Data Processing Addendum
(DPA)

1. General

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

2. Definitions

2.1. 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 Addendum:

Adequacy Decision	Means 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 data protection laws applicable including where European Commission has adopted an adequacy decision pursuant to Article 45 of the GDPR and/or the Government of the United Kingdom determines there is an adequate level of protection in transferring personal data in accordance with Section 17A of the Data Protection Act 2018.
CCPA:	Means the California Consumer Privacy Act, and its implementing regulations.
Data Controller:	Means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processor:	Means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller
Data Sub-Processor:	Means a third party engaged by Intent HQ to assist in the process of Personal Data in connection to the Agreement.
EU Standard Contractual Clauses:	Means the standards data protection clauses adopted by the European Commission pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council, and adopted by the Implementing Decision (EU) 2021/914, of 4 June 2021.
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:	Means 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:	Means any information relating to the Data Subject.
Processing:	Means any operation or set of operations which is performed by IHQ in the context of the Services on Personal Data or on sets of Personal Data, whether or not by automated means.
Supervisory Authority:	Means an official body or person responsible for the enforcement of data protection legislation or regulations.
User or Data Subject:	Means an identified or identifiable natural person.

3. Personal Data Processing

3.1. 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. This Addendum focuses on the processing of Personal Data by IHQ as a part of the provision of the Services. The Data Subject is the natural person whose Personal Data is being processed by IHQ, on behalf and under the instructions of the Client.

3.2. 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 Addendum, 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. It is the responsibility of the Client to ensure that the instructions provided to IHQ comply with all applicable data protection regulations.

3.3. In its use of the Services, 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, among others, obtaining the necessary consents from the Data Subjects, as well as providing the necessary notices with regards to the use of the Services. The Client is responsible for the quality and accuracy of Personal Data, as well as the legality of its means by which the Data Subject's data was acquired by the Client.

3.4. 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 Addendum.

4. Data Subject Access Requests

4.1. 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.

5. Disclosure of Personal Data

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

5.1.1. It is requested expressly and in writing by the Client,
5.1.2. it is allowed under this Addendum,
5.1.3. it is necessary to provide the Services,
5.1.4. it is required by applicable laws.

5.2. In the case that IHQ receives any order from a governmental authority, or any administrative or executive agency, including, but not limited to, judicial or administrative orders which relate to Personal Data (the "Order"), IHQ, to the extent that it is permitted by law, will promptly communicate in writing the Order to the Client. The responsibility for communicating directly with the entity making the Order is solely on the Client. IHQ does not have any responsibility of directly interacting with the entity making the Order.

6. International Transfers

6.1. In order for IHQ to provide the Services to the Client, the Client acknowledges and hereby consents that the personal data processed by IHQ on behalf of the Client may be transferred, stored and processed to locations outside of the United Kingdom and/or the European Economic Area. In any event, IHQ warrants that it will only undertake international transfers in accordance with applicable data protection laws. For the transfers of Personal Data to territories of which an Adequacy Decision has been adopted the transfer shall be treated as if it were in a transfer within the scope of such Adequacy Decision and no additional safeguards shall apply.

6.2. For transfers of Personal Data of data subjects originating in the European Union, the European Economic Area and/or its member states ("EEA"), Switzerland, or the United Kingdom, such transfers will be conducted in accordance with the EU Standard Contractual Clauses set out in Annex I to this Addendum. The EU Standard Contractual Clauses will not govern Personal Data that is not transferred outside the European Union, EEA and/or its member states, Switzerland, or the United Kingdom. The use of the EU Standard Contractual Clauses shall only apply in the absence of an applicable adequacy decision.

6.3. For transfers of Personal Data of data subjects originating in the United Kingdom, the International Data Transfer Addendum to the EU Standard Contractual Clauses shall apply in addition to the EU Standard Contractual Clauses.

6.4. For transfers of Personal Data of data subjects originating in Switzerland, when the data subject is subject to both the FADP and the GDPR, the Option two (2) contained in the chapter 2.3 of the FDPIC "The transfer of personal data to a country without an adequate level of data protection based on standard data protection clauses in accordance with Article 16 paragraph 2 letter d FADP", published on August 27th of 2021, shall apply.

7. Security

7.1. 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.

7.2. 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.

8. Minimum Technical and Organisational Measures

8.1. 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:

8.1.1. limiting access to information/systems to authorised users on a need-to-know basis;

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

8.1.3. 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;

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

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

9. Personal Data Breach Notifications

9.1. 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.

9.2. 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.

9.3. 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.

10. Audits

10.1. 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.

10.2. 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 Intent HQ.

10.3. Notwithstanding 10.1 and 10.2 above, any audit conducted under this Addendum shall be limited to the provision by IHQ of evidence of its current security certifications. Upon reasonable request, IHQ may also if requested by the Client complete and return a security questionnaire provided by the Client.

10.4. Nothing in this Addendum shall be interpreted as limiting or affecting any rights of a Supervisory Authority or data subject under the EU Standard Contractual Clauses.

11. Personal Data Records

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

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

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

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

12. Sub-processors

12.1. Due to the complex and technical nature of the Services, 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 sub-processors in the IHQ Legal Resource Centre (www.intenthq.com/legal) and update such list no less than fourteen (14) days before changing any sub-processor, (2) impose data protection terms on such sub-processors which are no less onerous than those set out in this Addendum and

(3) be liable for any acts or omissions of those sub-processors. Furthermore, the Client may opt in to receive email notifications of any changes to the sub-processor list by submitting a request to subprocessornotifications@intenthq.com. The Client may object to any proposed sub-processor change on legitimate data processing concerns within fourteen (14) days after receiving the notification from Intent HQ, otherwise the Client shall be deemed to have accepted the sub-processor change.

12.2. In the event that the Client objects to this new sub-processor on legitimate data processing concerns, 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 Services subscribed to which cannot be provided without the Processing of the Personal Data by the objected sub-processor.

13. Data Protection Impact Assessment

13.1. 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 is obliged to perform it, and from prior consultation of the Supervisory Authority.

14. CCPA Provisions

14.1. 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 Client's personal data to third parties in return for money or other valuable consideration. 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.

14.2. IHQ will only retain, use, or disclose Client's personal data within the context of the direct business relationship with the Client, except where expressly permitted by the CCPA.

15. Termination

15.1. This Addendum 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 Addendum 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. Within 30 days after the termination of the Agreement, IHQ will delete the Personal Data, unless required by law or to resolve disputes or enforce IHQ's legal agreements and policies, when permitted by law.

16. Notices

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

17. Miscellaneous

17.1. If there is a conflict between this Addendum and any provision of the Agreement, this Addendum shall prevail. The Addendum shall not restrict any applicable data protection laws. If any provision of the present Addendum is ineffective or void, the remaining provisions of the Addendum 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 business purpose of the ineffective or void provision. If a provision is missing in the Addendum, the Parties shall with good faith add an appropriate provision. The Agreement remains unchanged and in full force except for changes made by this Addendum. Any liability arising out of this Addendum is subject to the provisions related to limitation of liability present in the Agreement. This Addendum replaces and supersedes all previous written and oral agreements related to the processing of data.

---------- *END* ----------

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 Addendum, 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 Addendum. The EU Standard Contractual Clauses are hereby incorporated into this Annex I by reference, including the specific selections found below.

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 1 Part A of the EU Standard Contractual Clauses: the details of the Parties are set out in Schedule 1 of the Addendum.

With respect to Annex 1 Part B of the EU Standard Contractual Clauses: the Description of Transfer are set out in Schedule 2 of the Addendum.

With respect to Annex 1 Part C of the EU Standard Contractual Clauses: The Data Protection Commission of Ireland.

With respect to Annex 2 of the EU Standard Contractual Clauses: the technical and organisational security measures set out in Clause 8 of the Addendum.

With respect to Annex 3 of the EU Standard Contractual Clauses: the technical and organisational security measures set out in Clause 12 of the Addendum.

---------- *END* ----------

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 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 Addendum with the start date being the Effective Date of the Agreement.

Table 2 - the version of the EU Standard Contractual Clauses appended to the Addendum as Annex 1.

Table 3- the details set out Schedule 1 and 2 of the DPA and Clause 8 and Clause 12 of the DPA.

Table 4: shall be deemed to 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.

---------- *END* ----------

Annex 3 to the DPA – Supplement to the EU Standard Contractual Clauses for data transmissions exclusively subject to FADP.

1. The Parties agree that, when the data transmissions are exclusively subject to the Federal Act on Data Protection of Switzerland, the following provisions shall apply in connection to the EU Standard Contractual Clauses:

2. 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).

3. References to the GDPR are to be understood as references to the FADP.

4. The Competent Supervisory Authority in Annex 1 Part C is the Federal Data Protection and Information Commissioner of Switzerland.

---------- *END* ----------

Schedule 1 – Party Details

Role	Party	Contact Details
Data Importer	IHQ	As set defined in the Intent HQ Service 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.

---------- *END* ----------

Schedule 2 – Description of Transfers

Description	Lift Services	Edge Services
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.
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
The frequency of the transfer	Continuous	
Nature of the processing and Purpose(s) of the data transfer and further processing	For the data importer to provide the services as set out in the Agreement.	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	The Subscription Period	90 days by default, but the Client can decide to delete it at a different frequency, or per request
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Specialist technical support to maintain the Services which the Agreement relates to. Description of what processing activity is undertaken by each sub-processor is set out within the list of sub-processors. Such duration of the sub-processing shall be earlier of 1) the period in which the subprocessor is required to carry out such processing activities or 2) the Subscription Period.	