DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into as of the last date signed below, between [CUSTOMER LONG REFERENCE] ("Customer") and Redfish Labs, Inc. d/b/a Torch Leadership Labs. ("Company") and forms part of the Master Subscription Agreement (the "Agreement") executed by the parties. Capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. DEFINITIONS

"**CCPA**" or **"CPRA**" means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 *et seq*.) (the "**CCPA**") and the California Privacy Rights Act of 2020 (the "**CPRA**").

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

"**Data Protection Laws**" means all US and European laws and regulations that apply to Personal Data Processing in connection with any services provided by Company, including applicable international, federal, state, and local laws, rules**,** regulations, directives and governmental requirements currently in effect, and as they become effective, relating in any way to data privacy, data protection, data transfer, and data security.

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

"**GDPR**" means 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 (General Data Protection Regulation).

"**Personal Data**" shall have the meaning set forth under Applicable Data Protection Laws but at minimum means data that can be used to directly or indirectly identify a Data Subject or household.

"**Processing**" or "**Process**" have the meanings set forth in GDPR, UK GDPR, or the CPRA, as applicable.

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller.

"**SCCs**" means he standard contractual clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR, as amended or replaced from time to time by a competent authority under applicable Data Protection Laws.

"**Sub-processor**" means any entity engaged by Company to Process Personal Data on Company's behalf in connection with the Platform or Services.

"**UK Data Transfer Addendum**" means the international data transfer addendum to the EU SCCs issued by the UK Information Commissioner in accordance with section 119A of the UK Data Protection Act 2018, as amended or replaced from time to time by a competent authority under applicable DP Law.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. As between Customer and Company, Customer is the Controller, and Company is the Processor. With respect to CCPA and the CPRA, Company is Customer's "Service Provider."

2.2. **Details of Processing**. Attachment 1 (Details of Processing) to this DPA is incorporated herein.

2.3. **Restrictions on Use of Personal Data**. Company shall Process Customer Personal Data solely for the limited purpose of providing the Services under the Agreement, and Company shall Process the Personal Data in accordance with this DPA, Applicable Data Protection Laws, and the Agreement. Without limiting the foregoing, Company shall not (i) combine the Personal Data received from or on behalf of Customer with the Personal Data Processed on behalf of Company's other customers; and (ii) otherwise Process Customer Personal Data outside of the direct business relationship between Customer and Company. Nothing in the Agreement shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to Company.

2.4. **California**. Company shall not (i) combine the Personal Data received from or on behalf of Customer with the Personal Data Processed on behalf of Company's other customers; and (ii) otherwise Process Customer Personal Data outside of the direct business relationship between Customer and Company. Customer and Company hereby acknowledge and agree that nothing in the Agreement shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to Company. Company shall not retain, use, share, disclose, rent or sell any Personal Data unless the sharing or selling is for an authorized "business purpose" that is a part of the Services, and in accordance with Data Protection Laws, including, but not limited to, the CCPA and CPRA, and only to the extent reasonably necessary and proportionate to the purpose of its collection.

2.5. **Customer's Processing of Personal Data**. Customer will comply with its obligations under Data Protection Laws, including providing any required notice to Data Subjects. Customer is responsible for the accuracy and legality of Personal Data. Customer will not transmit Personal Data outside the scope of Attachment 1.

3. SUB-PROCESSORS

3.1. **Generally**. Company may retain Sub-processors to Process Personal Data to provide the Services and fulfill its contractual obligations under the Agreement, provided (i) Company will enter into a written contract with each Sub-processor that imposes terms as protective as those set out in Applicable Data Protection Laws, this DPA, and the Agreement; and (ii) Company remains liable for each Sub-processor's acts and omissions to the same extent Company would itself be liable under this DPA. A list of Company's current Sub-processors is attached hereto as Attachment 3.

3.2. **New Sub-processors**. Before any new Sub-processor processes Personal Data, Company will notify Customer at the following email address [____________]. If Customer reasonably objects to a new Sub-processor within 30 days of receiving notice, and if Company cannot provide the Platform or Services without the Sub-processor, Customer may immediately terminate the Agreement and receive a prorated refund.

4. DATA SECURITY

4.1. **Security**. Company shall implement and maintain a written information security program ("Information Security Program") that protect Personal Data and complies with Applicable Data Protection Laws and the security terms and requirements in the Technical and Organizational Measures Addendum described in Attachment 3.

4.2. **Training.** Company shall ensure that all authorized Company personnel with access to Personal Data are subject to a duty of confidentiality (whether statutory or contractual) and provide such personnel with the appropriate privacy and security training to ensure that Company maintains the requisite safeguarding and protection of Personal Data.

5. COOPERATION

5.1. **Data Subject Requests**. Company shall promptly notify Customer (and in no event later than forty-eight (48) hours) of receiving a Privacy Request or Privacy Inquiry, and Company will provide reasonable assistance to help Customer facilitate Data Subject requests it receives, including but not limited to a Privacy Request concerning a Data Subject's rights to, as applicable: (i) delete, (ii) opt-out, (iii) correct, (iv) access and receive a copy of, and (iv) limit the use, sharing, and sale of Personal Data. Company will not respond to a Privacy Request directly unless otherwise required by law.

5.2. **Compliance Assistance**. Company will cooperate and comply with all reasonable Customer instructions and requests in order for Customer to comply with its obligations under Data Protection Laws with respect to Data Subject Requests, data protection impact assessments, or supervisory authorities' inquiries.

5.3. Notification of Privacy Inquiries. If a competent judicial, government or other supervisory authority requires Company to disclose Personal Data, Company shall notify Customer in writing immediately but in no event later than forty-eight (48) hours of receipt of such request, so that Customer may seek to retain the confidentiality of the Personal Data. Company shall cooperate with Customer to redirect the appropriate authority to request the Personal Data directly from Customer.

5.4. Audits. Upon request, Company will provide Customer with a copy of its most recent third-party audit reports and additional relevant information. If such reports and information are not sufficient for Customer to meet its obligations under Data Protection Laws, Company and Customer will mutually agree upon the scope, timing, and duration of an on-site inspection, which will be conducted at Customer's expense. Information arising from an on-site audit is Company's Confidential Information, and Customer must promptly inform Company of any non-compliance discovered.

6. PERSONAL DATA BREACHES AND PROCEDURE

6.1. Breach Procedures. In accordance with Data Protection Laws and industry standards, Company agrees to deploy and follow policies and procedures to detect, respond to, and otherwise address security threats that may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data ("**Personal Data Breach**").

6.2. **Breach Response and Remediation**. Company will promptly investigate and take reasonable steps to contain, and mitigate a Personal Data Breach and will provide reasonable assistance as required for Customer to comply with its obligations under Data Protection Laws. Company will notify Customer without undue delay (and in no event later than 48 hours) after becoming aware of a breach of Personal Data Breach and will cooperate with Customer in any post-breach investigation, remediation, and communication efforts.

7. RETURN OR DELETION OF PERSONAL DATA

Duty to Delete, Destroy or Return. At the expiry or termination of the Agreement, or upon Customer's request, Company will safely delete, destroy or return all Personal Data to Customer as set out in Annex 1, except where it is required to retain copies under Data Protection Laws.

8. CROSS-BORDER PERSONAL DATA TRANSFERS

8.1. **Scope**. The Parties acknowledge that Data Protection Laws may require the implementation of specific cross-border data transfer mechanisms as a prerequisite for cross-border Personal Data transfers and agrees that they shall not transfer Personal Data cross-border unless all required data transfer mechanisms have been implemented in accordance with the requirements of Data Protection Laws. This Section 8 applies to cross-border transfers of Personal Data to a third country that does not provide an adequate level of data protection.

8.2. **Standard Contractual Clauses**. Unless another cross-border transfer mechanism is required by Data Protection Laws, the parties adopt the corresponding SCCs for the cross-border transfer of Personal Data, which will be made a part of this DPA and available on the official website of the European Union here.

8.2.1. **Transfers of Personal Data from the EEA and Switzerland**. Personal Data transfers outside of the EEA and Switzerland to a non-Adequate Country will utilize the SCCs annexed to the European Commission Decision 2021/914/EU or any successor clauses approved by the European Commission. The parties acknowledge that Module 2 of the SCCs applies to the transfers, with the following selections.

8.2.1.1. The optional Clause 7 (Docking clause) does not apply.

8.2.1.2. For Clause 9(a), Option 2 (General written authorization) applies, and notice will be provided at least 30 days in advance.

8.2.1.3. For Clause 17, Option 1 applies, and the SCCs will be governed by the laws of Ireland.

8.2.1.4. For Clause 18(b), disputes will be resolved by the courts of Ireland.

8.2.1.5. The contents of Attachment 1 form Annex I to the SCCs.

8.2.1.6. The contents of Attachment 2 form Annex II to the SCCs.

8.2.2. **Transfers of Personal Data from the United Kingdom**. Data transfers outside of the UK to a non-adequate Country shall use the SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 ("UK Addendum"). The UK Addendum attached as **Exhibit 2** will apply to such data transfers and is incorporated into this DPA.

9. MISCELLANEOUS

9.1. **Order of Precedence**. To the extent of any conflict between the Agreement and this DPA, this DPA will prevail. To the extent of any conflict between this DPA and the SCCs or the UK Addendum, the SCCs or UK Addendum will prevail.

9.2. **Limitation of Liability**. The parties' aggregate liability arising out of this DPA will be subject to the same limitations and exclusions of liability as apply under the Agreement, whether liability arises under the Agreement or this DPA.

9.3. **Governing Law**. Unless stated otherwise, this DPA will be construed in accordance with the governing law provision in the Agreement.

ATTACHMENT 1

ANNEX I
DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name: [CUSTOMER TO COMPLETE]

Address: [CUSTOMER TO COMPLETE]

Contact person's name, position, and contact details: [CUSTOMER TO COMPLETE]

Activities relevant to the data transferred under these Clauses: Determining the subject-matter of the Processing and performing Processing operations as required to receive and use the Platform and Services pursuant to the Agreement.

Signature and date: ____

Role: Controller

Data importer(s):

Name: Redfish Labs, Inc.;

Address: Redfish Labs, Inc.; 548 Market St PMB 24776, San Francisco, CA 94104-5401

Contact person's name, position and contact details: Corporate Counsel, legal@torch.io

Activities relevant to the data transferred under these Clauses: Processing operations as required to provide the Services to the data exporter pursuant to the Agreement.

Signature and date: ____

Role: Processor

B. DESCRIPTION OF TRANSFER

1. *Categories of Data Subjects Whose Personal Data is Transferred:*

    - Customer's employees, agents contractors or job applicants.

2. *Categories of Personal Data Transferred:*

    - Mandatory Profile Information: First Name; Last Name; Email Address
    - Additionally, Company may collect optional information which may include: Phone Number; Gender; Years of Experience; Birth Date; Career Reports; or Data Surveys Feedback

3. *Sensitive Data Transferred:*

- The personal data transferred concern the following special categories of data (please specify):

  Torch does not require data subjects to provide special category information, but data subjects may optionally provide information such as their race and ethnicity.

4. *Frequency of the Transfer:*
   - Continuous, depending on the data exporter's use of the Services

5. *Nature of the Processing:*
   - The nature of the Processing is the provision of the Services pursuant to the Agreement

6. *Purpose of the Data Transfer and Further Processing:*
   - Company will Process Personal Data as necessary to provide the Services pursuant to the Agreement

7. *Duration of the Processing:*
   - Data importer will Process Personal Data for the duration of the Agreement.

8. *Transfers to Sub-processors:*
   - Transfers to Sub-processors is governed by Section 3 of the DPA. The subject-matter, nature, and duration of Processing by Sub-processors is as required for the data importer to provide Services.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority/ies in accordance with Clause 13

ATTACHMENT 2

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES

Company will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Company's Information Security Program includes specific security requirements for its personnel and all subprocessors or agents who have access to Personal Data ("Data Personnel"). Company's security requirements covers the following areas:

a. Information Security Policies and Standards. Company will maintain written information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.

b. Physical Security. Company will maintain commercially reasonable security systems at all Company sites at which an information system that uses or stores Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

c. Organizational Security. Company will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.

d. Infrastructure Security. Company maintains controls to safeguard the infrastructure supporting its customer-facing applications (including its network, cloud computing instances, containers, and databases), including but not limited to DDoS protection, threat detection solutions, web application firewalls, automated vulnerability scans, and centralized logging.

e. Access Control. Company agrees that: (1) only authorized Company staff can grant, modify or revoke access to an information system that Processes Personal Data; and (2) it will implement commercially reasonable physical and technical safeguards to create and protect passwords.

f. Encryption. Web access to Company's platform is encrypted using the most current versions of SSL and TLS. Intra-system messaging on the platform uses SSH and SCP encryption methods. Archives and backups of the system are encrypted at rest using at least AES 256 or an equivalent cryptographic strength. Access and encryption keys are access-controlled and periodically refreshed.

g. Virus and Malware Controls. Company protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.

h. Application Security. As part of its application development process, Company requires all applications to undergo security reviews against a third-party standard (such as 12Factors of Saas Development and OWASP Top 10). Company employs security controls throughout the development process, including automated and continuous static code analysis, dynamic code analysis, peer review, and change control processes.

i. Testing. Company engages a third party to conduct penetration tests of its customer-facing applications no less than annually.

j. Personnel. Company has implemented and maintains a security awareness program to train employees about their security obligations. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.

k. Backups and Availability. Company maintains its infrastructure in multiple availability zones, and conducts daily automatic backups that are configured for cross- region replication.

ATTACHMENT 3
SUB-PROCESSORS

Sub-processor	Description of Processing	Location
AWS	Cloud infrastructure services.	U.S.
DataDog	Application logging.	U.S.
Cronofy	G-Suite integration for session scheduling.	U.S.
Twilio	Integrated video meeting services.	U.S.
Atlassian	Customer support services.	U.S.
Unbounce	Landing page optimization services.	U.S.
StitchData	Advanced business analytics.	U.S.
Postmark	End-user communications provider.	U.S.
Sentry	Application logging.	U.S.
Ziggeo	Integrated video recording services.	U.S.
LogRocket	Application logging.	U.S.
Zapier	System integration services.	U.S.
Salesforce	Customer support services.	U.S.
G-Suite	Facilitation of coach and user correspondence.	U.S.
Preset	Advanced business analytics.	U.S.
Cube	Advanced business analytics.	U.S.
Airbyte	Advanced business analytics.	U.S.
Tray.io	System Integration	U.S.

EXHIBIT 2

UK DATA TRANSFER ADDENDUM TO THE EU SCCs

Capitalized terms used but not defined in this addendum have the meanings given to them in the agreement into which this addendum is incorporated.

PART 1: TABLES

Table 1: Parties

Start date	As of the Effective Date set out in the DPA.
Parties	As set out in Annex I.A of the EU SCCs in Exhibit 1 of this DPA.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of “Approved EU SCCs” which this Addendum is appended to is the EU SCCs set out in Exhibit 1 of this DPA.

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	As set out in Annex I.A of the EU SCCs in Attachment 1 of this DPA.
Annex 1B: Description of Transfer:	As set out in Annex I.B of the EU SCCs in Attachment 1 of this DPA.
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data:	As set out in Annex II of the EU SCC in Attachment 2 of this DPA.
Annex III: List of Sub processors:	As set out in Annex III of the EU SCCs in Attachment 3 of this DTA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Both the data importer and the data exporter may end this addendum in accordance with the terms of the UK Data Transfer Addendum.

ALTERNATIVE PART 2: MANDATORY CLAUSES

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.