
Data Processing Agreement (Australia)

This Data Processing Agreement (DPA) is entered into as of [Date] between:

- **Client:** [Client Legal Name] (ABN/ACN: [●]), of [Client Address] (Client).
- **Service Provider:** emperiuus Pty Ltd ACN:150 410 567 (Service Provider).

This DPA forms part of and is incorporated into the main **Service Agreement / Consulting Agreement** between the parties (the **Agreement**). Capitalised terms not defined here have the meaning given in the Agreement.

Note: Australian law does not formally distinguish "controller/processor" in the same way as GDPR, but this DPA uses those ideas contractually while making clear that both parties must comply with the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs).

---

1. Purpose and Scope

1.1 This DPA sets out the terms on which the Service Provider will handle **Personal Information** on behalf of the Client in connection with the Services under the Agreement.

1.2 The parties acknowledge that:

- The Client is the entity that determines the purposes for which Personal Information is collected and used under the Agreement.
- The Service Provider handles such Personal Information for the limited purpose of providing the Services, in accordance with the Client's instructions and applicable privacy laws.

1.3 This DPA applies to all Personal Information processed by the Service Provider on behalf of the Client, including through AI tools, automation workflows, integrations, and related services.

---

2. Definitions

For the purposes of this DPA:

- **Australian Privacy Law** means the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), as amended from time to time.
- **Personal Information** has the meaning given in the Privacy Act 1988 (Cth) and includes any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.

- **Sensitive Information** has the meaning given in the Privacy Act 1988 (Cth) and includes health information and other categories of sensitive data.
- **Data Breach** means any unauthorised access to, unauthorised disclosure of, or loss of Personal Information that the Service Provider holds, in circumstances where unauthorised access or disclosure is likely to occur (including incidents that may trigger the Notifiable Data Breaches scheme).

---

3. Nature of Processing

3.1 **Subject matter.** The Service Provider will handle Personal Information to provide AI consulting, automation, integration, and related services as described in the Agreement and any applicable Statement/Scope of Work.

3.2 **Types of Personal Information.** Depending on the Client's use of the Services, this may include:

- Contact details (name, email address, phone number, address)
- Customer and lead records (e.g., pet owners, patients, clients)
- Appointment/booking information.
- Communication logs (email, SMS, call records, chat transcripts)
- Transaction or interaction metadata (timestamps, source, tags, campaign data)
- Other categories as described in the relevant Scope of Work or onboarding documents.

3.3 **Data subjects.** Individuals about whom the Client collects Personal Information, which may include the Client's customers, prospective customers, website users, and staff.

3.4 **Duration.** For the term of the Agreement and any additional period during which the Service Provider lawfully retains Personal Information under this DPA.

3.5 **Sensitive Information.** If the Client requires processing of Sensitive Information (e.g., health information in a veterinary, medical, or allied health context), this must be explicitly identified and agreed in writing, with any additional safeguards documented in the Scope of Work or an addendum.

---

4. Roles and Responsibilities

4.1 **Client obligations.** The Client is responsible for:

- Ensuring it has a lawful basis to collect and use Personal Information (including Sensitive Information where applicable).
- Providing appropriate privacy notices and, where required, obtaining consents from individuals.
- Ensuring that its instructions to the Service Provider comply with Australian Privacy Law.

4.2 **Service Provider obligations.** The Service Provider will:

- Handle Personal Information only to provide the Services and in accordance with the Client's documented instructions, this DPA, and Australian Privacy Law.
- Not use Personal Information for its own marketing purposes or disclose it to third parties except as permitted under this DPA, the Agreement, or required by law.

---

5. Instructions and Use of Personal Information

5.1 The Service Provider will only handle Personal Information:

- As necessary to provide the Services described in the Agreement.
- In accordance with the Client's written instructions (including this DPA and any SOW); and
- As required by applicable law (in which case the Service Provider will, where lawful, inform the Client of that requirement).

5.2 If the Service Provider believes any instruction from the Client would breach Australian Privacy Law, it will promptly notify the Client (to the extent legally permitted).

---

6. Security

6.1 The Service Provider will take **reasonable steps** to protect Personal Information from misuse, interference, and loss, and from unauthorised access, modification, or disclosure, consistent with APP 11.

6.2 Security measures may include, as appropriate:

- Access controls and role-based permissions.
- Use of strong authentication and password management.
- Encryption in transit and at rest where supported by the relevant tools.
- Secure configuration and patching of systems.
- Staff training and confidentiality undertakings.

6.3 The Client acknowledges that security measures may rely on the configuration and capabilities of third-party platforms chosen by the Client (e.g., CRM, cloud, AI tools). The Client remains responsible for its own systems and access controls.

---

7. Sub-Processors and Third-Party Services

7.1 The Client authorises the Service Provider to use third-party service providers and tools (Sub-Processors) to deliver the Services, which may include, for example:

- CRM, marketing, and automation tools (e.g., GoHighLevel, n8n, Zapier, Make)
- AI/LLM providers and hosting platforms
- Cloud and infrastructure providers
- Analytics, logging, and monitoring tools

7.2 The Service Provider will:

- Take reasonable steps to ensure Sub-Processors provide protections for Personal Information that are substantially similar to those in this DPA; and
- Remain responsible to the Client for the performance of Sub-Processors in relation to Personal Information handled on the Client's behalf.

7.3 Where the Client requests or requires the use of a specific third-party platform and agrees to its terms, the Client acknowledges and accepts the privacy and security posture of that platform.

---

8. Data Breach Notification

8.1 The Service Provider will notify the Client **without undue delay** after becoming aware of a Data Breach involving Personal Information it processes on the Client's behalf.

8.2 The notification will include:

- A description of the nature of the incident, to the extent known.
- The categories of Personal Information affected, if reasonably identifiable.
- Any initial steps taken or proposed to contain and remediate the incident.

8.3 The parties will cooperate in good faith to investigate, contain, and remediate the Data Breach. Any regulatory notifications or notifications to affected individuals will be the responsibility of the Client, unless otherwise required by law.

8.4 Reasonable assistance by the Service Provider beyond basic notification and initial cooperation may be chargeable at its standard professional rates.

---

9. Assistance with Privacy Requests and Compliance

9.1 Taking into account the nature of the Services, the Service Provider will provide **reasonable assistance** to the Client to:

- Respond to requests from individuals to access, correct, or delete their Personal Information, where such requests relate to data held or managed by the Service Provider.
- Respond to enquiries from the Office of the Australian Information Commissioner (OAIC) or other regulators relating to the Service Provider's handling of Personal Information for the Client.

9.2 The Client remains responsible for managing and responding to privacy requests and complaints from individuals.

---

10. Cross-Border Data Transfers

10.1 The Client acknowledges that some Sub-Processors and third-party platforms used to deliver the Services may store or access Personal Information outside Australia, depending on the Client's chosen tools and configurations.

10.2 The Client:

- Authorises such overseas transfers as reasonably necessary for the Services; and
- Is responsible for ensuring its privacy notices and consents adequately address cross-border disclosures under APP 8, and for any additional contractual or organisational measures it requires.

10.3 Where feasible, the Service Provider will support the Client in selecting tools or configurations that offer Australian or regionally appropriate data locations, if requested by the Client and supported by the relevant vendor.

---

11. Retention, Return and Deletion of Personal Information

11.1 The Service Provider will not retain Personal Information for longer than is reasonably necessary to provide the Services or to meet legal, tax, or audit requirements.

11.2 Upon termination or expiry of the Agreement, or upon the Client's written request, the Service Provider will:

- Delete Personal Information in its possession or control; or
- Return Personal Information to the Client in a commonly used format,

unless the Service Provider is legally required, or has a legitimate interest, to retain certain records (e.g., invoices, contractual documentation).

11.3 The Client is responsible for exporting any data it wishes to retain from third-party tools directly under its control.

---

12. Audits and Information

12.1 On reasonable written request, the Service Provider will provide high-level information about its data protection practices and the Sub-Processors it uses for the Services.

12.2 If the Client reasonably requires a more detailed review (e.g., questionnaire, documented assessment), the parties will negotiate scope and timing in good faith; the Service Provider may charge reasonable fees for time spent on such assessments.

---

13. Conflict and Order of Precedence

13.1 If there is any conflict between this DPA and the Agreement in relation to Personal Information, **this DPA prevails** to the extent of the inconsistency.

13.2 Other terms of the Agreement (including liability and dispute resolution) apply to this DPA.

---

14. Governing Law and Jurisdiction

14.1 This DPA is governed by the laws of **Victoria, Australia**, unless another Australian jurisdiction is specified in the Agreement.

14.2 The parties submit to the exclusive jurisdiction of the courts of that jurisdiction and any courts that may hear appeals from those courts.

---

15. Execution

Signed for and on behalf of **Client**:

Name: _____
Title: _____
Signature: _____
Date: _____

Signed for and on behalf of **[Your Business Name]**:

Name: _____
Title: _____
Signature: _____
Date: _____