SG-US controller-to-processor — US payments processor handling transaction 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 #02 · 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) Tanjong Commerce Pte Ltd, a company incorporated in Singapore [UEN: 201912034E] with its registered office at 8 Cross Street, #24-01, Manulife Tower, Singapore 048424 (the **"Controller"**); and

(2) Northbridge Payments, Inc., a Delaware corporation with its principal place of business at 535 Mission Street, 14th Floor, San Francisco, California 94105, United States of America (the **"Processor"**).

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

Recitals

(A) The Parties have entered into a payment services agreement dated 1 January 2026 (the **"Principal Agreement"**), under which the Processor provides card and electronic payment acceptance, settlement, fraud screening and chargeback handling services (the **"Services"**) to the Controller.

(B) In the course of providing the Services, the Processor Processes Personal Data on behalf of the Controller. For certain narrow purposes — card-scheme compliance, anti-money-laundering screening and statutory reporting — the Processor acts as an independent controller of payment-related personal data.

(C) The Parties enter into this Addendum to record their respective obligations in relation to the Processing of Personal Data and to give effect to the Controller's obligations under the Personal Data

Protection Act 2012 (No. 26 of 2012) of Singapore (the **"PDPA"**), including the Transfer Limitation Obligation.

1. Definitions

1.1 In this Addendum:

(a) **"Cardholder Data"** means the primary account number, cardholder name, expiry date and service code, together with any sensitive authentication data, in each case as defined under the Payment Card Industry Data Security Standard.

(b) **"Independent Controller Purposes"** means the limited purposes set out in Clause 2.3.

(c) **"Personal Data"** means data about an identified or identifiable individual that is Processed in connection with the Services and includes Cardholder Data and Transaction Data.

(d) **"Personal Data Breach"** has the meaning given in the PDPA.

(e) **"Process"**, **"Processing"** and **"Processed"** have the meaning given in the PDPA.

(f) **"Transaction Data"** means data describing a payment transaction, including amount, currency, timestamp, merchant identifier, terminal identifier, authorisation code, risk-screening signals and dispute history.

(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 References to the PDPA include the Advisory Guidelines on Key Concepts in the PDPA and other relevant guidance issued by the Personal Data Protection Commission (the **"PDPC"**).

1.3 Terms used but not defined in this Addendum have the meanings given to them in the Principal Agreement.

2. Roles and scope

2.1 In respect of Personal Data Processed in connection with the Services, the Controller is the data controller and the Processor acts as a data intermediary on behalf of the Controller, save as set out in Clause 2.3.

2.2 The Processor's Processing of Personal Data as data intermediary is described in Schedule 1.

2.3 The Parties acknowledge that, for the limited purposes of:

(a) compliance with the operating rules of Visa, Mastercard, American Express, NETS and any other applicable card scheme or payment network;

(b) anti-money-laundering, counter-terrorism financing and sanctions screening obligations applicable to the Processor or its banking partners;

(c) prevention, detection and investigation of fraud across the Processor's merchant base; and

(d) statutory and regulatory reporting required of the Processor or its banking partners,

(together, the **"Independent Controller Purposes"**), the Processor acts as an independent controller and is responsible for its own compliance with the laws applicable to that Processing. The Controller acknowledges that the Processor's role for the Independent Controller Purposes cannot be overridden by Controller instructions.

2.4 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 Save in respect of the Independent Controller Purposes, 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.

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 or of applicable card-scheme rules.

3.3 The Processor shall not sell, rent, lease or otherwise commercialise the Personal Data, and shall not use Personal Data for behavioural advertising or for any purpose unrelated to the Services or the Independent Controller Purposes.

4. Confidentiality

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

(a) employees, contractors and agents of the Processor who have a need to access Personal Data in order to perform the Services or the Independent Controller Purposes, and who are bound by written obligations of confidentiality;

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

(c) the relevant card schemes, acquiring banks and regulators, to the extent reasonably required for the Independent Controller Purposes; or

(d) any other person to whom disclosure is required by law.

4.2 The Processor shall ensure that all personnel referred to in Clause 4.1(a) are subject to written confidentiality obligations that survive termination of their engagement for 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, having regard to the nature of the Personal Data (which includes Cardholder Data) and the harm that would result from unauthorised access, collection, use, disclosure, copying, modification or disposal. These measures are set out in Schedule 2.

5.2 The Processor shall at all times maintain certification as a PCI DSS Level 1 service provider and shall provide the Controller with a copy of its current Attestation of Compliance on request.

5.3 The Processor shall not make any change to the measures set out in Schedule 2 that materially reduces the level of protection without the prior written consent of the Controller, except where such change is required by law, by a card scheme or by an applicable security standard to which the Processor is certified.

6. Sub-processors

6.1 The Controller grants the Processor a general written authorisation to engage Sub-processors to Process Personal Data, subject to 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, save that no prior notice is required where a card-network operator, acquiring bank, settlement bank or regulator becomes a recipient of Personal Data by operation of the card-scheme rules or applicable law. 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 resolve the objection within a further fifteen (15) days, the Controller may terminate the affected portion of the Services on written notice.

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

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 under the PDPA.

7.2 The Controller acknowledges that:

(a) requests for access to or correction of Personal Data Processed for the Independent Controller Purposes (including suspicious-transaction reports) may be lawfully refused by the Processor under section 21 of the PDPA, sections 39 and 40 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 or equivalent provisions of US federal or state law; and

(b) the Processor will make best efforts to coordinate any partial responses with the Controller.

7.3 If the Processor receives a request, complaint or communication from an individual or the PDPC that relates to the Controller or the Personal Data, the Processor shall notify the Controller without undue delay and in any event within five (5) Business Days of receipt.

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 affecting Personal Data Processed on behalf of the Controller, notify the Controller in writing.

8.2 The notification shall include, to the extent then known, the matters listed in section 26C of the PDPA, including:

(a) a description of the nature of the Personal Data Breach, the categories and approximate number of individuals concerned and the categories and approximate number of records concerned;

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

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

(d) a single point of contact at the Processor for further information.

8.3 The Processor shall provide such further information and assistance as the Controller reasonably requires to enable the Controller to discharge its Notification Obligation under section 26D of the PDPA, including in respect of any notifiable data breach.

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

9. International transfers and cross-border safeguards

9.1 The Controller authorises the Processor to transfer Personal Data to the United States and to such other countries as are necessary for the provision of the Services and the Independent Controller

Purposes, in each case as described in Schedule 4.

9.2 The Processor shall ensure that any transfer of Personal Data outside Singapore is made on terms that 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. The contractual safeguards set out in this Addendum, including the security obligations in Clause 5, the breach-notification obligations in Clause 8, the audit rights in Clause 10 and the deletion obligations in Clause 11, are intended to achieve that comparable standard.

9.3 The Processor confirms that, as at the Effective Date:

(a) it has implemented and shall maintain the technical and organisational measures set out in Schedule 2;

(b) its production environment is operated to PCI DSS Level 1; and

(c) it has assessed the laws of the recipient jurisdictions and has determined that, in combination with the contractual safeguards in this Addendum, the Personal Data will receive a comparable standard of protection.

9.4 If, during the term of this Addendum, the Processor becomes aware of a change in the laws of any recipient jurisdiction or in market guidance that materially undermines the safeguards in Clause 9.3, the Processor shall notify the Controller and the Parties shall negotiate in good faith additional safeguards or, failing such agreement, the Controller may terminate the affected portion of the Services.

9.5 Schedule 4 sets out the specific data flows, recipient jurisdictions and additional safeguards (including any sub-processor onward transfer terms).

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:

(a) the most recent PCI DSS Attestation of Compliance;

(b) the most recent SOC 2 Type II report; and

(c) summary results of the annual penetration test referred to in Schedule 2.

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 affecting the Controller's data or where required by a regulator with jurisdiction over the Controller), conduct an audit. 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 on dates agreed in advance;

(c) be subject to reasonable confidentiality undertakings;

(d) not unreasonably interfere with the Processor's business operations or compromise the confidentiality of other customers' data; and

(e) for the avoidance of doubt, not extend to access to the Processor's source code or to the systems used solely for the Independent Controller Purposes.

10.3 Each Party shall bear its own audit costs, save that where the audit reveals a material breach, 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 Controller's option, return or securely delete all Personal Data Processed on behalf of the Controller, and securely delete all existing copies.

11.2 Notwithstanding Clause 11.1, the Processor may retain Personal Data:

(a) to the extent and for the period required by applicable law, including under the Payment Services Act 2019 of Singapore, the US Bank Secrecy Act and applicable record-retention rules; and

(b) to the extent required by card-scheme rules for chargeback, retrieval-request and dispute-resolution purposes, typically not exceeding eighteen (18) months from the date of the relevant transaction.

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

11.4 The Processor shall, on request, provide a written certificate of deletion within ninety (90) days of the date of deletion (other than for data retained under Clause 11.2).

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 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. Financial penalties imposed on the Controller by the PDPC under section 48J of the PDPA, and any compensation ordered to be paid by the Controller under section 48O of the PDPA, are direct losses recoverable 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.

13.4 **Order of precedence.** The body of this Addendum prevails over any Schedule unless the Schedule expressly states otherwise. This Addendum prevails over the Principal Agreement in respect of the Processing of Personal Data.

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 is held invalid or unenforceable, the remaining provisions remain in force.

Signed for and on behalf of Tanjong Commerce Pte Ltd

Name: _____

Title: _____

Date: _____

Signed for and on behalf of Northbridge Payments, Inc.

Name: _____

Title: _____

Date: _____

Schedule 1 — Processing details

Item	Description
Subject matter	Acceptance, authorisation, clearing and settlement of card and electronic payments initiated by the Controller's customers; fraud screening and chargeback management.

Item	Description
Duration	The term of the Principal Agreement, plus any retention required by Clause 11.2.
Nature and purpose	Receipt of payment instructions from the Controller's e-commerce and point-of-sale channels; transmission to card schemes and acquiring banks; risk scoring; settlement reporting; dispute handling.
Types of Personal Data	Cardholder name; primary account number (where in scope of the Services); expiry date; tokenised card reference; billing address; shipping address; email address; phone number; device fingerprint; IP address; transaction amount, currency and timestamp; risk signals and decisioning outputs; chargeback correspondence.
Special categories	None expected. The Services are not configured to capture data revealing health, religion, political views or other sensitive categories.
Categories of data subjects	Customers and prospective customers of the Controller; named cardholders on payment instruments used in transactions with the Controller.

Schedule 2 — Technical and organisational measures

1. Hosting and segregation. The production environment is hosted in geographically distributed regions in the United States operated by a Tier 1 hyperscale cloud provider. Customer data is logically segregated by tenant identifier.

2. Cardholder Data handling. Cardholder Data is captured directly into the Processor's hosted payment fields or via point-to-point encryption from certified terminals, and is tokenised at the point of receipt. The Controller does not receive, store, process or transmit primary account numbers in clear text.

3. Encryption. Personal Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 with keys managed in a FIPS 140-2 Level 3 hardware security module. Primary account numbers are stored only in a dedicated cardholder data vault.

4. Access control. Access to production systems is restricted to authorised personnel on a least-privilege, need-to-know basis, requires multi-factor authentication, is logged and is reviewed quarterly.

5. Network security. Production systems are deployed behind managed web application firewalls and intrusion detection, with network segmentation enforced between application, vault, settlement and management tiers.

6. Vulnerability management. Continuous dependency scanning, quarterly internal ASV scans, monthly internal vulnerability scans, and a PCI-compliant annual external penetration test conducted by a CREST-accredited or PCI QSA-accredited tester.

7. Logging and monitoring. Application, system, and security logs are retained for not less than twelve (12) months in a tamper-evident store, with twenty-four-by-seven security monitoring.

8. Personnel. Background screening to the extent permitted by law, mandatory annual security and data protection training, written confidentiality obligations that survive termination.

9. Business continuity. Multi-region active-active deployment with documented recovery time and recovery point objectives, tested at least annually.

10. Certifications. PCI DSS Level 1 service provider certification; SOC 2 Type II; ISO/IEC 27001.

Schedule 3 — Approved Sub-processors

Sub-processor	Function	Location of Processing
Western Cloud Services LLC	Production cloud infrastructure	United States (multi-region)
Atlantic Settlement Systems Inc.	Acquiring bank settlement and reconciliation	United States
Pacific Fraud Signals Inc.	Network fraud and device-intelligence signals	United States
Lion City Settlement Partners Pte Ltd	SGD settlement and local-rail payouts	Singapore
Beacon Communications Inc.	Transactional email delivery	United States

Schedule 4 — Cross-border transfer mechanism

1. Recipient jurisdictions. Personal Data is Processed in:

(a) the United States, by the Processor and its Sub-processors listed in Schedule 3;

(b) Singapore, by the Sub-processor responsible for SGD settlement and by the Processor's regional support function; and

(c) such other countries as may be required for card-network routing (typically the Asia-Pacific switching nodes of Visa, Mastercard and American Express).

2. Safeguard mechanism. The Parties rely on contractual safeguards under the Transfer Limitation Obligation, comprising:

(a) the obligations in Clauses 3 to 11 of this Addendum;

(b) the technical and organisational measures in Schedule 2;

(c) the Processor's PCI DSS Level 1 and SOC 2 Type II programmes; and

(d) Sub-processor flow-down terms required under Clause 6.4 that bind each Sub-processor to a comparable standard of protection.

3. Transfer impact considerations. The Processor confirms that it has assessed the laws of the United States that may affect the Personal Data, including lawful access by public authorities, and has determined that, taking into account (i) the nature and sensitivity of the Personal Data (predominantly tokenised payment data with limited identifying fields), (ii) the existence of US contractual and statutory protections available to data subjects, and (iii) the additional safeguards in this Addendum, the Personal Data will receive a comparable standard of protection.

4. Onward transfers. Onward transfers by Sub-processors are permitted only:

(a) to entities bound by contractual terms imposing a comparable standard of protection;

(b) where required for card-scheme operation or by law; or

(c) with the prior written consent of the Controller.

5. Review. The Parties shall review this Schedule 4 at least every twenty-four (24) months, and earlier if either Party reasonably believes that the laws of any recipient jurisdiction have materially changed.