Simplify Workforce Data Protection Addendum (DPA)

This Data Protection Addendum ("DPA") is an Attachment to the Agreement. Customer and SaaS Provider (Simplify Workforce) enter into this DPA by executing a DPA Setup Page. Capitalized terms not defined in this DPA are defined in the Agreement or DPA Setup Page.

1. Definitions.

a. **"Agreement"** means the Agreement between Customer and SaaS Provider incorporating the Simplify Workforce Software License Agreement which is specified on the DPA Setup Page.

b. **"Audit" and "Audit Parameters"** are defined in Section 14 below.

c. "**Audit Report**" is defined in Section 14 below.

d. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

e. "**Customer Instructions**" is defined in Section 3a. below.

f. "**Customer Personal Data**" means Personal Data in Customer Data (as defined in the Agreement).

g. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and (iv) the UK Data Protection Act 2018; (v) the Privacy Act, 1988, (vi) The Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022, (vii) the Personal Information Protection and Electronic Documents Act 2000, (the "PIPEDA") in each case, as updated, amended or replaced from time to time.

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

i. "**DPA Effective Date**" is specified on the DPA Setup Page.

j. "**DPA Setup Page**" means a separate document executed by Customer and SaaS Provider which causes this DPA to become an Attachment to their Agreement.

k. "**EEA**" means European Economic Area.

l. "**Key Terms**" means Agreement, DPA Effective Date and Sub-processor List as specified by the parties on the DPA Setup Page.

m. "**Personal Data**" means information about an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

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

o. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

p. “**Restricted Transfer**” means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination to any other country that is not subject to an adequacy determination.

q. “**Schedules**” means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA are:

r. “**Sub-Processor**” means mean any Affiliate, agent or assignee of SaaS Provider that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by SaaS Provider.

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms
Schedule 5	Details of Sub-Processors

s. “**Security Incident**” means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by SaaS Provider.

t. “**Specified Notice Period**” is 48 hours.

u. “**Sub-processor**” means any third party authorized by SaaS Provider to Process any Customer Personal Data.

v. “**Sub-processor List**” means the list of SaaS Provider’s Sub-processors as identified or linked to on the DPA Setup Page.

2. Scope and Duration.

a. **Roles of the Parties.** This DPA applies to SaaS Provider as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data**.**

b. **Scope of DPA.** This DPA applies to Provider’s Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

c. **Duration of DPA.** This DPA commences on the DPA Effective Date and terminates upon expiration or termination of the Agreement (or, if later, the date on which SaaS Provider has ceased all Processing of Customer Personal Data).

d. **Order of Precedence.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. **Processing of Personal Data.**

   a. **Customer Instructions.**

      i. SaaS Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with SaaS Provider's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.
      ii. "**Customer Instructions**" means:
         1. Processing to provide the Service and perform SaaS Provider's obligations in the Agreement (including this DPA) and;
         2. other reasonable documented instructions of Customer consistent with the terms of the Agreement.
      iii. Details regarding the Processing of Customer Personal Data by SaaS Provider are set forth in Schedule 1 (Subject Matter and Details of Processing).
      iv. SaaS Provider will notify Customer if it receives an instruction that SaaS Provider reasonably determines infringes Data Protection Laws (but SaaS Provider has no obligation to actively monitor Customer's compliance with Data Protection Laws).

4. **Processing Purpose and Instructions.**

   a. The subject matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, shall be as set out in the Agreement, or in this Addendum attached Schedule 1, which is incorporated herein by reference.
   b. SaaS Provider shall Process Personal Data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Agreement and the Data Protection Law, unless SaaS Provider is otherwise required by law to which it is subject (and in such a case, SaaS Provider notify Customer of that legal requirement before Processing, provided that the SaaS Provider is not legally prohibited from doing so).
   c. To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between SaaS Provider and Customer, which may include any additional fees that may be payable by Customer to SaaS Provider for carrying out such Processing Instructions.
   d. SaaS Provider shall not retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the Parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under Data Protection Law. SaaS Provider's performance of the Services may include disclosing Personal Data to Sub-Processors where this is necessary for the performance of the Services. The SaaS Provider certifies that it, and any person receiving access to Personal Data on its behalf, understand the restrictions contained herein.

5. **Obligations of the Processor/SaaS Provider**.

   a. The SaaS Provider shall only process Personal Data as contractually agreed or as instructed by the Customer unless the SaaS Provider is legally obliged to carry out a specific type of data processing. Should the SaaS Provider be bound by such obligations, the SaaS Provider is to inform the Customer thereof prior to processing the data, unless informing him/her is illegal. Furthermore, the SaaS Provider shall not use the data provided for processing for any another purposes, specifically his/her own.

b. SaaS Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

c. Any individuals who could have access to the data processed on behalf of the Customer must be obliged in writing to maintain Confidentiality unless they are already legally required to do so via another written agreement.

d. Information may be provided to third parties by the SaaS Provider solely with the Customer's prior consent. Inquiries sent directly to the SaaS Provider will be immediately forwarded to the Customer.

e. It is understood between the Parties that the Customer will ensure that each Data Subject/Consumer has been informed of, and has already given consent to, the use, processing and transferring of his or her Personal Information, as required by applicable Information Protection Laws. The Customer will conform to applicable law (as may be amended from time to time or replaced).

6. Sub-Processors.

a. **Use of Sub-Processors.**

   i. Customer generally authorizes SaaS Provider to engage Sub-Processors to Process Customer Personal Data. Customer further agrees that SaaS Provider may engage its Affiliates as Sub-Processors.

   ii. SaaS Provider will: (i) enter into a written agreement with each Sub-Processor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Sub-Processor that cause SaaS Provider to breach any of its obligations under this DPA.

b. **Sub-Processor List.** SaaS Provider will maintain an up-to-date list of its Sub-Processors, including their functions and locations, as specified in the **Schedule 5**.

c. **Notice of New Sub-Processors.** SaaS Provider may update the Sub-Processor List from time to time. At least 30 days before any new Sub-Processor Processes any Customer Personal Data, SaaS Provider will add such Sub-Processor to the Sub-Processor List and notify Customer through email or other means specified on the DPA Setup Page.

d. **Objection to New Sub-Processors.** If, within 30 days after notice of a new Sub-Processor, Customer notifies SaaS Provider in writing that Customer objects to SaaS Provider's appointment of such new Sub-Processor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

7. Compliance with Laws.

a. SaaS Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

b. Customer will comply with Data Protection Laws in its issuing of Customer Instructions to SaaS Provider. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable SaaS Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

c. **Changes to Laws.** The Parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

8. Reasonable Security and Safeguards.

a. **Security Measures.** SaaS Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with SaaS Provider's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). SaaS Provider will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

b. **Incident Notice & Response.**

i. SaaS Provider will implement and follow procedures to detect and respond to Security Incidents.

ii. SaaS Provider will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within SaaS Provider's reasonable control.

iii. Upon Customer's request and considering the nature of the applicable Processing, SaaS Provider will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws. SaaS Provider notification regarding or response to a Security Incident under this clause shall not be construed as an acknowledgment by SaaS Provider of any fault or liability with respect to the Security Incident.

iv. Customer acknowledges that SaaS Provider's notification of a Security Incident is not an acknowledgement by SaaS Provider of its fault or liability.

v. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

9. Controller/Customer Responsibilities.

a. Customer is responsible for reviewing the information made available by SaaS Provider relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws.

b. Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

10. Notification obligations.

a. The SaaS Provider shall immediately notify the Customer of any personal data breaches. Any justifiably suspected incidences are also to be reported. Notice must be given to one of the Customer's known addresses within 48 hours from the moment the SaaS Provider realises the respective incident has occurred. This notification must contain at least the following information:

i. A description of the type of the personal data protection infringement including, if possible, the categories and approximate number of affected persons as well as the respective categories and approximate number of the personal data sets.
ii. The name and contact details of the data protection officer or another point of contact for further information.
iii. A description of the probable consequences of the personal data protection Infringement.
iv. A description of the measures taken or proposed by the SaaS Provider to rectify the personal data protection infringement and, where applicable, measures to mitigate their possible adverse effects.

b. SaaS Provider notification regarding or response to a Security Incident under this clause shall not be construed as an acknowledgment by SaaS Provider of any fault or liability with respect to the Security Incident.
c. Customer shall be responsible for providing the information to Data subjects on the processing of Personal Data/Information as required by applicable Data Protection Legislation.
d. Customer is responsible to inform Data Subject about the responsibility split between the contracting parties as per this DPA. Customer shall be the primary contact for Data Subject to exercise their rights as per applicable Data Protection Legislation.

11. **Data Protection Impact Assessment.** Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to SaaS Provider, SaaS Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

12. Data Subjects Requests.

a. **Assisting Customer.** Upon Customer's request and taking into account the nature of the applicable Processing, SaaS Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfil such requests independently (including through use of the Simplify Service).
b. **Data Subject Requests.** If SaaS Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, SaaS Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

13. Data Return or Deletion.

a. **During Subscription Term.** During the Subscription Term, Customer may, through the features of the SaaS Provider Service or such other means specified on the DPA Setup Page, access, return to itself or delete Customer Personal Data.

b. **Post Termination.**

  i. Following termination or expiration of the Agreement, SaaS Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from SaaS Provider's systems.
  ii. Deletion will be in accordance with industry-standard secure deletion practices. SaaS Provider will issue a certificate of deletion upon Customer's request.
  iii. Notwithstanding the foregoing, SaaS Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, SaaS Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

14. Audits.

a. **SaaS Provider Records Generally.** SaaS Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with SaaS Provider's obligations under this DPA and Data Protection Laws.

b. **Third-Party Compliance Program.**

  i. SaaS Provider will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "Audit Report") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).
  ii. Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.
  iii. Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 14.c (Customer Audit) below.

c. **Customer Audit.**

  i. Subject to the terms of this Section 14.c, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with SaaS Provider that is consistent with the Audit Parameters (an "Audit").
  ii. Customer may exercise its Audit right: (i) to the extent SaaS Provider's provision of an Audit Report does not provide sufficient information for Customer to verify SaaS Provider's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.
  iii. Each Audit must conform to the following parameters ("Audit Parameters"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with SaaS Provider, (ii) be limited in scope to matters reasonably required for Customer to assess SaaS Provider's compliance with this DPA

and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during SaaS Provider's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by SaaS Provider, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

d. Nothing in the Addendum will require SaaS Provider to either disclose to Customer or its third-party auditor, or to allow Customer or its third-party auditor to access: (i) any data of any other SaaS Provider's customer; (ii) SaaS Provider's internal accounting or financial information; (iii) any trade secret of a Service Provider or its Affiliates; (iv) any information that, in SaaS Provider's reasonable opinion, could compromise the security of any SaaS Provider's systems or cause any breach of its obligations under applicable law or its security or privacy obligations to any third party; or (v) any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Data Protection Laws.

15. Cross-Border Transfers/Region-Specific Terms.

a. **Cross-Border Data Transfers.**

i. SaaS Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Simplify Service.

ii. If SaaS Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

b. **Region-Specific Terms.** To the extent that SaaS Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

16. **Liability.** The Customer and the SaaS Provider shall be jointly liable for compensation to anyone for damage caused by any unauthorised party or for incorrect data processing within the scope of the contract.

17. Instructions.

a. The Customer reserves the right of full authority to issue instructions concerning data processing on his/her behalf.

b. The Customer and the SaaS Provider shall appoint the individuals who have been exclusively authorised to issue and accept instructions.

c. In the event of a change to the above-mentioned individuals or if they are subject to long-term incapacitation, the other party shall be immediately informed of any successors or representatives.

d. The SaaS Provider shall immediately inform the Customer if an instruction issued by the Customer violates, in his opinion, legal requirements. The SaaS Provider shall be entitled to forego carrying out the relevant instructions until they have been confirmed or changed by the party responsible on behalf of the Customer.

e. The SaaS Provider is to document the instructions issued and their implementation.

18. Miscellaneous.

a. Any claims brought under this DPA will be subject to the terms and conditions of the Main Agreement, including the exclusions and limitations set forth in the Main Agreement.

b. In the event of a conflict between the Main Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

c. SaaS Provider may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the SaaS Provider as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party’s rights to Process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by SaaS Provider.

d. If SaaS Provider intends to change this DPA, and such change will have a material adverse impact on Customer, as reasonably determined by SaaS Provider, then SaaS Provider will inform Customer (in the SaaS Provider's portal for customers) at least 10 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

e. Should any parts of this agreement be invalid, this will not affect the validity of the remainder of the agreement.

f. Any ancillary agreements must be in writing.