PRIVACY CONSIDERATIONS

FOR A SMALL AND MEDIUM-SIZED ENTERPRISE (SME)

For SMEs, understanding and implementing privacy measures can seem daunting. However, it's essential for your business's reputation, customer trust, and regulatory compliance. Here are some practical steps to get started:

Amstelveen

Privacy Considerations

For a Small and Medium-Sized Enterprise

Identification

Personal information includes a broad range of data that can identify someone. Understanding what data is accessible is key to managing it well and preventing unauthorised access.

▶ *How do I know what data my organisation handles?*

Start by listing which data systems and processes handle personally identifiable information (PII), financial records, or proprietary business information. PII can include:

- Residential Address
- Passport Number
- Phone Number
- Drivers License

Classification

By categorising data based on its sensitivity, organisations can implement appropriate security measures, control access, and safeguard personal information. This means sensitive data remains confidential, enhancing privacy compliance.

▶ *How can I organise and prioritise data based on privacy concerns?*

Implement a data classification policy and framework to assist data and process owners in identifying, categorising and prioritising sensitive data. Refer to standards such as ISO/IEC 27001, PCI DSS or NIST 800-53 for requirements and guidance.

Privacy by Design

Privacy by Design (PbD) is integrating privacy protections into the design and development of systems, processes, and technologies from the outset. This promotes transparency, minimises data collection, and empowers individuals to control their personal data.

▶ *How can I actively promote privacy considerations throughout the organisation?*

Conduct Privacy Impact Assessments (PIAs) for new projects or initiatives to enable the consideration of privacy risks and mitigation strategies early in the project life cycle, and continuously update the PIA as the project or initiative evolves.

Amstelveen

Privacy Considerations

For a Small and Medium-Sized Enterprise

Regulatory Compliance

Adhering to privacy regulations helps maintain trust and data security, expands global reach, and provides a competitive edge while safeguarding business reputation. Non-compliance can result in negative consequences such as financial penalties and reputational damage.

▶ *What type of regulatory compliance requirements is my organisation subject to?*

Understand your regulatory compliance requirements based on the type of data your organisation has access to and handles. Some examples include:

- Credit Card Handling: Payment Card Industry Data Security Standard
- Personal Data Handling: The Privacy Act 1988
- Financial Handling: APRA Prudential Standards CPS234 Information Security / CPS230 Operational Risk Management

---

Risk Culture

A strong risk culture helps employees understand the importance of safeguarding PII and adherence to privacy best practices. When organisations prioritise data protection as a core value, it infuses a sense of responsibility and vigilance across all operations, significantly reducing the risk of data mishandling and breaches.

▶ *How can I ensure privacy and data management is effective across the organisation?*

Perform periodic training programs, clearly communicate policies and procedures, and encourage a culture of transparency and accountability.

Whether you are handling customer data, employee records, or intellectual property, privacy must be at the forefront of your business strategy. Contact our team to find out more.

Amstelveen

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.

Amstelveen