Torch -- Data Privacy Addendum for Customers

This Data Privacy Addendum ("**Addendum**"), amends the Agreement between Customer and Redfish Labs, Inc. d/b/a Torch Leadership Labs ("**Torch**" or "**Vendor**"), each a "**Party**" and collectively the "**Parties**" agree as follows:

1. **Definitions**. For purposes of this Addendum:

   a. "**Data Protection Laws**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("**CCPA**"), the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**"), and the United Kingdom Data Protection Act of 2018 ("**UK Privacy Act**"). For the avoidance of doubt, if Vendor's Processing activities involving Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this Addendum.

   b. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

   c. "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, and such terms shall have the same meaning as defined by applicable Data Protection Laws, that is Processed in relation to the Agreement.

   d. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

   e. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

   f. "**Standard Contractual Clauses**" means one or both of the following, as the context requires:

      i. For Personal Data subject to the UK Data Protection Law, the "**2010 Standard Contractual Clauses**," defined as the clauses issued pursuant to EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec/2010/87/2016-12-17 and completed as described in the "Data Transfers" section below, until such time as the United Kingdom recognizes the 2021 Standard Contractual Clauses, in which case such clauses shall apply to Personal Data Transferred from the UK; and

      ii. For Personal Data subject to the GDPR or the FADP, the "**2021 Standard Contractual Clauses**," defined as the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.

2. **Scope and Purposes of Processing**.

   a. Vendor will Process Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this Addendum; (2) on Customer's behalf pursunt to Customer's instructions; and (3) in compliance with Data Protection Laws. Vendor will not sell Personal Data or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein. For purposes of this paragraph, "sell" shall have the meaning set forth applicable Data Protection Laws.

   b. Vendor will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-Personal Data or any other data without the express authorization of Customer.

3. **Personal Data Processing Requirements**. Vendor will:

   a. Ensure that the persons it authorizes to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

   b. Upon written request of Customer, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Protection Laws (such as rights to access or delete Personal Data), at Customer's reasonable expense.

   c. Promptly notify Customer of (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Vendor's Processing of Personal Data on Customer's behalf, unless prohibited by Data Protection Laws. Vendor will provide Customer with reasonable cooperation and assistance in relation to any such request. If Vendor is prohibited by applicable Data Protection Laws from disclosing the details of a government request to Customer, Vendor shall inform Customer that it can no longer comply with Customer's instructions under this Addendum without providing more details and await Customer's further instructions. Vendor shall use all available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

   d. Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws, and at Customer's reasonable expense.

   e. Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Vendor under Data Protection Laws to consult with a regulatory authority in relation to Vendor's Processing or proposed Processing of Personal Data.

4. **Data Security**. Vendor will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Exhibit A.

5. **Security Breach**. Vendor will notify Customer without undue delay of any known Security Breach and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation, by:

   a. Taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

   b. Providing Customer with the following information, to the extent known:

i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

ii. The likely consequences of the Security Breach; and

iii. Measures taken or proposed to be taken by Vendor to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. **Subprocessors**.

a. Customer acknowledges and agrees that Vendor may use Vendor affiliates and other subprocessors to Process Personal Data in accordance with the provisions within this Addendum and Data Protection Laws. Where Vendor sub-contracts any of its rights or obligations concerning Personal Data, including to any affiliate, Vendor will take steps to select and retain subprocessors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with applicable Data Protection Laws.

b. If Vendor processes Personal Data subject to the applicable Data Protection Laws in the European Economic Area, Switzerland, or the United Kingdom on Customer's behalf, Vendor will provide a current list of Vendor's subprocessors upon Customer's request, and Customer hereby consents to Vendor's use of such subprocessors. Vendor's current list of subprocessors is available at Schedule C below. Vendor will maintain an up-to-date list of its subprocessors, and it will provide Customer with prior notice at least twenty (20) days before any new subprocessor is added to the list. In the event Customer objects to a new subprocessor, Vendor will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to, Customer's use of the services to avoid Processing of Personal Data by the objected-to subprocessor. If Vendor does not reasonably consider Customer's request for a such a change, Customer may terminate the Agreement subject to the applicable termination provisions in the Agreement.

1. **Data Transfers.**

a. Customer authorizes Vendor to make international transfers of the Personal Data only if (i) applicable Data Privacy Law for such transfers is respected and (ii) the transfer is otherwise permitted by this DPA.

b. With respect to Personal Data transferred from the United Kingdom for which UK Data Protection Law (and not the law in any European Economic Area ("EEA") jurisdiction or Switzerland) governs the international nature of the transfer, and such law permits use of the 2010 Standard Contractual Clauses but does not permit use of the 2021 Standard Contractual Clauses, the 2010 Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict and shall be deemed completed as follows:

- The "exporter" is Customer, and the exporter's contact information is set forth below,
- The "importer" is Vendor, and Vendor's contact information is set forth below.
- Where Clause 9 of the 2010 Standard Contractual Clauses requires specification of the law that governs the Clauses, the parties select the law of the United Kingdom.
- The "illustrative indemnification clause" labelled "optional" is deemed stricken.

- Appendices 1 and 2 of the 2010 Standard Contractual Clauses are set forth in Schedule A below.
- By entering into this DPA, the Parties are deemed to be signing the 2010 Standard Contractual Clauses and their applicable Appendices.

c. With respect to Personal Data transferred from the EEA and Switzerland, the 2021 Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict, and they will be deemed completed as follows:

- Customer acts as a controller and Vendor acts as Customer's processor with respect to the Personal Data subject to the 2021 Standard Contractual Clauses, and its Module 2 applies.
- Clause 7 (the optional docking clause) is included.
- Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization). The initial list of sub-processors is set forth in Schedule C of this DPA and Vendor shall update that list and provide twenty (20) days' notice to Customer in advance of any intended additions or replacements of sub-processors.
- Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.
- Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the laws of Ireland.
- Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.
- Annexes I and II of the 2021 Standard Contractual Clauses are set forth in Schedule B of the DPA.
- Annex III of the 2021 Standard Contractual Clauses (List of subprocessors) is inapplicable.

d. Additional Safeguards for the Transfer and Processing of Personal Data from the EEA, Switzerland, and the United Kingdom. To the extent that Vendor Processes Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the EEA, Switzerland, or the United Kingdom, Vendor agrees to the following safeguards to protect such data to an equivalent level as applicable Data Protection Laws:

- Vendor and Customer shall encrypt all transfers of the Personal Data between them, and Vendor shall encrypt any onward transfers it makes of such personal data, to prevent the acquisition of such data by third parties.
- Vendor represents and warrants that:
    - as of the date of this DPA, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702").
    - no court has found Vendor to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

  - it is not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to FISA Section 702.

- Vendor will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

- Upon Customer's request, Vendor shall provide a transparency report indicating the types of binding legal demands for the Personal Data it has received, including national security orders and directives.

- Vendor will promptly notify Customer if Vendor can no longer comply with the applicable Standard Contractual Clauses or the clauses in this Section. Vendor shall not be required to provide Customer with specific information about why it can no longer comply, if providing such information is prohibited by applicable law. Such notice shall entitle Customer to terminate the Agreement in accordance with the termination provisions in the Agreement (or, at Customer's option, affected statements of work, order forms, and like documents thereunder).

7. **Audits**. Vendor will make available to Customer all reasonable information necessary to demonstrate compliance with this Addendum and will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, provided that, such audit shall occur nor more than once every twelve (12) calendar months, upon reasonable prior written notice, and to the extent Vendor's personnel are required to cooperate thereupon, during Vendor's normal business hours.

8. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Protection Laws, Vendor will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Protection Laws, Vendor will inform Customer if it is not able to return or delete the Personal Data.

9. **Survival**. The provisions of this Addendum survive the termination or expiration of the Agreement for so long as Vendor or its subprocessors Process the Personal Data.

Schedule A

Appendix 1 to the 2010 Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer): Customer, who is engaging Vendor for the purposes described in the Agreement and any relevant Statements of Work.

Data importer
The data importer is (please specify briefly activities relevant to the transfer): Vendor, who will process the Personal Data for the purposes described in the Agreement and any relevant Statements of Work.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Customer's employees.

Categories of data
The personal data transferred concern the following categories of data (please specify): Personal Data provided by Customer to Vendor for purposes of Vendor performing services pursuant to the Agreement, which consist of:

- Mandatory Profile Information
  - First Name
  - Last Name
  - Email Address
  - Company Role
- Optional Profile Information
  - Phone Number
  - Gender
- Mandatory Demographic Information
  - Years of Experience
- Optional Demographic Information
  - Birth Date
  - Career Direct Reports
  - Current Direct Reports
- Optional Feedback Data Surveys
  - Coach matching surveys
  - 360 degree review surveys

  - Goal progress surveys
  - Coaching session feedback surveys
- Website usage information

Special categories of data (if appropriate)
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.

Processing operations (including subject matter, nature, purpose and duration of Processing)
The personal data transferred will be subject to the following basic processing activities (please specify):

All Processing activities set forth in the Agreement and any relevant Statements of Work.

Appendix 2 to the 2010 Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Exhibit A.

Schedule B

Annexes I and II of the 2021 Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES
MODULE TWO: Transfer controller to processor

Data exporter(s):
Name: …
Address: …
Contact person's name, position and contact details: …
Activities relevant to the data transferred under these Clauses: The processing activities as described in the Agreement and any relevant Statements of Work.
Signature and date: …
Role (controller/processor): Controller

The exporter (Controller) is Customer and Customer's contact details and signature are as provided in the Agreement and the DPA.

Data importer(s): Vendor
Name: …
Address: …
Contact person's name, position and contact details: …
Activities relevant to the data transferred under these Clauses: The processing activities as described in the Agreement and any relevant Statements of Work
Role (controller/processor): Processor

The importer (Processor) is Vendor and Vendor's contact details and signature are as provided in the Agreement and the DPA.

B. DESCRIPTION OF TRANSFER
MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred:

Customer's employees and/or job applicants.

Categories of personal data transferred:

Personal Data provided by Customer to Vendor for purposes of Vendor performing services pursuant to the Agreement, which consist of:

- Mandatory Profile Information
    - o First Name
    - o Last Name
    - o Email Address
    - o Company Role
- Optional Profile Information
    - o Phone Number
    - o Gender
- Mandatory Demographic Information

- o Years of Experience
- Optional Demographic Information
  - o Birth Date
  - o Career Direct Reports
  - o Current Direct Reports
- Optional Feedback Data Surveys
  - o Coach matching surveys
  - o 360 degree review surveys
  - o Goal progress surveys
  - o Coaching session feedback surveys
- Website usage information

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 measure:

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

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

On a continuous basis for as long as Customer is engaging Vendor to provide the Services.

Nature of the processing:

The nature of the Processing is as forth in the Agreement and any relevant Statements of Work.

Purpose(s) of the data transfer and further processing:

The purposes for the data transfer are to facilitate Vendor's provision of services pursuant to the Agreement and any relevant Statements of Work.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Transfers to subprocessors are for the same purposes as transfers to the processor.

C. COMPETENT SUPERVISORY AUTHORITY
MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: Ireland Data Protection Commissioner

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See Exhibit A immediately below.

Exhibit A

VENDOR DATA SECURITY MEASURES

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

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

a. Information Security Policies and Standards. Vendor 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. Vendor will maintain commercially reasonable security systems at all Vendor 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. Vendor will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.

d. Infrastructure Security. Vendor 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. Vendor agrees that: (1) only authorized Vendor 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 Vendor'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. Vendor 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, Vendor requires all applications to undergo security reviews against a third-party standard (such as 12Factors of Saas Development and OWASP Top 10). Vendor 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. Vendor engages a third party to conduct penetration tests of its customer-facing applications no less than annually.

j. Personnel. Vendor 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. Vendor maintains its infrastructure in multiple availability zones, and conducts daily automatic backups that are configured for cross- region replication.

Schedule C

Torch Subprocessors

Name of Subprocessor	Purpose of Processing	Location of Processing
AWS	Cloud infrastructure services.	U.S.
Sisense	Advanced business analytics.	U.S.
DataDog	Application logging.	U.S.
Cronofy	G-Suite integration for session scheduling.	U.S.
Zoom	Integrated video meeting services.	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.
Segment	Customer data management services.	U.S.
Salesforce	Customer support services.	U.S.
Zapier	System integration services.	U.S.
G-Suite	Facilitation of coach and user correspondence.	U.S.