# SPOS Group APP Privacy Policy

## 1. Purpose & Scope

This policy outlines our commitment to the **open and transparent management** of personal information (APP 1). It applies to all employees, contractors, and third-party partners.

## 2. Accountability & Governance Structure

- **Data Protection Officer (DPO):** The DPO is responsible for the oversight of this policy and acts as the primary contact for the OAIC (Office of the Australian Information Commissioner).
- **Privacy by Design:** New systems or processes involving new sensitive personal information must undergo a **Privacy Impact Assessment (PIA)** before commencement to identify and mitigate risks.
- **Training:** All staff must complete privacy awareness training annually and upon induction.

## 3. Risk Management & Technical Controls

- **Data Collection:** In accordance with **APP3**, SPOS shall only collect personal information that is reasonably necessary for one or more of our specific functions or activities. We do not collect data based on "future potential utility" or "nice-to-have" insights.
    - Necessity Test:
        - *"If we did not have this specific data point, would we be legally or operationally unable to complete the requested service?"*
    - We will typically collect Name, Address, Email Address and Contact Numbers of customers. We must not collect Date of Birth (DOB), gender, or secondary identification without reasonable reason and customer consent.
- **Data Processing Agreements (DPAs):** We will not share sensitive personal data with third-party vendors without a signed DPA that guarantees compliance with Australian privacy standards.
- **Security (APP 11):** Sensitive data must be encrypted at rest and in transit. Access is granted via the **Principle of Least Privilege (PoLP)**—users only see what they absolutely need to do their jobs.
- **Overseas Disclosure (APP 8):** We do not sell or disclose customer personal information to overseas third parties for their own marketing purposes. However, in the course of our operations, we utilize cloud-based service providers for data storage, email, and business management (such as Odoo and Microsoft). These providers may store or process data on servers located outside of Australia, typically in the **United States, Belgium, and Singapore**.

## 4. Data Lifecycle Management

- **Retention:** Personal information will be destroyed or de-identified once it is no longer needed for its primary purpose unless otherwise required by law.
- **Data Quality (APP 10):** We offer multiple readily available opportunities and methods for our customer to amend and update their data.

## 5. Monitoring & Incident Response

- **Audit Trail:** Access logs are reviewed to detect unauthorized access.
- **Notifiable Data Breaches (NDB):** Any suspected breach must be reported to the DPO immediately. If a breach is likely to result in "serious harm," we will notify the affected individuals and the OAIC within 30 days.
- **CCTV On Site:** We collect personal information via on-site CCTV surveillance at our office and warehouse location in Seven Hills, NSW. This information is collected for the purposes of ensuring the safety of our staff and visitors, protecting our assets, and investigating security incidents or theft. All surveillance is overt, with clear signage displayed at all entries to the premises. Footage is stored securely with restricted access and is typically retained for 30 days before being overwritten.

## 6. Complaints & Redress

- If you believe we have breached the Australian Privacy Principles, you may lodge a complaint with our DPO at admin@sposgroup.com. We will respond within 30 days. If you are unsatisfied with our response, you may take your complaint to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.
- We only use your personal information for direct marketing if you have provided consent. You may opt-out at any time by clicking the 'unsubscribe' link in our emails or contacting our DPO admin@sposgroup.com
- We do not use automated decision-making systems to process your data for the purposes of service eligibility or marketing. You have the right to request information about how these decisions are reached.