SG-SG controller-to-processor — SaaS HR vendor processing employee data

> **Sample document — not legal advice.** This document is one of a library of sample legal drafts published by LawCrew at `lawcrew.ai/samples`. It illustrates how the LawCrew agent team approaches a common Singapore DPA scenario. **It is not legal advice and is not tailored to any specific transaction.**
>
> LawCrew is a legal-technology service, not a law firm. For your own matter, run an intake through the product and engage an independent Singapore-qualified lawyer to review before signing.
>
> *Sample DPA #01 · Hand-authored pending specialist roll-out · Published 2026-05-22*

Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") is entered into as of 1 January 2026 (the "**Effective Date**") between:

(1) Meridian Logistics Pte Ltd, a company incorporated in Singapore [UEN: 201438291K] with its registered office at 12 Marina Boulevard, #18-01, Marina Bay Financial Centre Tower 3, Singapore 018982 (the "**Controller**"); and

(2) Cendana People Cloud Pte Ltd, a company incorporated in Singapore [UEN: 202017845W] with its registered office at 79 Anson Road, #22-04, Singapore 079906 (the "**Processor**").

The Controller and the Processor are each a "**Party**" and together the "**Parties**".

Recitals

(A) The Parties have entered into a master subscription agreement dated 1 January 2026 (the "**Principal Agreement**"), under which the Processor provides a cloud-based human resources information system (the "**Services**") to the Controller.

(B) In the course of providing the Services, the Processor will Process Personal Data on behalf of the Controller.

(C) The Parties enter into this Addendum to record their respective obligations in relation to such Processing and to give effect to the Controller's obligations under the Personal Data Protection Act 2012 (No. 26 of 2012) of Singapore (the "**PDPA**").

1. Definitions

1.1 In this Addendum, unless the context requires otherwise, the following terms have the following meanings:

(a) **"Affected Individual"** means an individual whose Personal Data is the subject of a Personal Data Breach.

(b) **"Authorised Personnel"** means an employee, contractor or agent of the Processor who has a need to access Personal Data in order to perform the Services and who is bound by written obligations of confidentiality.

(c) **"Personal Data"** means data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the Processor has or is likely to have access, that is Processed by the Processor on behalf of the Controller under the Principal Agreement.

(d) **"Personal Data Breach"** means an unauthorised access, collection, use, disclosure, copying, modification or disposal of Personal Data, or a loss of any storage medium or device on which Personal Data is stored, in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal is likely to occur.

(e) **"Process"**, **"Processing"** and **"Processed"** mean any operation or set of operations performed on Personal Data, including collection, recording, storage, retrieval, use, disclosure, transmission, erasure or destruction.

(f) **"Protection Obligation"**, **"Retention Limitation Obligation"**, **"Transfer Limitation Obligation"**, **"Access and Correction Obligations"** and **"Notification Obligation"** each have the meaning given to them under the PDPA and the Advisory Guidelines issued by the Personal Data Protection Commission (the **"PDPC"**).

(g) **"Sub-processor"** means any third party engaged by the Processor to Process Personal Data on its behalf in connection with the Services.

1.2 Terms used but not defined in this Addendum have the meanings given to them in the Principal Agreement or, where not defined there, in the PDPA.

2. Roles and scope

2.1 The Parties acknowledge that, for the purposes of the PDPA, the Controller is the organisation that determines the purposes for which, and the manner in which, the Personal Data is Processed, and the Processor is a data intermediary acting on behalf of the Controller in respect of such Personal Data.

2.2 This Addendum applies to all Processing of Personal Data by the Processor in the course of providing the Services. Schedule 1 sets out the subject matter, nature and purpose of the Processing, the categories of Personal Data and the categories of data subjects.

2.3 In the event of any conflict between this Addendum and the Principal Agreement in relation to the Processing of Personal Data, this Addendum prevails.

3. Processor's obligations and instructions

3.1 The Processor shall Process Personal Data only:

(a) for the purposes set out in Schedule 1;

(b) in accordance with the documented instructions of the Controller, including those set out in this Addendum and the Principal Agreement; and

(c) as required by any law applicable to the Processor, in which case the Processor shall, to the extent permitted by that law, notify the Controller of the legal requirement before Processing.

3.2 The Processor shall promptly inform the Controller if, in its opinion, an instruction from the Controller would cause the Processor to be in breach of the PDPA. The Processor is not obliged to monitor or audit the Controller's compliance with the PDPA generally.

3.3 The Processor shall not sell, rent, lease or otherwise commercialise the Personal Data, and shall not Process the Personal Data for its own purposes or for the purposes of any third party, except for the limited internal purposes of providing, securing and improving the Services in a manner that does not identify any individual.

4. Confidentiality

4.1 The Processor shall treat all Personal Data as confidential information and shall not disclose any Personal Data to any person other than:

(a) Authorised Personnel;

(b) Sub-processors engaged in accordance with Clause 6; or

(c) any other person to whom disclosure is required by law, in which case Clause 3.1(c) applies.

4.2 The Processor shall ensure that all Authorised Personnel are subject to written obligations of confidentiality that survive the termination of their engagement with the Processor for a period of not less than three (3) years.

5. Security measures

5.1 The Processor shall implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised access, collection, use, disclosure, copying, modification, disposal and similar risks, having regard to the nature of the Personal Data and the harm that would result from any such event. These measures are set out in Schedule 2.

5.2 The Processor shall not make any material change to the measures set out in Schedule 2 that materially reduces the level of protection afforded to the Personal Data without the prior written consent of the Controller, except where such change is required by law or by a generally accepted security standard to which the Processor is certified.

5.3 The Processor's security programme is, as at the Effective Date, certified to ISO/IEC 27001 and is independently audited at least annually. The Processor shall provide the Controller with a copy of the most recent audit report or attestation summary on request, subject to reasonable confidentiality undertakings.

6. Sub-processors

6.1 The Controller grants the Processor a general written authorisation to engage Sub-processors to Process Personal Data, subject to the conditions in this Clause 6.

6.2 The Processor shall maintain an up-to-date list of Sub-processors at a URL notified to the Controller, and shall give the Controller not less than thirty (30) days' prior written notice before adding or replacing a Sub-processor. The current list of approved Sub-processors as at the Effective Date is set out in Schedule 3.

6.3 The Controller may object to the appointment or replacement of a Sub-processor on reasonable grounds relating to data protection by giving written notice to the Processor within the thirty (30) day notice period. If the Parties cannot agree on a resolution within a further fifteen (15) days, the Controller may terminate the affected portion of the Services on written notice without liability for early-termination fees in respect of that portion. Charges already paid for that portion of the Services will be refunded on a pro-rata basis.

6.4 The Processor shall enter into a written contract with each Sub-processor that imposes on that Sub-processor obligations no less protective than those imposed on the Processor under this Addendum, and the Processor remains liable to the Controller for the acts and omissions of each Sub-processor as if they were the acts and omissions of the Processor.

7. Data subject rights

7.1 The Processor shall, taking into account the nature of the Processing, provide reasonable assistance to the Controller by appropriate technical and organisational measures, insofar as this is possible, to enable the Controller to comply with the Access and Correction Obligations and any other rights of individuals under the PDPA.

7.2 If the Processor receives any request, complaint or communication from an individual or the PDPC that relates to the Controller or the Personal Data, the Processor shall:

(a) not respond to the request, complaint or communication on its own initiative beyond confirming that the request should be addressed to the Controller; and

(b) notify the Controller without undue delay and in any event within five (5) Business Days of receipt.

7.3 The Processor's reasonable costs of providing the assistance described in Clause 7.1 are included in the Service fees, except where the volume or complexity of requests materially exceeds the assistance contemplated by the Principal Agreement, in which case the Processor may charge its standard professional services rates on prior written notice.

8. Personal Data Breach

8.1 The Processor shall, without undue delay and in any event within seventy-two (72) hours of becoming aware of a Personal Data Breach, notify the Controller of the breach in writing.

8.2 The notification under Clause 8.1 shall include, to the extent then known to the Processor:

(a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Affected Individuals and of records concerned;

(b) the likely consequences of the Personal Data Breach;

(c) the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including measures to mitigate its possible adverse effects; and

(d) a single point of contact at the Processor from whom further information can be obtained.

8.3 The Processor shall provide such further information as the Controller may reasonably require to enable the Controller to discharge its Notification Obligation to the PDPC and to Affected Individuals, including in respect of any breach that is a notifiable data breach under section 26B of the PDPA.

8.4 The Processor shall not make any public communication concerning a Personal Data Breach affecting the Personal Data without the prior written consent of the Controller, except where required by law.

9. International transfers

9.1 The Processor shall Process and store the Personal Data within Singapore. The production environment of the Services, including all primary databases and backups, is hosted in a Singapore data centre region, as further described in Schedule 2.

9.2 The Processor shall not transfer the Personal Data outside Singapore without the prior written consent of the Controller. Where consent is given, the Processor shall ensure that the recipient is bound by legally enforceable obligations to provide a standard of protection that is comparable to the protection under the PDPA, in accordance with the Transfer Limitation Obligation and the relevant PDPC Advisory Guidelines.

9.3 Clause 9.1 does not prevent the Processor from providing remote technical support from outside Singapore, provided that such access is read-only, logged, time-bounded and does not result in the storage of Personal Data outside Singapore.

10. Audit and information rights

10.1 The Processor shall, on reasonable written request, make available to the Controller all information necessary to demonstrate compliance with this Addendum, including the most recent third-party audit reports referred to in Clause 5.3.

10.2 The Controller may, on not less than thirty (30) days' prior written notice and not more than once in any twelve (12) month period (except following a Personal Data Breach or where required by the PDPC or any other regulator with jurisdiction over the Controller), conduct an audit of the Processor's compliance with this Addendum. The audit shall:

(a) be conducted by the Controller or by an independent auditor of recognised standing appointed by the Controller and not being a competitor of the Processor;

(b) take place during normal business hours and on dates agreed in advance;

(c) be subject to reasonable confidentiality undertakings; and

(d) not unreasonably interfere with the Processor's business operations.

10.3 The Parties shall each bear their own costs of an audit, save that where the audit reveals a material breach of this Addendum, the Processor shall reimburse the Controller's reasonable audit costs.

11. Return and deletion

11.1 On termination or expiry of the Principal Agreement, or at any earlier time on the written instruction of the Controller, the Processor shall, at the option of the Controller:

(a) return all Personal Data to the Controller in a structured, commonly used and machine-readable format; or

(b) securely delete all Personal Data,

and in either case shall securely delete all existing copies, except to the extent that retention is required by applicable law.

11.2 Personal Data retained pursuant to Clause 11.1 shall remain subject to this Addendum for so long as it is retained, and shall be Processed solely to the extent and for the period necessary to comply with that legal requirement.

11.3 The Processor shall, on request, provide the Controller with a written certificate of deletion signed by an authorised officer of the Processor within ninety (90) days of the date of return or deletion.

12. Term and termination

12.1 This Addendum takes effect on the Effective Date and continues for so long as the Processor Processes Personal Data on behalf of the Controller, notwithstanding the termination or expiry of the Principal Agreement.

12.2 A material breach of this Addendum by either Party that is not remedied within thirty (30) days of written notice shall constitute a material breach of the Principal Agreement.

13. General

13.1 **Liability.** The liability of each Party under this Addendum is subject to the limitations of liability set out in the Principal Agreement. For the avoidance of doubt, the financial penalties that may be imposed on the Controller by the PDPC under section 48J of the PDPA, and any compensation ordered to be paid by the Controller to an individual under section 48O of the PDPA, are direct losses recoverable by the Controller from the Processor to the extent caused by a breach of this Addendum by the Processor or its Sub-processors.

13.2 **Governing law.** This Addendum is governed by and construed in accordance with the laws of Singapore.

13.3 **Jurisdiction.** The dispute resolution and jurisdiction provisions of the Principal Agreement apply to any dispute arising out of or in connection with this Addendum.

13.4 **Order of precedence.** In the event of any conflict between (a) the body of this Addendum and (b) any Schedule, the body prevails unless the Schedule expressly states otherwise.

13.5 **Variation.** This Addendum may only be varied by written agreement signed by an authorised representative of each Party.

13.6 **Severability.** If any provision of this Addendum is held to be invalid or unenforceable, the remaining provisions remain in full force and effect, and the Parties shall negotiate in good faith to replace the invalid provision with a valid provision having as nearly as possible the same commercial effect.

Signed for and on behalf of Meridian Logistics Pte Ltd

Name: _____

Title: _____

Date: _____

Signed for and on behalf of Cendana People Cloud Pte Ltd

Name: _____

Title: _____

Date: _____

Schedule 1 — Processing details

Item	Description
Subject matter	Provision of a cloud-based human resources information system to the Controller, including employee records, leave management, payroll input data preparation, performance reviews and benefits administration.
Duration	The term of the Principal Agreement, plus any retention period required by applicable law.
Nature and purpose	Storage, retrieval, organisation, structuring, transmission and presentation of Personal Data for the purpose of enabling the Controller to administer the employment relationship with its workforce.
Types of Personal Data	Full name; NRIC / FIN / passport number (masked, last four characters); date of birth; residential address; personal contact details (mobile, personal email); employment details (job title, department, reporting line, employment start date); compensation data (base salary, allowances, bonus); leave records; performance review records; emergency contact details; bank account information for payroll input; CPF account number.
Special categories	None expected. The Services are not configured to store medical records, biometric identifiers, or data concerning racial or ethnic origin, religion or political views. The Controller shall not upload such categories without prior written notice to the Processor.
Categories of data subjects	Current employees of the Controller; former employees within applicable retention windows; job applicants; contractors engaged by the Controller and onboarded through the Services; emergency contacts of the foregoing.

Schedule 2 — Technical and organisational measures

1. Hosting and segregation. The production environment is hosted in a Singapore data centre region operated by a Tier IV co-location provider. Customer data is logically segregated by tenant identifier, and tenant access is enforced at the application, API and database layers.

2. Encryption. Personal Data is encrypted in transit using TLS 1.2 or higher with modern cipher suites, and at rest using AES-256 with keys managed in a FIPS 140-2 Level 3 hardware security module. Database backups are encrypted with separate keys.

3. Access control. Access to production systems is restricted to Authorised Personnel on a least-privilege, need-to-know basis. All such access requires multi-factor authentication and is logged. Administrative access is reviewed quarterly. Customer-facing access uses role-based access control with optional single sign-on (SAML 2.0 / OIDC).

4. Network security. Production systems are deployed behind a managed web application firewall, with intrusion detection, DDoS mitigation and network segmentation between application, database and management tiers.

5. Vulnerability management. The Processor performs continuous dependency scanning, monthly internal vulnerability scans and an annual external penetration test conducted by an independent CREST-accredited tester. Critical vulnerabilities are remediated within seven (7) days of identification and high-severity vulnerabilities within thirty (30) days.

6. Logging and monitoring. Application, system and security logs are retained for not less than twelve (12) months in a tamper-evident store, with automated alerting for anomalous access patterns.

7. Personnel. All Authorised Personnel undergo background screening to the extent permitted by law, complete annual data protection and security training, and are bound by written confidentiality obligations that survive termination.

8. Business continuity. Production data is replicated to a secondary Singapore availability zone. The recovery time objective is four (4) hours and the recovery point objective is one (1) hour. Disaster recovery procedures are tested at least annually.

9. Secure development. The Processor follows a secure software development lifecycle that includes mandatory code review, static analysis and pre-deployment security review for changes affecting the handling of Personal Data.

10. Certifications. The Processor maintains ISO/IEC 27001 certification, with a current Statement of Applicability available on request.

Schedule 3 — Approved Sub-processors

Sub-processor	Function	Location of Processing
Tanjong Hosting Pte Ltd	Co-location and managed cloud infrastructure	Singapore
Raffles Quay Communications Pte Ltd	Transactional email delivery (e.g. password reset, leave-approval notifications)	Singapore
Pasir Panjang Analytics Pte Ltd	Product usage analytics; pseudonymised event data only, no Personal Data fields	Singapore

Sub-processor	Function	Location of Processing
Bras Basah Support Tools Pte Ltd	In-product customer support messaging tooling	Singapore