

How to get a binding Data Processing Addendum with Reejig: (1) Complete the signatory information below these instructions; (2) complete and sign in the signature box on page 5; (3) send the completed and signed DPA to Reejig as follows, either: (i) if you are a new customer, to your sales representative at Reejig with a copy to legal@Reejig.com, or (ii) if you are an existing customer, to legal@Reejig.com.

This Data Processing Addendum (the **"Addendum"**) is between _____ (**"Customer"**) located at _____, and the Reejig entity set forth in the Agreement (as hereinafter defined) (**"Reejig"**). Both Customer and Reejig are individually referred to as a **"Party"**, and jointly referred to as the **"Parties"**.

This Addendum has been pre-signed by the Reejig entity set forth above. Any hand-written or other changes to this Data Processing Addendum made without Reejig's prior written approval will not be binding against Reejig. This Addendum is subject to the document signed between the Parties governing Customer's Subscription to Reejig's software. If there is no Agreement between the Parties, executing this Addendum will have no force or effect between Reejig and the person or entity that countersigns this Addendum.

1. Definitions.

Any capitalized words not defined in this DPA shall have the definitions given to them elsewhere in the Agreement.

Terms such as **"Controller," "Data Subject," "Personal Data," "Process"** (including its variants) and **"Processor"** have the meanings given in the GDPR.

"Affiliate" means any business entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with a party to the Agreement. For purposes of this definition, "control" means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question.

"Agreement" means (i) the master subscription agreement or other subscription agreement between Customer and Reejig governing Customer's access to Reejig's Software, and/or (ii) any service agreement between Customer and Reejig governing the provision of professional services by Reejig if such professional services are linked to access to Customer's Personal Data by Reejig.

"Data Protection Law(s)" means Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 repealing Directive 96/46/EC (General Data Protection Regulation 2016/679 (**"GDPR"**)), national laws implementing GDPR, the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the **"UK GDPR"**), any other applicable data protection laws, including the Australian federal Privacy Act 1988, and each case as may be amended or superseded from time to time.

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 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 (the **"EU SCCs"**); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (the **"UK SCCs"**).

2. Subject Matter of this Addendum.

2.1. Data Processor and Controller. This Addendum stipulates the rights and obligations of Customer and Reejig regarding the Processing of Customer's Personal Data under the Agreement, and if applicable, Customer's Affiliates. This DPA applies to all activities within the scope of and related to the Agreement. As between Reejig and Customer, Reejig is a Data Processor and Customer, and if applicable Customer's Affiliates that Customer permits to use Reejig's Software and Services under the Agreement, act as Data Controllers.

2.2. Governance. Customer acts as a single point of contact. Where authorizations, consent, instructions, or permissions are provided by Customer, these are provided not only on behalf of the Customer but also on behalf of any Customer Affiliates using Reejig's Software and Services under the Agreement. Where Reejig informs or gives notice to Customer, such information or notice is deemed received by Customer Affiliates permitted by Customer to use Reejig's Software and Services under the Agreement. Customer shall forward such information and notices to such Customer Affiliates. This DPA does not constitute a third-party beneficiary agreement.

2.3. Scope. The Addendum does not affect the agreed scope of the services under the Agreement. To the extent that its obligations under this Addendum require Reejig to perform any additional services or activities that are not included in the scope the Agreement, Reejig shall be entitled to charge for these additional services or activities on a time and material basis according to Reejig's then current price list.

3. Data Processing Obligations.

3.1. Processing Scope. Reejig shall Process Customer's Personal Data on behalf of Customer as Customer's Data Processor. The scope of the Personal Data, as well as the extent and nature of the Processing of Customer's Personal Data, is determined exclusively by Customer, and is for the sole purpose of Reejig's Software and Services to Customer as further specified in the Agreement and in **Annex 1 – Processing Details**.

3.2. Instructions. The initial instructions to Reejig are laid out in the Agreement and this Addendum. Customer shall be entitled to issue modifications to its instructions and to issue new instructions. Because of the nature of Reejig's services as multi-client services, Customer shall take the technical and operational feasibility of following its instructions into account. Reejig will use reasonable efforts to follow any Customer instructions if they are required by Data Protection Law and technically and operationally reasonably feasible. If carrying out an instruction is not required by Data Protection Law and/or technically and/or operationally reasonably feasible, or Reejig considers the instruction unlawful, Reejig will notify Customer without undue delay. The Parties will then discuss the matter and work together in good faith to find a solution that is feasible and addresses the underlying legal issue or other concern or interest of the Customer.

3.3. Customer Warranty. Customer hereby warrants and represents, on a continuous basis throughout the Term of the Agreement, that all Personal Data provided or made available by Customer to Reejig for Processing in connection with the Agreement was collected by Customer and transmitted to Reejig in accordance with applicable Data Protection Laws and Customer has obtained all necessary approvals, consents, authorizations and licenses from each and every Data Subject required under Data Protection Laws to enable Reejig to Process Personal Data pursuant to the Agreement and to exercise its rights and fulfil its obligations under the Agreement.

3.4. Assistance. Reejig shall provide Customer with reasonable assistance with data protection impact assessments, prior consultations with data protection authorities that Customer is required to carry out under Data Protection Laws, dealing with requests from Data Subjects, and any other assistance obligations required by applicable law. If Reejig receives a request from a Data Subject in relation to the Personal Data processing hereunder, Reejig will promptly ask the Data Subject to redirect its request to Customer.

3.5. Appropriate Personnel. Reejig shall only engage personnel who have committed themselves to observing data privacy obligations. Reejig shall regularly train those employees to whom it grants access to Customer's Personal Data on security and privacy law compliance.

3.6. Technical and Organizational Measures. Reejig has taken appropriate technical and organizational measures according to Article 32 GDPR to keep Personal Data secure and protected against unauthorized or unlawful processing and accidental loss, destruction, or damage, and undertakes to continue doing so during the term of this Addendum. Reejig has implemented the technical and organizational measures further described in **Annex 2 – Technical and Organizational Measures**. Reejig may implement alternative measures provided the security level of the measures as specified in **Annex 2 – Technical and Organizational Measures** hereto is not reduced. Upon Customer's request, Reejig shall provide updated versions of **Annex 2 – Technical and Organizational Measures**. To evidence compliance with this Addendum, Customer agrees Reejig may provide up-to-date attestations, reports, or extracts from independent bodies (e.g., ISO 27001 reports/certificates) that scrutinize and confirm the processing of Customer's Personal Data is in accordance with this Addendum.

3.7. Data Breach. After Reejig has a reasonable degree of certainty about the occurrence of accidental or unlawful

destruction, loss or alteration of, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Reejig pursuant to this Addendum (a “**Personal Data Breach**”), Reejig shall notify Customer without undue delay of a Personal Data Breach, provide such information as Customer may reasonably require to meet its obligations under Data Protection Laws regarding the Personal Data Breach, and take steps to remediate the Personal Data Breach. Reejig may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Reejig.

3.8. Correction; Deletion; or Blocking of Personal Data. Reejig may be required to correct, erase and/or block Customer Personal Data if and to the extent the functionality of the Service does not allow the Customer to do so. However, Reejig shall not correct, erase and/or block Personal Data unless instructed by Customer.

3.9. Data Deletion. Reejig shall delete all of Customer Data within 30 days of Customer’s request.

4. Standard Contractual Clauses.

4.1. Reejig as Data Exporter. If Reejig acts as a data exporter, it has entered the Standard Contractual Clauses and Module 3 (Processor to Processor) thereof with the respective Subprocessor acting as a data importer or will do so prior to the start of Sub-processing. Reejig has procured or, for new Subprocessors, will procure that pursuant to Clause 17 Option 2 of the Standard Contractual Clauses, they will be governed by the law of the EU Member State in which the data exporter is established.

4.2. Reejig’s Subprocessor as Data Exporter. If a Subprocessor of Reejig acts as data exporter, Reejig has procured or will procure that such Subprocessor executes the Standard Contractual Clauses and Module 3 (Processor to Processor) thereof with each Subprocessor prior to the start of the Sub-processing. Section 4.1, sentence 2 applies accordingly.

4.3. Restricted Transfers. The Parties agree that when the transfer of Customer Personal Data from Customer to Reejig is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

4.3.1. EU GDPR Application. Regarding Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows: (s) Module Two will apply; (t) in Clause 7, the optional docking clause will apply; (u) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 5 of this Data Protection Addendum; (v) in Clause 11, the optional language will not apply; (w) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established ; (x) in Clause 18(b), disputes shall be resolved before the courts of the member state where the data exporter is established; (y) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Data Protection Addendum; and (z) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Data Protection Addendum.

4.3.2. UK GDPR Application. Regarding Customer Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(1) For so long as it is lawfully permitted to rely on Standard Contractual Clauses for the transfer of Personal Data to processors set out in the European Commission’s Decision 2010/87/EU of 5 February 2010 (the “**Prior C2P SCCs**”) for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between Customer and Reejig on the following basis: (x) Appendix 1 shall be completed with the relevant information set out in Annex I to this Data Protection Addendum; (y) Appendix 2 shall be completed with the relevant information set out in Annex II to this Data Protection Addendum; and (z) the optional illustrative indemnification Clause will not apply.

(2) Where sub-clause 4.3.2(1) above does not apply, but the Customer and Reejig are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a “UK Addendum to the EU Standard Contractual Clauses” (the “**UK Addendum**”) issued by the Information Commissioner’s Office under s.119A(1) of the Data Protection Act 2018, then: (y) The EU SCCs, completed as set out above in clause 4.3.1 of this Data Protection Addendum shall also apply to transfers of such Customer Personal Data, subject to the following sub-clause (z); and (z) the UK Addendum shall be deemed to form part of this Data Protection Addendum, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Customer Personal Data.

4.4 Order of Priority. If any provision of this Data Protection Addendum or the Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5. Subprocessors.

5.1. Subprocessor Approval. In accordance with Art. 28 (2) sentence 2 GDPR, Customer hereby provides its general authorization to Reejig to appoint any Subprocessors identified by Reejig in **Annex 3 – SubProcessor List** (the

“Subprocessor List”) to Process Personal Data on Reejig’s behalf. Reejig shall ensure that Subprocessors on the Subprocessor List are contractually obligated to protect Personal Data in compliance with Data Protection Laws and consistent with the obligations imposed on Reejig in this Addendum. Reejig shall remain responsible for the acts and omissions of each Subprocessor on the Subprocessor List as if they were the acts and/or omissions of Reejig. Customer agrees that Reejig may provide written notification of any change to the Subprocessor List by updating the Subprocessor List at the following link <https://www.reejig.com/subprocessors>. Any updates to the Subprocessor List regarding new Subprocessors shall occur thirty days prior to Reejig utilizing the entity as a subprocessor for Customer (the **“30 Day Period”**).

5.2. Subprocessor Objections. If Customer has a legitimate and material data protection reason to object to a Subprocessor added to the Subprocessor List, Customer may object by sending Customer’s objection and the basis for such objection to legal@reejig.com within fifteen days of such addition. If the Parties cannot mutually agree to a reasonable resolution to Customer’s objection within further fifteen days of Reejig’s receipt of Customer’s objection, Customer may terminate the Agreement and this Addendum upon written notice to Reejig. For the avoidance of doubt Customer’s objection and/or the discussions between the Parties do not affect Reejig’s right to use the new Subprocessor after the 30-Day Period. If Customer terminates, the termination shall take effect at the time determined by the Customer which shall be no later than 60 days from the date of Reejig’s notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this 60-day period, Customer is deemed to have accepted the new Subprocessor.

5.3. Emergency Replacement. Reejig may replace a Subprocessor without advance notice where the reason for the change is outside of Reejig’s reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Reejig will inform Customer of the replacement Subprocessor as soon as possible following its appointment.

6. Auditing Rights. If Customer is subject to an audit or investigation from a data protection regulator, Reejig shall, when required, respond to any information requests, and/or agree to submit its premises and operations to audits, including inspections by Customer and/or the competent data protection regulator, in each case for the purpose of evidencing its compliance with this Addendum, provided that: (v) Customer shall ensure that all information obtained or generated in connection with any information request, audit or inspection is kept strictly confidential (unless disclosure to a competent data protection regulator or as otherwise required by applicable law), (w) Customer shall ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to Reejig’s business, and acknowledging that such information request, audit or inspection shall be subject to any reasonable policies, procedures or instructions of Reejig for the purposes of preserving security and confidentiality; (x) Customer shall give Reejig at least 15 days’ prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides Customer with less than 15 days’ notice, in which case Customer shall provide Reejig with as much notice as practically possible, (y) a maximum of one information request, audit and/or inspection may be requested by Customer in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing, and (z) Customer shall pay Reejig’s reasonable costs for any assistance or facilitation of any audit or inspection or other work undertaken unless such costs are incurred due to Reejig’s breach of its obligations under this Addendum. If any audit request is not at the request of a data protection regulator, Customer agrees (1) to request information in the first instance in written form, (2) Reejig may respond to such requests by providing up-to-date attestations, reports or extracts from independent bodies (e.g., ISO 27001 reports/certificates) that scrutinizes and confirms the processing of Customer’s Personal Data is in accordance with the agreed to measures herein, it being understood that Customer may demand additional clarifications and perform on-site inspections where necessary to satisfy Data Protection Law requirements, or (3) on Reejig’s request, to conduct the audit through a certified auditor the Parties jointly agree on.

7. International Data Transfers. This Section 7 applies when Reejig or its subprocessors Processes Customer’s Personal Data in countries outside the EEA or Switzerland (**“International Transfer”**). Reejig shall undertake (and shall ensure that its subprocessors undertake) an International Transfer only if the requirements according to Art. 44 seqq. GDPR are met (collectively, the **“International Transfer Mechanisms”**). When this Section 7 applies, the terms of this Addendum shall be read in conjunction with the applicable International Transfer Mechanism. Nothing in this Addendum shall be construed to prevail over any conflicting clause of the applicable International Transfer Mechanism. Should the Standard Contractual Clauses be invalidated, replaced, annulled, or otherwise designed in such a way that they no longer constitute adequate safeguards for data transfers to third countries, Reejig shall undertake, together with Customer, to

find an alternative solution that complies with the applicable Data Protection Laws and ensures the lawfulness of processing Personal Data in third countries.

8. Notifications.

8.1. If Reejig receives a request, subpoena, or court order (including through an obligation due to legal provisions or official injunctions from state authorities) requiring Reejig to provide any Customer's Personal Data Processed under this Addendum to an authority, Reejig shall attempt to redirect the relevant authority to request that data directly from the Data Controller, and notify Customer without undue delay, unless Reejig is prohibited from doing so.

8.2. Where Customer's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Reejig' control, Reejig' shall notify Customer of such action without undue delay. Reejig shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Customer's sole property and area of responsibility, that Personal Data is at Customer's sole disposition, and that Customer is the Data Controller.

9. California Consumer Privacy Act ("CCPA"); California Privacy Rights Act ("CPRA"). If Reejig Processes a California resident's Personal Data on behalf of Customer, Reejig does so as a service provider under the CCPA, or the CPRA when applicable. Reejig agrees it will not use Personal Data other than for the business purpose set forth in the Agreement, or for a commercial purpose other than providing the services specified in the Agreement. Reejig shall not sell Customer Personal Data. Reejig represents that it understands the restrictions in this Addendum, and its obligations under the CCPA & CPRA, and will comply with them. Reejig shall only notify Customer if it can no longer comply with the CCPA or CPRA. Reejig shall comply with the CCPA & CPRA as a service provider and provide the level of protection the CCPA and CPRA requires as applicable.

10. Term. This Addendum shall follow the term of the Agreement (the "**Term**").

11. Miscellaneous. No modification of this Addendum shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to this Addendum. The foregoing shall also apply to any waiver or modification of this mandatory written form. This Addendum shall take precedence over any conflicting provisions of the Agreement. The Standard Contractual Clauses shall take precedence over any conflicting provisions in the main body of this Addendum and the Agreement.

Reejig PTY LTD	Customer
	
NAME: Siobhan Savage	NAME:
TITLE: CEO & Founder	TITLE:
DATE: September 1, 2023	DATE:

ANNEX 1 – Processing Details

Categories of Personal Data Processed: Customer may upload, submit, or otherwise provide certain personal data to Reejig, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- Personal data including full name, contact information, general work location, and date of birth (if supplied);
- Company name, job title, job grades, job awards, remuneration and work history;
- Photos;
- Education history;
- Certifications, professional affiliations, and honors; and
- Any other personal data uploaded, submitted, or otherwise provided to Reejig by Customer in its sole discretion.

Categories of Data subjects:

- Customer and its Authorized Users; and
- Customer's current and former employees, independent contractors, and job applicants.

Special categories of data (if appropriate): If a customer provides special categories of Personal Data, then Reejig may also process special categories Personal Data.

Data Transfer Frequency: continuous basis.

The Period for which the Personal Data will be retained: as set forth in the Agreement.

In case of a Restricted Transfer:

Data exporter:

The data exporter is (please briefly specify your activities relevant to the transfer):

- **Customer Name:** Customer as listed above and as set forth in the Agreement.
- **Customer Address:** Customer's address is set forth in the Agreement.
- **Activities relevant to data transfer:** use of Reejig's workforce intelligence software.
- **Contact Person's name, position, and contact details:** as set forth in the Agreement.
- **Customer Role:** controller.

Data importer:

The data importer is (please briefly specify activities relevant to the transfer):

- **Data Importer:** Reejig PTY LTD, a software provider that provides its customers access to a workforce intelligence software platform.
- **Address:** 383 George Street, Sydney 2000, NSW Australia.
- **Activities relevant to data transfer:** Providing workforce intelligence software platform specified in the Agreement between Data Exporter and Data Importer.
- **Role:** processor.

Description of Transfer:

- Module Two: controller to processor.

Purposes of the Data Transfer and Further Processing:

- **Purpose:** as set forth in the Agreement.
- **Further Processing:** as set forth at: <https://www.reejig.com/subprocessors>.

Subprocessor Processing:

- **Subject Matter:** the types of data described above.
- **Nature of Processing:** as set forth at: <https://www.reejig.com/subprocessors>.
- **Duration:** as set forth in the Agreement.

Competent Supervisory Authority: Customer's competent supervisory authority.

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

A. Information Security

- Maintain relevant security certifications, such as the ISO27001 certification.
- Have a documented Information Security Policy (reviewed at least annually) that is communicated and made available to all relevant personnel.
- Ensure that information security systems and processes are reviewed and updated by the Information Security Management Team at least annually.
- Maintain a Risk Register which contains an assessment of information security risks and the controls required to mitigate/reduce those risks.
- Deliver regular (at least annually) information security awareness training to all employees.
- Conduct regular external penetration tests (at least annually).
- All Customer Data is encrypted at rest and in transit.

B. Physical Security & Disaster Recovery

- Reejig uses Amazon Web Services ('AWS') to host its data. AWS has implemented security measures around all its data centers. The most up-to-date details of these security measures can be accessed at <https://aws.amazon.com/compliance/data-center/controls/>

C. Network Security

- Access to systems is restricted to authorized users only and are reviewed on a regular basis.
- The principle of least privilege is applied when provisioning access to systems.
- Multi-factor authentication is used wherever available, and employees are required to use passwords that meet minimum complexity requirements.
- The production and test environments are separated.

D. Human Resources Security

- Appropriate background checks are conducted on all employees in accordance with documented policies.
- Access is revoked on a timely basis in accordance with security procedures upon the departure of any personnel.

Subprocessor Technical and Organizational Security Measures

The technical and organizational security measures utilized by subprocessors are substantially similar to those set forth above.

ANNEX 3 SUBPROCESSORS

Customer has authorized the following subprocessors:

<https://www.reejig.com/subprocessors>

Description of processing: The description of processing is set forth at the link above in this Annex 3.