SMB Solutions Cloud Services

Data Processing Agreement (DPA)

Australia · New Zealand

Parties to this Agreement

Processor	SMB Solutions Cloud Services Pty Ltd ABN 50 625 203 787 Brisbane, Queensland, Australia
Controller	[Client Legal Name] | [ABN/Registration Number] | [Registered Address]
MSA Reference	[Master Services Agreement dated _____]
Effective Date	[_____ / _____ / 20___]

Schedules in Force

The parties agree that the following Schedules form part of this Agreement. Mark each Schedule that applies and initial to confirm:

Apply?	Schedule	Initials
☐ Yes ☐ No	**Schedule A** — Australian Privacy Act 1988 (Cth) & Australian Privacy Principles (2014)	Processor: _____ Controller: _____
☐ Yes ☐ No	**Schedule B** — New Zealand Privacy Act 2020	Processor: _____ Controller: _____

Agreement Execution

By signing below, the parties agree to be bound by the terms of this **Data Processing Agreement**, including all applicable Schedules selected above.

PROCESSOR
SMB Solutions Cloud Services Pty Ltd

_____
Signed

_____
Name

_____
Title

_____
Date

CONTROLLER (CLIENT)
[Client Legal Name]

_____
Signed

_____
Name

_____
Title

_____
Date

Core Agreement

Obligations applicable to all engagements regardless of jurisdiction

1 Definitions and Interpretation

In this Agreement, unless the context requires otherwise:

Agreement	This Data Processing Agreement together with the cover page, all applicable Schedules, and all Annexures.
Controller	The Client, being the entity that determines the purposes and means of processing Personal Data.
Processor	SMB Solutions Cloud Services Pty Ltd, processing Personal Data on behalf of the Controller.
Personal Data / Personal Information	Any information relating to an identified or identifiable natural person, as defined under the Applicable Privacy Law.
Processing	Any operation performed on Personal Data, including collection, storage, use, disclosure, and destruction.
Applicable Privacy Law	The privacy or data protection legislation applicable to the Controller or the data subjects, as identified in the relevant Schedule(s) selected on the cover page.
Data Breach	Any unauthorised access to, or disclosure, loss, or destruction of, Personal Data processed under this Agreement.
Sub-processor	Any third party engaged by the Processor to process Personal Data on the Controller's behalf.
Services	The cloud hosting, managed IT services, and SAP Business One services described in the MSA.
MSA	The Master Services Agreement between the parties, as referenced on the cover page.

2 Scope and Purpose

2.1 Application

This Agreement applies wherever the Processor processes Personal Data in the course of providing the Services to the Controller. It operates as an addendum to the MSA and does not replace any obligation under the MSA except to the extent of any inconsistency, in which case this Agreement prevails.

2.2 Processor Role

The Processor acts solely as a Processor in respect of Personal Data processed under this Agreement. The Processor does not determine the purposes or means of processing and acts only on the documented instructions of the Controller. If the Processor processes Personal Data other than in accordance with the Controller's documented instructions, the Processor acknowledges that it may be directly responsible for that processing under Applicable Privacy Law.

2.3 Governing Law

This Agreement is governed by the laws of Queensland, Australia. The parties submit to the non-exclusive jurisdiction of the courts of Queensland, save that where a Schedule requires compliance with the laws of another jurisdiction, the provisions of that Schedule shall be construed in accordance with the relevant law.

3 Processing Instructions

3.1 Documented Instructions

The Processor shall process Personal Data only on the documented instructions of the Controller, including as set out in Annexure 1 (Processing Details) and any subsequent written instructions. Annexure 1 is the Controller's primary documented instruction and specifies the purposes for which the Processor may process Personal Data. A request or change made by an Authorised Contact through the Processor's support system (currently HubSpot Service Hub), or by email to the Processor's support address, is a written instruction for the purposes of this Agreement. The Processor shall keep a record of written instructions for the term of this Agreement and for 7 years afterwards. The terms of the MSA apply as instructions only to the extent they are consistent with Annexure 1.

3.2 Notification of Conflicting Instructions

If the Processor reasonably considers that an instruction would breach any Applicable Privacy Law, it shall promptly notify the Controller. The Processor may suspend processing of the affected data until the parties agree a lawful approach.

3.3 Change of Purpose

The Processor shall not process Personal Data for any purpose other than the Permitted Purpose set out in Annexure 1 without the prior written consent of the Controller.

3.4 Authorised Contacts and Partners

The Controller shall nominate in Annexure 1 the individuals authorised to give instructions on its behalf (Authorised Contacts) and shall notify the Processor in writing of any change. Where the Controller has engaged an SAP Business One partner, that partner may give instructions only as an Authorised Contact of the Controller. The Controller remains the controller of the Personal Data, executes this Agreement directly with the Processor, and is responsible for instructions given by its Authorised Contacts. The Processor may decline to act on an instruction it reasonably believes has not been authorised by the Controller.

4 Confidentiality

4.1 The Processor shall ensure that all personnel authorised to process Personal Data are subject to binding confidentiality obligations and receive appropriate data protection training. This obligation survives termination of this Agreement.

5 Security

5.1 Technical and Organisational Measures

The Processor shall implement and maintain appropriate technical and organisational security measures to protect Personal Data against unauthorised access, loss, destruction, or disclosure. These measures shall at a minimum include:

- Encryption of Personal Data in transit and at rest
- Multi-factor authentication for systems containing Personal Data
- Role-based access controls and least-privilege principles
- Regular vulnerability assessments and penetration testing
- Security incident management procedures
- Business continuity and disaster recovery arrangements

5.2 Certification

The Processor maintains ISO/IEC 27001 certification and SOC 2 Type II attestation. Current certificates and reports are available to the Controller on request and shall be treated as confidential.

5.3 Security Reviews

The Processor shall review and update its security measures at least annually or following any material change to the Services or threat environment.

6 Sub-processors

6.1 Approval

The Processor shall not engage a new Sub-processor or materially change the role of an existing Sub-processor without providing the Controller at least 30 days' prior written notice. The Controller may object to any proposed Sub-processor on reasonable grounds within that period.

6.2 Obligations

Where a Sub-processor is engaged, the Processor shall impose data protection obligations on the Sub-processor that are no less protective than those in this Agreement. The Processor remains liable to the Controller for the acts and omissions of its Sub-processors. The Processor shall pass on the Controller's documented instructions to each Sub-processor to the extent relevant to the processing that Sub-processor performs.

6.3 Current Sub-processors

The Processor's current list of Sub-processors is set out in Annexure 2 and shall be updated as changes are approved.

7 Data Breach Response

7.1 Notification to Controller

Upon becoming aware of a Data Breach that may affect Personal Data processed under this Agreement, the Processor shall notify the Controller without undue delay and in any event within 24 hours of becoming aware. The notification shall include, to the extent then known:

- A description of the nature of the breach
- The categories and approximate number of data subjects affected
- The categories and approximate volume of Personal Data affected
- The likely consequences of the breach
- Measures taken or proposed to address the breach

Where full information is not available within that period, the Processor shall give an initial notification with the information then known and provide further information in stages, without undue delay, as it becomes available.

7.2 Cooperation

The Processor shall cooperate fully with the Controller in investigating and remedying the breach, and in meeting any notification obligations under Applicable Privacy Law. Specific notification timelines under each jurisdiction are set out in the relevant Schedule. The Processor shall, as soon as practicable after becoming aware of a Data Breach or suspected Data Breach, take reasonable steps within its control to contain it and to prevent or reduce harm to affected individuals. The Processor shall maintain, and test at least annually, practices, procedures and systems for responding to Data Breaches.

8 Data Subject Rights

8.1 The Processor shall, taking into account the nature of the processing, assist the Controller to respond to requests from data subjects exercising their rights under Applicable Privacy Law (including rights of access, correction, deletion, and portability). The Processor shall forward any such request received directly from a data subject to the Controller within 5 business days.

9 Audit Rights

9.1 The Controller may, on reasonable written notice of at least 20 business days and no more than once per calendar year, audit the Processor's compliance with this Agreement. The Processor may satisfy audit obligations by providing its current ISO 27001 certificate and SOC 2 Type II report in lieu of an on-site audit. Where the Controller has reasonable grounds to suspect a material breach, additional audit rights may be exercised.

10 Data Retention and Return

10.1 Retention

The Processor shall retain Personal Data only for as long as necessary to provide the Services or as required by Applicable Privacy Law or a lawful legal obligation. Retention periods applicable to specific data categories are set out in Annexure 1.

10.2 Return and Deletion on Termination

Upon termination or expiry of the MSA, the Processor shall, at the Controller's election and within 30 days of a written request, either return all Personal Data in a structured, machine-readable format or securely delete or destroy it, and provide written certification of deletion. This obligation does not apply to the extent that the Processor is required to retain data by Applicable Privacy Law.

11 International Data Transfers

11.1 The Processor shall not transfer Personal Data outside Australia, New Zealand, or the UK/EEA (as applicable) without the Controller's prior written consent, except where an applicable Schedule expressly permits a transfer subject to appropriate safeguards. Specific cross-border transfer requirements are set out in the relevant Schedule(s). The Processor shall identify in Annexure 2 any Sub-processor that stores, or can access, Personal Data from outside Australia, and the countries concerned.

12 Liability and Indemnity

12.1 Each party's liability under this Agreement is subject to the limitations and caps set out in the MSA, except to the extent that any liability arises from a party's wilful misconduct, fraud, or breach of obligations under Applicable Privacy Law that cannot be excluded by contract. Nothing in this clause limits the Processor's obligation to cooperate with any regulatory investigation.

13 Term and Termination

13.1 This Agreement commences on the Effective Date and continues for the duration of the MSA. It terminates automatically on expiry or termination of the MSA. Clauses 4 (Confidentiality), 10 (Data Retention and Return), and 14 (General) survive termination.

14 General

14.1 Entire Agreement

This Agreement (together with the MSA) constitutes the entire agreement between the parties regarding the processing of Personal Data and supersedes all prior agreements, representations, or understandings on the same subject matter.

14.2 Amendments

This Agreement may only be amended by written instrument signed by authorised representatives of both parties.

14.3 Severability

If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

14.4 Notices

Notices under this Agreement shall be in writing and delivered by email with read receipt or by registered post to the contact addresses recorded in the MSA.

Annexure 1 – Processing Details

To be completed by the parties at execution and updated as required

Subject Matter	Provision of SAP Business One cloud hosting, managed IT services, and related support as described in the MSA.
Duration	For the term of the MSA, subject to any retention obligations under Applicable Privacy Law.
Nature of Processing	Hosting, storage, backup and restore, disaster recovery, infrastructure and security monitoring (including endpoint and threat detection), patching and upgrades, configuration, support access on request by an Authorised Contact, maintenance, and secure decommissioning of data held within the Client's SAP Business One environment and related systems.
Permitted Purpose	To provide the Services as defined in the MSA. No secondary use or processing for the Processor's own purposes is permitted.
Authorised Contacts	[Insert name, role and email of each individual authorised to give instructions for the Client. Include the SAP Business One partner contact, if any, as an Authorised Contact (clause 3.4).]
Categories of Personal Data	Customer contact details, supplier contact details (if relevant), employee and payroll details (where the Client uses SAP Business One for HR or payroll), and other personal information the Client enters into SAP Business One. [Client to confirm.]
Categories of Data Subjects	Client's employees, customers, contractors, suppliers (as relevant)
Sensitive / Special Category Data	[Insert: Yes / No. If Yes, describe categories and additional safeguards agreed.]
Data Retention Periods	7 years for financial records in accordance with the Corporations Act 2001 (Cth)
Data Hosting Location	Sydney, New South Wales, Australia (primary).

Annexure 2 – Approved Sub-processors

Current as at the Effective Date — updates notified per Clause 6.1

Sub-processor Name	Service Provided	Data Location	Privacy Certification
Equinix Australia	Colocation data centre (production and backup storage)	Australia	ISO 27001 / SOC 2
Sophos	Managed detection and response; endpoint protection	Australia	ISO 27001
Microsoft 365	Email and file storage for support communications	Australia	ISO 27001 / SOC 2
HubSpot	Support ticketing (tickets may contain Personal Data)	Australia	ISO 27001 / SOC 2

Schedule A – Australian Privacy Act 1988 (Cth) & Australian Privacy Principles

Applies where the Controller is an APP entity or processes the Personal Information of individuals in Australia

A.1 Application

This Schedule applies where the Controller is an APP entity within the meaning of the Privacy Act 1988 (Cth) (Privacy Act) or where the Personal Data processed under this Agreement includes the Personal Information of individuals located in Australia. Where this Schedule applies, it supplements and must be read together with the Core Agreement. Where the Controller is not an APP entity (for example, a small business operator), the Processor shall comply with this Schedule as a contractual obligation.

A.2 Australian Privacy Principles

The Processor acknowledges that, to the extent it holds Personal Information on behalf of the Controller, it acts as a processor for the Controller. As an APP entity, the Processor complies directly with APP 1 (open and transparent management of personal information) and APP 11 (security and destruction of personal information). To support the Controller's compliance with the other Australian Privacy Principles (APPs), the Processor shall:

- Process Personal Information only for the purposes specified in the Controller's documented instructions (Annexure 1 and clause 3.1)
- Take reasonable steps to protect Personal Information from misuse, interference, loss, and unauthorised access, modification, or disclosure (APP 11)
- Destroy or de-identify Personal Information when it is no longer needed and no legal obligation requires retention (APP 11.2)
- Not adopt a Government Related Identifier as its own identifier of an individual (APP 9)
- Assist the Controller to give individuals access to their Personal Information and to correct it, in accordance with APPs 12 and 13

The parties acknowledge that, under amendments to the Privacy Act proposed in the Privacy Amendment (Personal Data Protection) Bill 2026, a processor acting in accordance with a controller's instructions documented in writing would be exempt from the APPs other than APP 1 and APP 11, and its acts would be attributed to the controller. On commencement of those amendments, the parties intend that the Processor is a processor and the Controller is a controller for that purpose, and that Annexure 1 and written instructions under clause 3.1 are the Controller's documented instructions.

A.3 Cross-Border Disclosure — APP 8

Before disclosing Personal Information to an overseas recipient, the Processor shall take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information. The parties agree the following cross-border disclosures are authorised under this Agreement:

- Disclosures to Sub-processors listed in Annexure 2, where those Sub-processors are subject to binding obligations equivalent to the APPs

- Disclosures required by a court order or applicable law

The Processor shall not otherwise disclose Personal Information to an overseas recipient without the prior written consent of the Controller, except where the Controller has expressly instructed the Processor to do so and the Controller has satisfied its obligations under APP 8.

A.4 Notifiable Data Breach Scheme

Where a Data Breach occurs involving Personal Information that may give rise to a real risk of serious harm to affected individuals, the Processor shall:

- Notify the Controller within 24 hours of becoming aware of the suspected breach (per Clause 7.1 of the Core Agreement)
- Provide sufficient information to enable the Controller to assess whether the breach is an Eligible Data Breach within the meaning of Part IIIC of the Privacy Act
- Cooperate with the Controller in preparing any statement to be provided to the Office of the Australian Information Commissioner (OAIC) and affected individuals

For the avoidance of doubt, the obligation to notify the OAIC and affected individuals under Part IIIC rests with the Controller as the APP entity. The Processor's obligation is to facilitate that notification by prompt disclosure to the Controller. The Processor shall provide information in time for the Controller to meet any statutory deadline for notifying the OAIC. If the Processor is itself required by law to notify the OAIC of a Data Breach affecting the Controller's Personal Information, it shall, where lawful, consult the Controller first so that the parties' statements are consistent.

Under the Privacy Act at the date of this Agreement, the Controller must assess a suspected breach within 30 days (s 26WH) and notify the OAIC as soon as practicable after forming the belief that an eligible data breach has occurred (s 26WK). Under the proposed amendments, a statement must be given to the OAIC within 72 hours of the entity having reasonable grounds to believe an eligible data breach has occurred.

A.5 Privacy Act Amendments — 2024 and Forward

The parties acknowledge that the Privacy and Other Legislation Amendment Act 2024 (Cth) introduced significant changes commencing from December 2024 and June 2025, including a new statutory tort for serious invasions of privacy and enhanced security and breach reporting obligations. The parties agree to review and update this Schedule within 60 days of any further substantive amendments to the Privacy Act that affect the Services.

A.6 Automated Decision-Making

Where the Services involve substantially automated decision-making using Personal Information that could reasonably be expected to significantly affect the rights or interests of an individual, the Processor shall notify the Controller. From 10 December 2026, the Controller must disclose details of such processing in its privacy policy in accordance with the Privacy Act Amendment Act 2024. The Processor shall provide the Controller with sufficient information about automated processes to enable this disclosure.

A.7 OAIC Investigations

If the OAIC commences an investigation involving Personal Information processed under this Agreement, the Processor shall promptly notify the Controller and cooperate with any investigation, access request, or audit by the OAIC to the extent permitted by law.

Schedule B – New Zealand Privacy Act 2020

Applies where the Controller processes the Personal Information of individuals in New Zealand

B.1 Application

This Schedule applies where the Controller is an agency within the meaning of the Privacy Act 2020 (NZ) or where Personal Data processed under this Agreement includes the Personal Information of individuals located in New Zealand. Where this Schedule applies, it supplements and must be read together with the Core Agreement.

B.2 Information Privacy Principles

The Processor acknowledges that it is an agency under the NZ Privacy Act 2020 to the extent it collects, holds, or uses Personal Information about New Zealand individuals on behalf of the Controller. The Processor shall comply with the Information Privacy Principles (IPPs) as applicable, including:

- Processing Personal Information only for the purpose for which it was obtained or a directly related purpose (IPP 2)
- Retaining Personal Information only as long as is required for the permitted purpose (IPP 9)
- Taking reasonable security safeguards against loss, access, use, modification, or disclosure of Personal Information (IPP 5)
- Making information available for correction on request and attaching a statement of correction where disputed (IPP 7)

B.3 Mandatory Privacy Breach Notification — Privacy Commissioner

The NZ Privacy Act 2020 introduced a mandatory notification regime. Where a privacy breach occurs involving Personal Information of New Zealand individuals and that breach is likely to cause serious harm:

- The Processor shall notify the Controller within 48 hours of becoming aware (per Clause 7.1 of the Core Agreement)
- The Controller, as the agency responsible, must notify the New Zealand Privacy Commissioner and affected individuals as soon as reasonably practicable
- The Processor shall provide all information reasonably required by the Controller to make that notification, including the nature of the breach, data affected, and remediation steps taken

A breach is not required to be notified if the Controller reasonably believes it has taken action to prevent serious harm before notification would otherwise be required.

B.4 Cross-Border Transfers

Personal Information of New Zealand individuals must not be transferred outside New Zealand unless:

- The receiving country or recipient provides comparable safeguards to those under the NZ Privacy Act 2020
- The transfer is authorised by the Controller and the Controller has satisfied its obligations under IPP 12
- The individual has expressly authorised the transfer after being informed of the destination country

The Processor shall not transfer Personal Information of New Zealand individuals to any country or recipient not listed in Annexure 2 without the prior written consent of the Controller.

B.5 New Zealand Privacy Commissioner

If the New Zealand Privacy Commissioner commences an investigation or issues a compliance notice involving Personal Information processed under this Agreement, the Processor shall promptly notify the Controller and cooperate with the investigation to the extent permitted by law.

B.6 Comparison with Australian Obligations

The parties acknowledge that the NZ Privacy Act 2020 is structurally more aligned with the GDPR than the Australian Privacy Act 1988, including its mandatory breach notification obligations and stronger individual rights. Where this Agreement is performed in both jurisdictions, the higher standard applicable to a given processing activity shall prevail.

_____END DOCUMENT_____