OPAL DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("DPA") is agreed to between Opal Labs Inc., an Oregon corporation with its principal place of business at 555 SE MLK Jr. Blvd. Suite 105, Portland, OR 97214, U.S.A. ("Opal") and the entity appearing on the signature page of the associated Order ("Customer"), and is incorporated into the Order (defined below) and the associated Master Software as a Service Agreement (referred to herein as the "Main Agreement"). Each of Customer and Opal may be referred to herein as a "party" and together as the "parties."

RECITALS:

A. Opal provides or shall provide to Customer certain software and related services (collectively, the "Service") pursuant to the applicable order form ("Order") and the Main Agreement.

B. In connection with the Service, the parties anticipate that Opal may process certain personal data and, in so doing, may be subject to certain laws, such as Data Protection Laws (as defined below), including where Customer is established in, or Opal processes personal data of data subjects located in, the EEA, the United Kingdom, or Switzerland.

C. The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such personal data as required by any applicable laws.

1. Applicability

1.1. Sections 3 (Incorporation of Standard Contractual Clauses and UK Addendum) and other provisions of this DPA that are expressly applicable to Data Protection Laws apply only to the extent that: (1) Customer is established in the EEA or Switzerland; (2) Customer is subject to the UK GDPR / the UK Data Protection Act 2018; and/or (3) Opal processes personal data of data subjects located in the EEA, the UK, or Switzerland on behalf of Customer. Notwithstanding the foregoing, Sections 3 and related transfer provisions will also apply to the extent that the laws of any other jurisdiction require or permit the use of the SCCs (and/or substantially similar transfer mechanisms) for international transfers, and such requirements may be satisfied through the mechanisms described in this DPA. All other provisions of this DPA, including Section 6 (Sub-processors) and Exhibit 1 (Annexes), apply regardless of the applicability of Data Protection Laws.

1.2. If the Customer entity signing this DPA has ordered the Service under the Main Agreement but is not a direct party to the Main Agreement, this DPA will be incorporated into such order(s).

2. Definitions: The following definitions are used in this DPA:

2.1. "Customer" is defined above in the introductory paragraph.

2.2. "Data Protection Laws" means (as applicable) the GDPR; the UK GDPR and the UK Data Protection Act 2018; and the Swiss Federal Act on Data Protection ("FADP"), in each case to the extent applicable to the processing of personal data under the Main Agreement.

2.3. "Privacy Contact" means Opal's designated point of contact for privacy matters, as described in Section 5.1.1 (which may or may not be a statutory data protection officer depending on applicable law).

2.4. "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

2.5. "SCCs" and "New SCCs" have the meaning set forth in Section 3.2 of this DPA.

2.6. "UK Addendum" has the meaning set forth in Section 3.2 of this DPA.

2.7. "Personal data", "processing", "data controller", "data subject", "supervisory authority", "sub-processor", "data processor" and the other data processing terms used herein have the meanings ascribed to them in the GDPR.

2.8. "UK GDPR" means the GDPR as incorporated into United Kingdom law under the UK European Union (Withdrawal) Act 2018, as amended.

2.9. "FADP" means the Swiss Federal Act on Data Protection, as amended.

3. Incorporation of Current Standard Contractual Clauses and UK Addendum

3.1. This Section 3 shall apply only to the extent Customer is: (1) established within the EEA or Switzerland; (2) subject to the UK GDPR and/or the UK Data Protection Act 2018; and/or (3) to the extent Opal processes personal data of data subjects located in the EEA, the UK, or Switzerland on behalf of Customer. Notwithstanding the foregoing, this Section 3 shall also apply to the extent that the current or future laws regarding personal data of any other jurisdiction apply to Customer's personal data and may be satisfied by implementation of the Standard Contractual Clauses as described herein.

3.2. The European Commission has provided certain Standard Contractual Clauses ("SCCs") as the approved mechanism for the transfer of Personal Data under the GDPR / EEA Data Protection Laws. As of June 4, 2021, the European Commission's Implementing Decision 2021/914 has replaced prior SCCs with new SCCs which are available at *https://eurlex.europa.eu/eli/dec_impl/2021/914/oj* ("New SCCs"). As of March 21, 2022 the Addendum issued by the Information Commissioner's Office under s119A(1) of the UK's Data Protection Act 2018 ("UK Addendum") may serve as the transfer mechanism in respect of the UK GDPR.

3.3. The parties agree that the New SCCs and UK Addendum are hereby incorporated into the Main Agreement and this DPA as follows and entirely replace and supersede any reference to prior SCCs.

3.3.1. The optional language at Clause 11(a) of the New SCCs shall not apply and the following applies: (i) Clause 7 (Docking Clause) applies; (ii) Module Two (Controller to Processor) applies; (iii) Clause 9(a), Option 2 (General Written Authorization) applies, and the notice period is "thirty (30) calendar days"; (iv) Clause 11(a) is not selected; (v) Clause 17, Option 1 applies, and the governing law is Ireland; and (vi) Clause 18 designates Ireland as the forum and jurisdiction.

3.3.2. The information in Exhibit 1, attached hereto, shall be used as Annex I, II and III of the New SCCs. Annex III (Sub-processors) is provided by reference via the URL in Exhibit 1 (Annex III).

3.3.3. For transfers of personal data originating from Switzerland: (i) references in the New SCCs to a "Member State" shall not be read to prevent data subjects from Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e. Switzerland); (ii) references to the "GDPR" shall be understood to include the FADP, as applicable; and (iii) the competent supervisory authority for Switzerland is the Federal Data Protection and Information Commissioner ("FDPIC"), to the extent transfers are subject to the FADP.

3.3.4. For transfers of personal data originating from the UK, the UK Addendum is appended to the New SCCs subject to the following (i) the New SCCs are considered amended as set out in the UK Addendum (ii) "Exporter" is selected for the purpose of Section 19 and Table 4 of the UK Addendum; and (iii) the Parties recognize that the information required to populate the Tables of the UK Addendum is provided in this DPA, including the Exhibits, and that by entering into this DPA and the New SCCs as provided for in this Section 3 then they have also entered into the UK Addendum and agree to be bound by its terms.

3.4. Opal shall ensure sub-processors involved in processing personal data are subject to the relevant commitments regarding access by public authorities as set out in Clause 15 of the New SCCs.

3.5. If either the New SCCs, UK Addendum or other legal instrument in relation to international transfers of personal data from the EEA, UK or Switzerland is invalidated, amended or replaced, the parties agree to work together in good faith to resolve any resulting non-compliance issue and enter into such other form of contract as necessary to ensure that processing of personal data remains compliant with applicable Data Protection Laws and the parties will execute documentation to effectuate the legality of such.

3.6. This DPA reflects the processing of personal data by Opal as agreed and defined in the Main Agreement and Order and any other written agreement between the parties pertaining to the services provided to Customer.

4. Status of the Parties

4.1. Each party warrants in relation to personal data that it will comply with Data Protection Laws applicable to it in its role (e.g., controller or processor, as applicable), and will ensure that its personnel and any permitted sub-processors comply with the obligations applicable to them under this DPA and applicable Data Protection Laws.

4.2. In respect of the parties' rights and obligations under this DPA regarding the personal data, the parties hereby acknowledge and agree that Customer is the data controller and Opal is the data processor, and accordingly Opal agrees that it shall process all personal data in accordance with its obligations pursuant to this DPA and the Main Agreement.

4.3. Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the personal data and each party shall deal with such enquiries promptly.

5. Opal Obligations:

5.1. Opal shall:

5.1.1. Appoint a dedicated person in charge of privacy matters in writing and shall provide Customer with the contact details of such person (the "Privacy Contact"). Opal shall ensure that appropriate personnel are informed of and trained on applicable data protection obligations relevant to their roles in processing Personal Data under this DPA.

5.1.2. Ensure that only authorized personnel have access to such personal data and that any persons whom it authorizes to have access to the personal data are under obligations of confidentiality and are notified of the data protection obligations specifically arising from the work to be carried out.

5.1.3. Make available to Customer on request information reasonably necessary to demonstrate Opal's compliance with this DPA and applicable Data Protection Laws, and shall allow for and contribute to reasonable audits and inspections in accordance with Section 7 (Audit and Records).

5.1.4. Shall promptly notify Customer about any third-party request for personal information, unless prohibited by law.

5.1.5. Shall promptly notify Customer about any request of data subjects regarding the processing of personal data, including but not limited to rectification, erasure, restriction of processing, portability requests and objection to processing to ensure an appropriate reaction regarding the requests.

5.1.6. Opal shall not respond to any request of data subjects except on a documented instruction by Customer or as required under the applicable data protection laws, in which case it will, to the extent permitted under applicable data protection law, inform Customer of that legal requirement before responding to the request.

5.1.7. Only process personal data on behalf of the Customer following instructions defined in the Main Agreement and this DPA.

5.1.8. Provide at no extra cost to Customer prompt assistance in relation to Customer's obligations under Data Protection Laws with respect to:

5.1.8.1. data protection impact assessments;

5.1.8.2. a data subject's request according to Art. 12 – 22 GDPR. Opal will not substantively respond to a data subject request unless instructed by Customer (or required by applicable law), but may acknowledge receipt and direct the data subject to Customer where appropriate. Upon Customer's request Opal shall at no extra charge to Customer provide reasonable assistance to Customer (as Customer's request shall specify) to facilitate such data subject request;

5.1.8.3. notifications to the supervisory authority competent according to GDPR and/or communications to data subjects by Customer in response to any Security Breach (as defined below); and

5.1.8.4. Customer's compliance with their respective obligations under the GDPR with respect to the security of processing.

5.2. Opal represents and warrants:

5.2.1. It will only process personal data in order to provide the Service, and shall act only in accordance with: (a) this DPA, and (b) Customer's written instructions.

5.2.2. Upon becoming aware, to immediately inform Customer if, in Opal's opinion, any instruction provided by Customer or any other processing of personal data according to this DPA infringes Data Protection Laws.

5.2.3. Upon becoming aware, to notify Customer without undue delay, with a target of forty-eight (48) hours and in any event no later than seventy-two (72) hours of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by Opal, its sub-processors, or any other identified or unidentified third party (a "Security Breach");

5.2.4. To promptly provide Customer with full cooperation and assistance in respect of a Security Breach and all reasonable information in Opal's possession concerning such Security Breach insofar as it affects Customer, including the following to the extent then known:

5.2.4.1. the possible cause and consequences of the Security Breach;

5.2.4.2. the categories of personal data involved;

5.2.4.3. a summary of the possible consequences for the relevant data subjects;

5.2.4.4. a summary of the unauthorized recipients of the personal data; and

5.2.4.5. the measures taken by Opal to mitigate any damage.

6. Sub-processors

6.1. Customer provides Opal with general authorization to engage sub-processors to process Personal Data in connection with the Services. Opal may appoint, replace, or add sub-processors in accordance with this Section 6.

6.1.1. Opal may, by giving no less than thirty (30) days' notice to Customer, add or make changes to the sub-processors. Where Customer's contract requires direct notice, Opal will provide such notice by email. Where the parties' agreement permits notice by posting, Opal may provide notice by updating its sub-processor list at https://workwithopal.com/sub-processors/, which shall constitute notice as of the date of posting. Customer may object to the appointment of an additional sub-processor within fourteen (14) calendar days of such notice on reasonable grounds relating to the protection of the personal data, in which case Opal shall have the right to cure the objection through one of the following options (to be selected at Opal's sole discretion): (a) Opal will cancel its plans to use the sub-processor with regard to personal data or will offer an alternative to provide the Service without such sub-processor; or (b) Opal will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the sub-processor with regard to personal data; or (c) Opal may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve the use of such sub-processor with regard to personal data, subject to a mutual agreement of the parties to adjust the remuneration for the Service considering the reduced scope of the Service. Objections to a sub-processor shall be submitted to Opal by following the directions set forth in the sub-processor list. If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within thirty (30) days after Opals' receipt of Customers' objection, either party may terminate the Main Agreement, and Customer will be entitled to a pro-rata refund for prepaid fees for the Service not performed as of the date of termination.

6.1.2. Opal may replace a sub-processor if the reason for the change is beyond Opal's reasonable control. In such instance, Opal shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement sub-processor pursuant to Section 6.1.1.

7. Audit and Records

Opal shall, in accordance with Data Protection Laws, make available to Customer such information in Opal's possession or control as is reasonably necessary to demonstrate Opal's compliance with this DPA and applicable Data Protection Laws. Customer may conduct audits and inspections only (i) to the extent required by applicable Data Protection Laws, and (ii) subject to the following: (a) no more than once per twelve (12) months unless a material Security Breach affecting Customer's Personal Data has occurred or a competent supervisory authority requires otherwise; (b) reasonable advance written notice (at least thirty (30) days, except in connection with a Security Breach); (c) during Opal's normal business hours; (d) in a manner that does not unreasonably interfere with Opal's business operations; (e) subject to Opal's confidentiality, security, and site access policies; and (f) Customer shall bear its own costs and reimburse Opal for any reasonable out-of-pocket costs incurred in connection with any audit or inspection. As an alternative to any audit or inspection, Opal may satisfy audit requests by providing relevant third-party audit reports or certifications (e.g., SOC 2 / ISO 27001) and reasonable supporting information, unless Customer demonstrates a specific regulatory requirement for additional audit procedures.

8. General

8.1. This DPA is incorporated into and subject to the terms of the Main Agreement and applicable Order and shall be effective and remain in force for the term of the Main Agreement, applicable Order, or the duration of the Service. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of personal data.

8.2. This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

8.3. This DPA and any action related thereto shall be governed by and construed in accordance with the laws of England and Wales, without giving effect to any conflicts of laws principles. The parties' consent to the personal jurisdiction of, and venue in, the English courts. Notwithstanding the foregoing, to the extent the SCCs apply, the governing law and forum for disputes arising under the SCCs shall be as specified in the SCCs (including Clause 17 and Clause 18) and the UK Addendum, as applicable.

8.4. This DPA is the final, complete, and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party.

Exhibit 1 – Annexes to the New Standard Contractual Clauses

Annex I

A. LIST OF PARTIES

Data exporter(s):

Name	As set forth in the associated Order
Address	As set forth in the associated Order
Contact person's name, position and contact details	As set forth in the associated Order
Activities relevant to the data transferred under these Clauses	As set forth in the associated Order
Role (controller/processor)	Controller

Data importer(s): 1:

Name	Opal Labs Inc.
Address	555 SE Martin Luther King Jr Blvd ste 105, Portland, OR 97214
Contact:	Contact: Opal Privacy Contact Contact Details: privacy@workwithopal.com
Activities relevant to the data transferred under these Clauses	Opal is the marketing and communications calendar that unites teams and bridges the gap between strategy and execution of campaigns. Opal will process marketing information on behalf of the data exporter.
Role (controller/processor)	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Authorized users of the Services (including Customer's employees, contractors, and other end users) and Customer contacts, to the extent their personal data is processed in connection with the Services.
Categories of personal data transferred:	Account and user data for the performance of the Services, which may include: name, business email address, username/user ID, authentication-related information (e.g., password hash or similar), IP address, device/browser and access-log information, and other profile fields enabled by Customer.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Opal processes user account and usage data (e.g., name, username/user ID, business email address, IP address, and access logs) and Customer content uploaded to the Service. The parties do not intend that the Services be used to process special categories of data under applicable Data Protection Laws, and Customer shall not provide such data to Opal via the Services. All data is encrypted in transit using TLS 1.2 or greater and at rest using AES-256. Although all Opal employees are trained on safe data handling practices, access to databases is strictly restricted on a need-to-know basis for approved employees only.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis
Nature of the processing:	The performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing:	Data Importer shall process the Personal Data as necessary to perform the Services pursuant to 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:	Subject to the terms of the Agreement and unless otherwise agreed in writing, Data Importer shall process the Personal Data for the duration of the Agreement.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Sub-processors shall process Personal Data as necessary to perform the Services pursuant to the Agreement.
The identities of the sub-processors used in the provision of the Services and the subject matter which they process are listed here:	https://workwithopal.com/sub-processors/
In the case of specific authorizations of subprocessors, the identities of the sub-processors used in the provision of the Services, contact persons details, description of processing (including a clear delineation of responsibilities in case of several subprocessors) and the subject matter which they process are listed here:	Not applicable – General Written Authorization applies.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
Ireland - Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2
D02 Rd28, Ireland in parallel with the Swiss Federal Data Protection Information Commissioner insofar as data transfer(s) are governed by the FADP.

Annex II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Opal Platform is hosted on Azure. Opal's cloud provider maintains SOC 2 and ISO 27001 compliance, stringent backup and environment control systems, amongst other best-in-class countermeasures. More information about Microsoft's compliance programs can be found at (https://learn.microsoft.com/enus/azure/compliance/).

Opal is compliant with the ISO 27001:2022 and SOC 2 Trust Service Criteria standards.

Customer data is encrypted end to end by default using TLS 1.2 or greater for data in transit and AES-256 for data at rest. Encryption keys are stored in Hardware Security Modules.
Opal conducts annual third-party penetration testing and maintains a Threat Intelligence and Vulnerability Management Program to identify and assess security risks. Service level agreements are established to ensure vulnerabilities are promptly remediated.

Opal maintains a risk management program to identify, assess, and mitigate risks to the security, confidentiality, and integrity of Personal Data processed in connection with the Services.

Opal has implemented network monitoring systems , robust authentication methods, and data classification methods to maintain application integrity and data security. The database uses logical segregation to maintain the separation of customer records.

Opal maintains an incident response, business continuity and disaster recovery program which is tested every year to ensure business continuity after a disaster or outage. Automated backups are scheduled to support data availability and recovery.

All Opal employees receive annual information security awareness and data handling training Opal developers complete annual secure coding training with material covering the OWASP Top 10. All code changes undergo peer review, regression testing, automated testing, and manual testing to ensure appropriateness of the code change for production use.

Opal has a comprehensive vendor management program to ensure vendors and subprocessors have security and privacy equal to or greater than Opal's. Opal may share data with a Sub Processor. Sub Processors must comply with Opal data privacy and security requirements.

Annex III: LIST OF SUB-PROCESSORS

The Parties agree that the list of Sub-processors for purposes of Clause 9 and Annex III of the New SCCs is provided by reference at: https://workwithopal.com/sub-processors/ (the "Sub-processor List"). The Sub-processor List will be kept up to date and changes will be notified in accordance with Section 6 of this DPA (including the notice and objection process). For clarity, the Sub-processor List forms part of this DPA and the New SCCs as Annex III.