INCOMPASS LABS DATA PROCESSING AGREEMENT

This Data Processing Agreement between Customer and Incompass Labs, Inc:

By agreeing to Incompass Labs' Terms of Service, Customer also accepts without modification of the terms, conditions, and notices contained herein (the "Terms"). Your use of www.incompass.io constitutes your agreement to all such Terms. Please read these carefully and keep a copy of them for your reference.

WHEREAS

(A) The Parties acknowledge that the provision of the services by using www.incompass.io may require Supplier to process personal data on behalf of Customer.

(B) In light of the above the Parties agree to enter into this DPA to specify the terms and conditions on which such processing may take place.

NOW, THEREFORE, IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions.

o "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, including all laws and regulations implementing or supplementing the CCPA and successor or modifying legislation.

o "**Customer Personal Data**" means any personal data which is processed by Supplier on behalf of Customer under the Main Agreement.

o "**data controller**", "**data subject**", "**personal data**", "**processing**" ("**process**" and "**processed**" to be construed accordingly), "**data processor**" and "**appropriate technical and organizational measures**" have the meanings given to them in the Data Protection Legislation. For the purposes of this DPA, "personal data" shall only be personal data that is processed in connection with the Main Agreement.

o "**Data Protection Legislation**" means, as applicable: (a) the EU GDPR; (b) the UK GDPR; (c) the CCPA; (d) any other data protection and privacy laws which apply to the processing of Customer Personal Data by Supplier, whether international, foreign, national, state, and/or local in the United States of America, European Union or United Kingdom; and (e) any amendments or successor legislation to (a) to (d).

o "**EU GDPR**" means the General Data Protection Regulation ((EU) 2016/679).

o "**EU SCCs**" means module 2 of the standard contractual clauses approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021, which is incorporated herein by reference.

o "**Standard Contractual Clauses**" means the EU SCCs including the UK Addendum;

o **"Third Country"** means a country which the EU Commission or the UK Government (as applicable) has not designated as a country that provides adequate protections in respect of Personal Data.

o "**UK GDPR**" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

o "**UK Addendum**" means the UK Information Commissioner's international data transfer addendum to the EU SCCs issued under section 119A of the Data Protection Act 2018 and which entered into force on 21 March 2022, which is incorporated herein by reference.

1.2 Interpretation. The Parties agree that: (a) unless the context requires otherwise: (i) "including" (and any of its derivative forms) means including but not limited to; (ii) "may" means has the right, but not the obligation to do something and "may not" means does not have the right to do something; (iii) "will" and "shall" are expressions of command, not merely expressions of future intent or expectation; (iv) "written" or "in writing" includes email, unless otherwise stated; (v) use of the singular imports the plural and vice versa; and (vi) use of a specific gender imports the other gender(s)'; (b) a reference to a statute or statutory provision: (i) is a reference to it as amended, extended or re-enacted from time to time; and (ii) shall include all subordinate legislation made from time to time under that statute or statutory provision; and (c) the captions and headings used in the DPA are used for convenience only and are not to be given any legal effect.

2. SCOPE, STATUS OF THE PARTIES AND TERM

2.1 This DPA shall apply to the Parties whenever Customer Personal Data is processed by Supplier pursuant to the Main Agreement.

2.2 In respect of the processing of Customer Personal Data under this DPA, Customer acts as data controller in respect to Customer Personal

Data and Supplier acts as a data processor on behalf of Customer.

2.3 Details of the applicable processing activities (including categories of personal data and data subjects) are described in Schedule 1 to this DPA.

2.4 This DPA shall commence on the DPA Effective Date and shall remain in force until expiry or termination of the Main Agreement.

3. CUSTOMER'S OBLIGATIONS

3.1 Customer warrants, represents and undertakes to Supplier that:

3.1.1 it will comply at all times with the Data Protection Legislation; and

3.1.2 all necessary consents and notices are in place to enable the lawful transfer (including international transfers) of Customer Personal Data to Supplier for the duration of the required processing (including without limitation, lawful grounds for processing).

4. SUPPLIER'S OBLIGATIONS

4.1 Where Supplier processes Customer Personal Data under or in connection with the performance of its obligations under the Main Agreement, Supplier shall:

4.1.1 process the Customer Personal Data only in accordance with Main Agreement and with other mutually agreed and documented instructions of Customer (including in relation to any international transfer of Customer Personal Data made in accordance with Section 6 of this DPA), unless applicable Data Protection Legislation requires Supplier to otherwise process such Customer Personal Data;

4.1.2 implement appropriate technical and organizational measures (TOMs), which as at the DPA Effective Date shall be those TOMs set out in Schedule 2 of this DPA. Supplier shall be permitted to update its TOMs from time to time, provided that it provides a copy of the updated TOMs to Customer and any changes do not adversely affect the level of security provided by Supplier in respect of the Customer Personal Data. Customer acknowledges and agrees that Supplier's TOMs are appropriate and sufficient taking into account the nature and scope of the Personal Data and processing activities under this DPA and that they meet the requirements of the Data Protection Legislation;

4.1.3 ensure Supplier personnel authorized to process Customer Personal Data are subject to appropriate confidentiality obligations;

4.1.4 taking into account the nature of the processing and the information available to Supplier, reasonably assist Customer to fulfil Customer's obligations under Data Protection Legislation:

(a) to respond to data subjects' requests exercising their rights; and

(b) with respect to security, data protection impact assessments, data breach notifications and consultations with data protection supervisory authorities;

4.1.5 save as required by applicable law, at Customer's option (provided in writing), either delete or return Customer Personal Data in Supplier's possession to Customer within a reasonable period of time following expiry or termination of the Main Agreement;

4.1.6 notify Customer without undue delay after becoming aware of any personal data breach involving Customer Personal Data; and

4.1.7 make available to Customer, or an auditor mandated by Customer, written information reasonably necessary to assess or demonstrate Supplier's (and its sub-processors') compliance with the Data Protection Legislation with respect to the processing of Personal Data pursuant to this DPA, which shall be completed by written questionnaire to the extent commercially practicable. If an on-site audit or inspection is expressly required under the Standard Contractual Clauses or otherwise by Data Protection Legislation or by the applicable Supervisory Authority with respect to the processing of Personal Data pursuant to this DPA, Customer shall submit an advanced written request with respect thereto (unless prohibited from doing so by the Data Protection Legislation), and after the Parties have agreed on the start date, scope and duration of, and security and confidentiality controls applicable to, such audit or inspection, Supplier shall allow and contribute to such audit or inspection, provided that:

(a) Customer shall: (i) give Supplier reasonable advance written notice of such audit or inspection to be conducted; and (ii) use (and ensure that each of its mandated auditors use) commercially reasonable efforts to: (A) avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the applicable premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection; and (B) conduct the audit or inspection during normal business hours; and

(b) notwithstanding anything to the contrary: (i) Supplier shall only be required to grant access to physical locations or provide documentation to the extent that it controls such facilities or documentation or has the right to grant access thereto under its contracts with the relevant sub-processor (which Supplier shall use commercially reasonable efforts to facilitate); (ii) in no event shall Supplier be contractually required to permit any audit or other activity that may compromise, jeopardize or otherwise adversely impact the security, confidentiality, operability or integrity of services that Supplier provides to other customers or disclose any internal accounting or financial information or trade secrets of Supplier.

4.2 Supplier shall be entitled to charge Customer, at Supplier's then-current rate card for any Supplier effort or costs incurred in complying with the requirements of Sections 4.1.4 to 4.1.7 (inclusive), except in respect of audit assistance where any such audit or inspection is required due to a material breach by Supplier of its obligations under this DPA or such audit reveals such a material breach.

5. SUB-PROCESSORS

5.1 Supplier shall be generally permitted to engage sub-processors to process Customer Personal Data solely as necessary in order for Supplier to comply with its obligations under the Main Agreement. Customer may request a then current list of Supplier's sub-processors on reasonable notice from time to time.

5.2 Supplier shall, in relation to all of its sub-processors processing Customer Personal Data:

5.2.1 ensure that, to the extent required by the Data Protection Legislation, equivalent requirements to those set out in this DPA are imposed on the sub-processors through a written agreement;

5.2.2 remain liable to Customer for the performance of the sub-processor's obligations; and

5.2.3 notify Customer of any change or addition to such sub-processors in order to provide Customer with the opportunity to object (which must be within 14 days and on reasonable grounds relating to security concerns or breach of the Data Protection Legislation in respect of the use of such sub-processor). If Customer objects to a sub-processor in accordance with this Section 5.2.3, Supplier will make commercially reasonable efforts to provide Customer with the same level of service described in the Main Agreement, without using the sub-processor to process the Customer Personal Data. If Supplier's efforts are not successful within a reasonable time, Customer shall, as its sole right in such circumstances, have the right to terminate the applicable service(s) under the Main Agreement immediately on written notice to Supplier and without consequence (other than payment of any outstanding fees due for such service(s)).

6. INTERNATIONAL TRANSFERS

6.1 Onward Transfers by Supplier. Supplier may transfer Customer Personal Data to any country or territory (including Third Countries) provided that Supplier ensures that any Customer Personal Data that is subject to such transfers is provided an adequate level of protection, including the use of:

6.1.1 appropriate technical and organizational measures; and

6.1.2 appropriate safeguards or derogations under Data Protection Legislation,

- and that, in any event, such transfer is effected in compliance with the applicable Data Protection Legislation.

6.2 International Transfers between the Parties. In respect of any transfers of Customer Personal Data by Customer from the European Economic Area or UK to Supplier in a Third Country, the Parties agree that the Standard Contractual Clauses shall apply, which are deemed executed by the Parties on execution of this DPA, as follows:

6.2.1 EU SCCs Clause 7: This optional clause shall not apply.

6.2.2 EU SCCs Clause 9: Option 2 shall apply subject to the provisions of Section 5 (Sub-processors) of this DPA.

6.2.3 EU SCCs Clause 11(a): The optional paragraph shall not apply.

6.2.4 EU SCCs Clause 17: Option 1 shall apply and the governing law shall be the law of Ireland.

6.2.5 EU SCCs Clause 18(b): The applicable forum shall be the courts of Ireland.

6.2.6 EU SCCs Annex I: The details for this annex are set out in Schedule 1 of this DPA, with the Irish Data Protection Commission being the competent authority and Supplier as importer and Customer as exporter.

6.2.7 EU SCCs Annex II: The details for this annex are set out in Schedule 2 of this DPA.

6.2.8 EU SCCs Annex III: The details for this annex are set out in Schedule 1 of this DPA.

6.2.9 UK Addendum Table 1 – Start Date is the DPA Effective Date and the rest of the details are set out in Schedule 1 of this DPA.

6.2.10 UK Addendum Tables 2 and 3 – Refer to the EU SCCs as incorporated herein with start date is the DPA Effective Date.

6.2.11 UK Addendum Table 4 – Neither Party.

7. CCPA

7.1 The Parties hereby agree that: (a) the terms and conditions set forth in this Section 7 apply where the CCPA is the governing Data Protection Legislation that applies to the Customer Personal Data being processed by Supplier under this DPA; and (b) Customer shall be the "business" and Supplier shall be the "Service Provider" as defined in the CCPA.

7.2 Customer shall disclose Customer Personal Data to Supplier solely for:

7.2.1 a valid business purpose (as defined in the CCPA); and

7.2.2 Supplier to perform its obligations under the Main Agreement.

7.3 Subject to Section 7.4, Supplier is prohibited from:

7.3.1 selling or sharing (as defined in the CCPA) the Customer Personal Data;

7.3.2 retaining, using, or disclosing Customer Personal Data for a commercial purpose other than performing its obligations under the Main Agreement and not outside of the business relationship between Customer and Supplier;

7.3.3 retaining, using, or disclosing the Customer Personal Data outside of the Main Agreement; and

7.3.4 combining Customer Personal Data received from Customer with personal data that Supplier receives from, or on behalf of, another person or company, except as permitted by the CCPA,

o Supplier hereby acknowledges that it understands the prohibitions outlined in this Section 7.3.

7.4 Section 7.3 shall not restrict Supplier's:

7.4.1 use of sub-contractors and sub-processors in accordance with the Main Agreement and this DPA; or

7.4.2 use of the Customer Personal Data to:

(a) build or improve the quality of the services it provides to Customer, provided that the use does not include use of Customer Personal Data to perform services on behalf of another person;

(b) detect data security incidents or protect against malicious, deceptive, fraudulent or illegal activity;

(c) comply with federal, state, or local laws or comply with a court order or subpoena to provide information;

(d) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;

(e) cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate federal, state, or local law;

(f) cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury;

(g) exercise or defend legal claims;

(h) collect, use, retail, sell, share or disclose consumers' personal information that is deidentified or aggregate consumer information; or

(i) without prejudice to the other Sections of this DPA, collect, sell or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California.

1.2 Supplier shall promptly notify Customer if it determines it can no longer meet its obligations under the CCPA.

2. LIABILITY

2.1 Each Party's liability under this DPA shall be governed by the liability provisions (including limitations and exclusions of liability) set out in the Main Agreement.

3. INDEMNITY

3.1 Subject to Section 8.1, each Party shall indemnify and keep indemnified the other Party against any liability, fines, claims, demands, expenses and costs (including reasonable legal fees) incurred by the other arising out of or in connection with with any third party claim in connection with any breach by the other Party of its obligations under the Data Protection Legislation.

4. GOVERNING LAW AND JURISDICTION

4.1 Without prejudice to the governing law and jurisdictions of the Standard Contractual Clauses, this DPA and the relationship of the Parties under it shall be governed and construed by the laws of the jurisdiction specified in the Main Agreement.

4.2 The courts specified in the Main Agreement shall have exclusive jurisdiction over all suits and proceedings arising out of or in connection with this DPA. Both Parties hereby submit to the jurisdiction of such courts for the purposes of any such suit or proceeding and irrevocably waive any claim that such forum is inconvenient or inappropriate.

4.3 Before the Parties resort to litigation to solve any dispute, the Parties will enter into good faith negotiations in an attempt to resolve the dispute. Nothing in this Section 10.3 shall prevent Supplier from seeking any interim or interlocutory relief.

4.4 EACH PARTY IRREVOCABLY WAIVES ANY RIGHT TO TRIAL BY JURY IN CONNECTION WITH ANY ACTION, SUIT OR PROCEEDING ARISING OUT OF OR RELATING TO THIS DPA.

5. GENERAL

5.1 Status of Parties. Nothing in this DPA is intended to, or shall be deemed to, make Supplier and Customer partners, joint venturers or otherwise associated in or with the business of the other. Neither Party is authorized to incur debts or other obligations of any kind on the part of or as agent for the other, or to make or enter into any commitments for or on behalf of the other Party.

5.2 Assignment and Transfers. Either Party may only assign or transfer this DPA in connection with a permitted assignment or transfer of the Main Agreement.

5.3 Variation. No variation of this DPA shall be effective unless it is in writing and signed by the duly authorized representatives of both Parties.

5.4 Notices. All notices and other communications required or permitted hereunder must be in writing and sent to the addresses or email addresses set out in above and will be deemed to have been duly given: (a) when delivered by hand with a copy provided by another means specified in this Section 11.4: (i) one (1) day after delivery by receipted overnight delivery; or (ii) three (3) days after being posted by certified or registered post, proof of postage requested, with postage prepaid to the Party at the address set forth above, or to such address as either Party shall furnish to the other Party in writing, pursuant to this Section 11.4; or (b) where delivered by email, at the time of receipt. The Parties agree that notice via email is not valid for notices related to legal proceedings and that this Section is subject to any specific notice requirements or timings that apply to legal proceeding notices in the applicable jurisdiction.

5.5 Waiver. No waiver of any of the provisions of this DPA shall constitute a waiver of any other provision of this DPA, nor shall such waiver constitute a continuing waiver. The failure of either Party to enforce at any time any of the provisions of this DPA, or the failure of either Party to require the performance by the other Party of any provisions of this DPA, shall not be construed as a waiver of such provisions in the future, nor will it affect the ability of a Party to enforce each and every provision thereafter.

5.6 Further Assurance. Each Party will do and execute, or arrange for the doing or executing of, each necessary act, document and thing that is reasonably necessary to give effect to any of the Parties' rights under this DPA.

5.7 Cumulative Remedies. Except as expressly provided in this DPA, all rights, remedies and powers of the Parties hereunder are irrevocable and cumulative, and not alternative or exclusive, and shall be in addition to all other rights, remedies and powers to which it may be entitled by applicable law.

5.8 Entire Agreement. This DPA and the Main Agreement constitute the entire agreement between the Parties with respect to their subject matter and supersede all prior and contemporaneous communications, understandings, and agreements concerning the subject matter hereof and thereof, whether written or oral. Each Party agrees that in entering into this DPA it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this DPA. Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this DPA.

5.9 Conflict. In the event of a conflict or inconsistency between the provisions of this DPA and the Main Agreement, then to the extent that the conflict or inconsistency relates to the processing of Customer Personal Data, the provisions of this DPA shall take precedence and in all other circumstances the provisions of the Main Agreement shall take precedence.

5.10 Counterparts. Unless prohibited pursuant to applicable law (in which case the necessary formalities required by such applicable law shall be followed), this DPA may be executed in separate counterparts, including by electronic or digital signature, and by the different Parties on the same or separate counterparts. Any signed copy of this DPA made by reliable means will be considered an original, and all signed counterparts will constitute one and the same instrument.

5.11 Invalidity. If any provision or part provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but shall not affect the validity and enforceability of the other provisions of this DPA. If any provision or part provision of this DPA is deemed deleted under this Section the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

5.12 Survival. Any term or condition of this DPA which expressly or by implication is required for the interpretation of this DPA or necessary for the full observation and performance by each Party of all rights and obligations arising prior to the date of expiration shall survive the expiration or termination of this DPA.

5.13 No Third Party Rights. Without prejudice to the rights of data subject under Data Protection Legislation and the Standard Contractual Clauses, this DPA is entered into solely by and between Supplier and Customer and will not be deemed to create any rights in any third parties (whether under applicable law (which the parties hereby exclude to the fullest extent permitted) or otherwise).

SCHEDULE 1

PERSONAL DATA AND PROCESSING ACTIVITY

The Parties agree that, as applicable, the following personal data processing activities shall apply. Additional or amended processing activities may be specified in the applicable Main Agreement.

Subject matter of the processing	The subject matter of the processing under the applicable Main Agreement is Customer Personal Data collected by Supplier on behalf of, or submitted to Supplier by, Customer or a third party on Customer's behalf in accordance with the applicable Main Agreement.
Duration of the processing	The term of the Main Agreement to which the processing of Customer Personal Data relates, plus any period of retention specified in the applicable Main Agreement or required by applicable law. For the avoidance of doubt, where a data subject's account has been deactivated or soft-deleted by Customer (e.g., following the departure of an employee from Customer's organization), Supplier shall continue to retain and process such data subject's Customer Personal Data for the duration of the Main Agreement, unless Customer instructs Supplier otherwise in writing.
Nature and purpose of the processing	The nature of processing is the way in which the Customer Personal Data shall be processed in accordance with the services being provided under the applicable Main Agreement. The purpose of the processing is Supplier's performance of its obligations under the applicable Main Agreement.
Type of personal data processed	Types of personal may include: ● Name ● Names of managers ● Email Address ● Job title ● Job level ● Job tenure ● Team ● Division ● Gender ● Ethnicity ● Geographic Location
Categories of data subjects	Data subjects may include: ● Customer's personnel
Obligations and rights of Customer	The obligations and rights of Customer are set out in the applicable Main Agreement and this DPA.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

1. The Supplier shall ensure that appropriate technical and organizational measures are in place to protect the Customer Personal Data, such measures shall include the following:

1.1. Encryption and protection of Customer Personal Data during transmission and storage:

1.1.1. Customer Personal Data is encrypted while in transit or at rest in the servers.

1.1.2. Secure protocols (e.g., HTTPS/SSL/TLS) on Google's ISO 27001 certified Firebase systems are used for encryption of Customer Personal Data during transmission over the internet and server APIs.

1.1.3. Customer Personal Data at rest is secured using AES encryption in the physically-secure servers provided by Google.

1.1.4. Access to networks and systems is protected by role-based authorization protocols.

1.1.5. Physical access to servers is restricted.

1.1.6. Access to Customer Personal Data is restricted through multiple layers of security, including authentication and authorization checks.

1.2. Limited data retention, data minimization, and data maintenance:

1.2.1. Customer Personal Data is only retained for as long as necessary for the purpose of the processing.

1.2.2. Customer Personal Data is securely destroyed or anonymized once it is no longer needed by Customer.

1.2.3. No Customer Personal Data is collected beyond what is provided directly by Customer as detailed in the Main Agreement and this DPA.

1.2.4. The minimum amount of Customer Personal Data is processed, only when necessary, for the agreed purpose of the application.

1.2.5. Customer Personal Data will be regularly backed-up in private servers protected from unauthorized access.

1.2.6. Policies for anonymization and pseudonymization are applied when appropriate.

1.3. Authentication and authorization:

1.3.1. Authorized users are predetermined by the data configuration provided by Customer.

1.3.2. Access rights to Customer Personal Data are granted on a need-to-know basis.

1.3.3. Google Firebase email authentication and/or other authentication (third-party, e.g., Microsoft) methods are used for email sign-ins to ensure only authenticated and authorized users have access to the software.

1.3.4. Security protocols are implemented to ensure only authorized users can access relevant Customer Personal Data.

1.4. Ongoing confidentiality, integrity, availability, and resilience of processing systems and services:

1.4.1. Integrity and resilience are ensured with regular security and risk assessments, penetration testing, employee training, and vulnerability management.

1.4.2. CI/CD pipeline is implemented for continuous and regular testing of APIs and user interfaces.

1.4.3. Events related to the processing of Customer Personal Data are logged with access logs and change logs.

1.4.4. Users, administrators, and personnel are identified and logged with unique IDs.

1.5. The Supplier has designed the services to have a high level of security and prevent personal data breaches. Testing is integrated in the development process, and a system for continuous deployment with automated tests running before deployment is in place.

1.6. The Supplier has strict processes for requiring any personnel to sign NDAs or contracts containing confidentiality DPA before access is given to systems which contain Customer Personal Data. Access is given on a need-to-know basis. The Supplier has established a routine for offboarding of employees who leave.

1.7. The Supplier has an appointed Data Protection Officer who is responsible for the processes and procedures related to privacy and security.

1.8. The Supplier has a Data Protection Policy in place. This policy, along with risk assessments, routines and security objectives are reviewed regularly in order to ascertain whether they are appropriate in relation to the needs of Supplier its customers, market conditions and threats.