Data subject rights. IHQ shall provide reasonable assistance to the Client to enable it to respond to requests under Article 18 of the LGPD.

(d) Security and incidents. IHQ shall notify the Client without undue delay on becoming aware of a security incident affecting Personal Data subject to the LGPD, and shall provide the information reasonably necessary for the Client to comply with Article 48 of the LGPD.

(e) Sub-operators. IHQ shall not engage a sub-operator in respect of Personal Data subject to the LGPD except in accordance with Clause 11 of the DPA, and shall impose obligations consistent with this Annex 5.

(f) Precedence. In the event of conflict between this Annex 5 and the DPA, this Annex 5 shall prevail solely in respect of Processing subject to the LGPD.

ANNEX 6 TO THE DPA: SUPPLEMENT FOR PROCESSING SUBJECT TO NIGERIAN DATA PROTECTION LAW

This Annex applies where the Processing of Personal Data under the Agreement is subject to the Nigeria Data Protection Act 2023 (the "**NDPA**").

(a) Roles. The Client is the data controller and IHQ is the data processor within the meaning of the NDPA. IHQ shall Process Personal Data only on the documented instructions of the Client.

(b) International transfers. Where Personal Data subject to the NDPA is transferred outside Nigeria, such transfer shall be made on the basis of the contractual safeguards permitted under section 41 of the NDPA, and not in reliance on a data subject consent derogation.

(c) Data subject rights, security and breach. IHQ shall provide reasonable assistance to the Client in responding to data subject requests and shall notify the Client without undue delay of any Personal Data Breach, providing the information reasonably necessary for the Client to comply with its notification obligations to the Nigeria Data Protection Commission.

(d) Sub-processors. IHQ shall impose obligations consistent with this Annex 6 on any Data Sub-Processor.

(e) Precedence. In the event of conflict between this Annex 6 and the DPA, this Annex 6 shall prevail solely in respect of Processing subject to the NDPA.

DATA PROCESSING ADDENDUM

SCHEDULE 1: PARTY DETAILS

Role	Party	Contact Details
Data Importer	IHQ	As defined in the IHQ General Terms. FAO Data Processing Officer: legal@intenthq.com.
Data Exporter	Client	As set out in the Order Form which forms part of the Agreement or as otherwise formally communicated to IHQ.

SCHEDULE 2: DESCRIPTION OF TRANSFERS

Description	Lift	Edge	IntentOne
Categories of data subjects	Customer information from the Client's customer relationship management software which the Client requests IHQ to process.	The user of the device which has the SDK installed.	End customer, Client, Engineers, Product Managers.
Categories of personal data transferred	Age, gender, location, weblogs, MSISDNs and any other personal data the Client voluntarily discloses to IHQ under the terms of the Agreement.	Categories of personal data may differ depending on the permissions defined by the Client, and could include unique identifiers, precise location or timing, approximate location, demographics, inference and device partial identifiers.	As specified in the applicable Order Form.
Sensitive data transferred (if applicable) and applied restrictions or safeguards	None. The Client shall not submit special category personal data to the Product without IHQ's prior written agreement (Clause 2.7).	None by default. Segments identified by IHQ as capable of revealing special category personal data are disabled by default and enabled only on the Client's written instruction under Clause 2.7, subject to the following safeguards: access restricted to named personnel on a need-to-know basis; retention limited to the period specified in the "Period for which the personal data will be retained" row of this Table; and logging of enablement and access.	As specified in the applicable Order Form. The Client shall not submit special category personal data without IHQ's prior written agreement (Clause 2.7).
Frequency of the transfer	Continuous	Continuous	Continuous
Nature of the processing and purpose(s) of the data transfer	For the data importer to provide the Product as set out in the Agreement.	For the data importer to provide the Product as set out in the Agreement.	For the data importer to provide the Product as set out in the Agreement.

DATA PROCESSING ADDENDUM

and further processing			
Period for which the personal data will be retained	The Subscription Period.	Ninety (90) days by default, but the Client can decide to delete it at a different frequency, or per request.	The Subscription Period.
For transfers to (sub-processors: subject matter, nature and duration of the processing	Specialist technical support to maintain the Product which the Agreement relates to. Description of processing activity undertaken by each sub-processor is set out within the list of sub-processors. Duration of sub-processing shall be the earlier of (1) the period in which the sub-processor is required to carry out such processing activities or (2) the Subscription Period.	Specialist technical support to maintain the Product which the Agreement relates to. Description of processing activity undertaken by each sub-processor is set out within the list of sub-processors. Duration of sub-processing shall be the earlier of (1) the period in which the sub-processor is required to carry out such processing activities or (2) the Subscription Period.	Specialist technical support to maintain the Product which the Agreement relates to. Description of processing activity undertaken by each sub-processor is set out within the list of sub-processors. Duration of sub-processing shall be the earlier of (1) the period in which the sub-processor is required to carry out such processing activities or (2) the Subscription Period.

SCHEDULE 3: DEFINITIONS

Any capitalised terms not defined herein shall have the meaning set out in the Agreement. The following capitalised terms have the following meanings in this DPA:

Term	Definition
Adequacy Decision	Any country or territory recognised by a relevant regulatory or supervisory authority as providing an adequate level of protection for personal data in accordance with applicable data protection laws, including where the European Commission has adopted an adequacy decision pursuant to Article 45 of the GDPR and/or the Secretary of State has made regulations under Article 45A of the UK GDPR (including regulations made under section 17A of the Data Protection Act 2018 which are treated as made under Article 45A).
AI System	Any system, software, model, tool, or component that performs tasks using machine-based techniques designed to approximate cognitive functions, including (but not limited to) learning, reasoning, prediction, pattern recognition, natural language processing, or decision-making. For the purposes of this DPA, an AI System includes any such technology provided, hosted, operated, or integrated by IHQ that processes Client Data or is used to generate Outputs derived from Client Data.
CCPA	The California Consumer Privacy Act of 2018, as amended (including by the California Privacy Rights Act of 2020), and its implementing regulations.
Data Controller	The entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processor	A natural or legal person, public authority, agency or other body which

DATA PROCESSING ADDENDUM

	processes Personal Data on behalf of the Data Controller.
Data Sub-Processor	A third party engaged by IHQ to assist in the processing of Personal Data in connection to the Agreement.
EU Standard Contractual Clauses	The standard data protection clauses adopted by the European Commission pursuant to Regulation (EU) 2016/679, and adopted by the Implementing Decision (EU) 2021/914, of 4 June 2021.
FADP	The Swiss Federal Act on Data Protection.
International Data Transfer Addendum	The International Data Transfer Addendum to the EU Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner's Office, and in force on 21st March 2022.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Personal Data	Any information relating to the Data Subject.
Processing	Any operation or set of operations which is performed by IHQ on Personal Data or on sets of Personal Data on behalf of the Client under the Agreement, whether or not by automated means, including in the context of the Product and in the course of any Professional Services or support services.
Supervisory Authority	An official body or person responsible for the enforcement of data protection legislation or regulations.
User or Data Subject	An identified or identifiable natural person.

DATA PROCESSING ADDENDUM

SIGNATURE PAGE

Signed on behalf of Intent HQ limited by:	**Signed on behalf of the client by:**
Signed ..... Name ..... Position..... Date	Signed ..... Name ..... Position..... Date .....