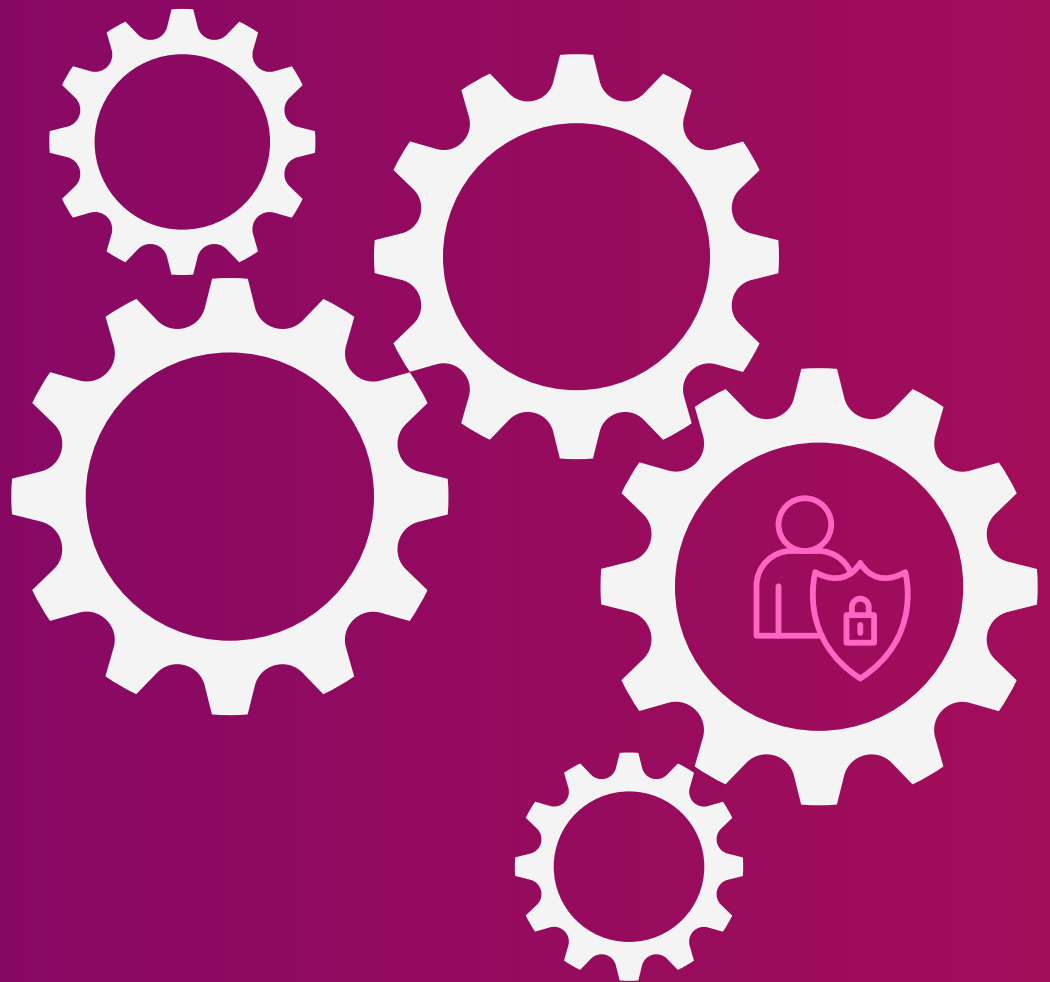




**Privacy108**  
We Protect Privacy

# PRIVACY BY DESIGN: Practical tips to get started



---

Edition 1.0  
June 2025

## Copyright © Privacy 108 Consulting Pty Ltd

Materials developed by Privacy 108 are provided on the basis of a non-exclusive licence for non-commercial use. This document must not be resold, copied, shared, provided, assigned, transferred or licensed in any way to any third party, displayed in a public place, published on the internet or republished in any way without the prior written permission of Privacy 108.

## This document is not legal advice

While prepared to the best of our ability, this document is a general guide only. It does not cover every situation that applies to your organisation, or reflect your organisation's circumstances.

This document is not legal advice, and should not be construed or relied upon as legal advice.

## About Privacy 108

Privacy 108 is a specialist privacy, data governance and information security consultancy. We offer a range of privacy consultancy and legal services. Our team includes some of Australia's leading experts in privacy law and information security.

Learn more at [privacy108.com.au](https://privacy108.com.au)

## About The Author: Siska Lund

Siska is a data privacy, IT and corporate and commercial counsel with an extensive background working at the intersection of business strategy, technology, law and data across a range of industries: healthcare, cloud computing, energy management, insurance, energy and infrastructure.



***Privacy by Design embeds privacy into business processes, ensuring ethical, compliant, and transparent data practices.***

# INTRODUCTION

---

In today's data-fuelled economy, organisations are increasingly looking to leverage their personal information holdings to help drive innovation.

At the same time, organisations also face increasing scrutiny over how they collect, handle and store personal information. Regulators, consumers, and business partners have come to expect transparent, ethical, and legally sound data practices.

Privacy by design (PbD) offers a structured methodology for organisations to tap into the value of personal information while complying with privacy obligations and building and maintaining community trust. At its essence, PbD refers to a proactive approach of embedding privacy into systems, process and technologies from the outset. It ensures that privacy is a fundamental consideration throughout the lifecycle of a product or service, rather than an afterthought.

# INTRODUCTION

---

This guide has been created for organisations and Privacy Officers looking to begin implementing PbD. The objective of this guide is to move beyond theory and provide actionable steps to integrate PbD into common day-to-day business scenarios.

Throughout this guide, you will find:

- An introduction to PbD that lists key drivers and benefits for implementing PbD
- Strategies for implementing PbD when:
  - Developing new products
  - Onboarding a new vendor
  - Carrying out marketing activities
  - Setting up a data warehouse.

Ultimately, implementing PbD is a continuous journey that will evolve alongside technological advancements, regulatory changes, and shifting consumer expectations. Our goal with this guide and at Privacy 108 is to help simplify this journey and help organisations build sustainable, ethical, and legally compliant data practices that support long-term success.

# Table of Contents

Page 4	.....	Understanding Privacy by Design
Page 7	.....	Resourcing Requirements for PbD
Page 8	.....	Developing New Products using PbD
Page 10	.....	Onboarding a New Vendor
Page 12	.....	PbD in Marketing
Page 14	.....	PbD in Data Warehousing
Page 16	.....	Conclusion

# UNDERSTANDING PRIVACY BY DESIGN

---

*Privacy by Design is a key to unlocking the value of personal information.*

## What is PbD?

At its core, implementing PbD requires an organisation to treat privacy with the same importance as functionality. Privacy risks and harms should be proactively addressed and mitigated, before they occur.

## Benefits of PbD

Integrating PbD reduces the likelihood of non-compliance and minimises exposure to data breaches, which can help you maintain customer trust. But, PbD also offers the following strategic benefits for organisations:

- **Driving Cost Efficiencies.**

Addressing privacy gaps reactively—after a breach or regulatory action—is costly and operationally disruptive. Embedding privacy controls from the outset streamlines compliance, reduces risk exposure, and delivers long-term financial savings by avoiding remediation costs and regulatory penalties.

- **Fostering Innovation and Competitive Advantage.**

Organisations with strong privacy foundations can use privacy as a competitive differentiator with an organisation's customers, unlocking new market opportunities.

- **Cross-Border Data Management.**

PbD aligns with Organisation for Economic Co-operation and Development (OECD) privacy principles that are at the core of international privacy regimes such as the General Data Protection Regulation (GDPR). Implementing Pbd helps support an organisation's readiness to engage with international partners and meet multi-jurisdictional privacy requirements.

## There are 7 foundational principles for implementing PbD:

**Proactive not reactive:** Privacy risk mitigation should be preventative, not remedial. Embedding privacy controls—for example, by mandating privacy reviews at the design stage of product development—will help reduce exposure to compliance risks and strengthen stakeholder confidence.

**Privacy by default:** Privacy should require no user intervention—settings must be configured to automatically provide the highest level of protection. For example, consent preferences should be pre-set to opt-out of data sharing unless actively changed by the user.

**Privacy embedded into design:** Privacy must be integral to all systems, services, and business processes. This means incorporating encryption, secure deletion capabilities, and privacy-enhancing technologies at the development stage—not retroactively. Privacy must be an architectural requirement, ensuring compliance and security at scale.

**Positive-sum thinking:** Protecting privacy should not come at the expense of business objectives—both can coexist. Priority should be given to solutions that align privacy protection with commercial success. For instance, de-identification techniques can enable analytics while safeguarding personal information

**End-to-end lifecycle protection:** Data protection must cover the entire information lifecycle, from collection to destruction. Robust security measures should extend to active datasets and archived records alike, ensuring continuous safeguards against misuse, unauthorised access, and non-compliance.

**Transparency and accountability:** An organisation must maintain clear, open communication about its privacy practices to build stakeholder trust. Transparency is not limited to policy documents—it requires demonstrable accountability, such as regular audits, compliance assessments, and independent reviews.

**User-centric privacy experience:** Privacy should be intuitive and accessible, with seamless opt-out mechanisms and straightforward preference management

# Resourcing Requirements for Implementing PbD

How an organisation implements PbD will ultimately depend on a number of factors, such as its size and organisational structure.

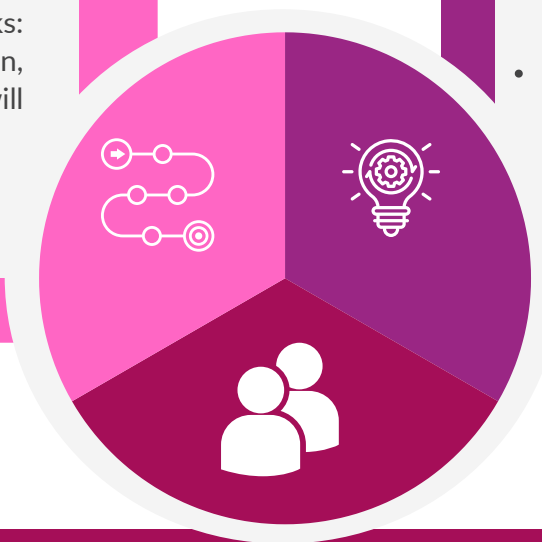
The following are possible resourcing requirements for implementing PbD:

## PROCESS

- Privacy Impact Assessments (PIAs): A standardised process to assess the privacy implications of new initiatives before launch will need to be developed.
- Data Governance Frameworks: Policies for data classification, retention and deletion will usually need to be developed

## TECHNOLOGY

- Privacy-enabling tools: Invest in encryption, anonymisation, and pseudonymization technologies to safeguard personal information. Consent and preference management solutions may also be needed.
- Access controls & authentication: Implement role-based access and multi-factor authentication to protect personal information



## PEOPLE

- Appoint a dedicated Privacy Officer to carry out privacy reviews and advocate for strategic prioritisation.
- PbD will likely require support from legal, IT, data governance, marketing, and risk management teams.
- Ongoing education programs instills a culture of privacy-conscious decision-making across all levels of the organisation.

# DEVELOPING NEW PRODUCTS USING PBD

---

## Why Privacy Matters in Product Development

An organisation's products or services are usually how it interacts with customers and collects personal information. Individuals may be asked to do things like create an account or submit a form to access a service. Embedding PbD into the product development process helps ensure that these products respect user privacy and are compliant with privacy regulations.

## Strategies for Embedding PbD During Product Development

### 1 Conduct a PIA at the Ideation Stage.

Before development begins, assess potential privacy risks and establish mitigation strategies early. Carrying out a PIA at the ideation/design stage of product development can help identify areas where privacy safeguards need to be integrated into the product's design.

### 2 Limit Data Collection to What's Essential

When collecting personal information, adhere to data minimisation principles. Collect only what is necessary to deliver the intended service.

### 3 Enhance User Control Over Consent and Preferences

If the product involves user consent for marketing or other activities, explore technical solutions that allow individuals to update their choices easily. Implementing preference management functionalities empowers users while ensuring regulatory compliance.

### 4 Secure Data Collection, Transmission, and Storage

Consider how personal information will move through the organisation's systems and platforms following collection – including to any third parties. Ensure that collection, transfer, and storage mechanisms follow robust security practices. At the very minimum, encryption technologies should be applied to both data in transit and at rest to mitigate risks of unauthorised access.

## BEST PRACTICE TIP

---

Establish triggers for Privacy Impact Assessments or Privacy Threshold Assessments.

These should be conducted when introducing changes to a product or service.

This will help ensure the product or service's ongoing compliance with privacy regulations.

Plus, it's usually more cost effective and more effective than 'bolt-on' privacy fixes.

# ONBOARDING A NEW VENDOR

---

## Why Privacy Matters When Onboarding a New Vendor

Organisations increasingly rely on third-party vendors to provide a range of services, from managing communications and data storage to event administration. Often, these engagements involve vendors handling personal information on the organisation's behalf. It is important to remember that an organisation cannot outsource its privacy obligations, and that it may be subject to regulatory and/or reputational damage if a vendor mishandles personal information.

## Strategies for Implementing PbD During Onboarding

### 1 Assess Vendor Privacy Posture

Before engaging a vendor, it is critical to evaluate their privacy and security capabilities to identify potential risks. Organisations should conduct thorough due diligence by asking key questions, such as:

- What security measures and controls are in place to protect the organisation's personal information?
- Does the vendor provide privacy training for its staff?
- Has the vendor experienced any privacy incidents that need to be addressed?
- Can the vendor support its attestations by providing copies of key policies and certifications, such as its internal privacy policy, data breach response plan and/or ISO 27001 report?

### 2 Establish Strong Contractual Safeguards.

Once a vendor is selected, appropriate contractual protections must be in place. The contract should address matters such as:

- Roles, responsibilities and expectations regarding privacy compliance
- Permitted uses of personal information
- Security requirements and confidentiality clauses
- How the data will be stored, accessed, transferred and deleted.
- Processes to be followed in the event of a data breach incident
- Audit rights to ensure vendor's compliance with its contractual obligations.

3

### Ongoing vendor oversight and compliance monitoring

Vendor management is not a one-time activity but a continuous process requiring regular oversight. Organisations should implement regular review mechanisms based on the nature of services provided and the sensitivity of the data involved.

Key considerations for ongoing monitoring include:

Assessing vendor performance in meeting privacy requirements.

Reviewing how privacy incidents have been managed and resolved

Considering if agreements need to be updated to reflect new use cases or personal information datasets being handled by the vendor.



## Minimise personal information being shared.

Organisations should implement data minimisation and limit the amount of data being shared with a vendor to what is strictly necessary. This can be an effective way of reducing the inherent risk associated with an outsourcing arrangement.

# PBD IN MARKETING

---

Organisations must carefully consider what personal information is used to target individuals and whether those individuals would reasonably expect their data to be used for marketing purposes.

Additionally, organisations may need to navigate multiple legislative regimes that may apply to marketing activities—in Australia this can include the Privacy Act 1988 (Cth) and the Spam Act 2003 (Cth). Adopting PbD can help ensure that marketing activities are conducted in a privacy-conscious and transparent manner, thereby minimising risks while fostering trust.

## Our Top Tips

### **USE OPT-IN MECHANISMS**

Avoid opt-out consents and ensure individuals can easily update their preferences. This helps engender trust when carrying out marketing activities.

### **USE OF SENSITIVE DATA IS SELDOM APPROPRIATE**

The use of sensitive personal information—such as information about an individual’s health, ethnicity or philosophical beliefs—for marketing will rarely be within their reasonable expectations and will therefore not be appropriate. Organisations should review these use cases carefully and seek legal of privacy advice as appropriate.

*Marketing presents unique challenges in balancing business goals with privacy expectations.*

# Strategies for Implementing PbD: Marketing Department

## **Conducting a PIA**

Before launching a marketing campaign, conduct a PIA. This can help identify privacy risks, relevant privacy obligations, and define appropriate mitigation strategies.

## **Implementing Clear Consent Mechanisms:**

Where possible, provide individuals with the option of opting into receive marketing communications. Explicit consent offers a stronger foundation than relying solely on privacy notices, which may not be thoroughly read by individuals.

## **Minimising Data Collection:**

Limit the collection of personal information to what is strictly necessary for marketing purposes. Whether obtaining data from individuals, third parties, or internal teams, ensure only the minimal amount of personal information is gathered.

## **Ensuring Transparency in Marketing Practices:**

Individuals should be informed about how marketing activities are conducted. Organisations should clearly communicate these processes through privacy policies and notices, ensuring individuals understand how and what personal information is being used for marketing.

## **Safeguarding Personal Information in Analytics:**

Marketing campaigns often rely on analytics tools to segment and target customers. If third-party solutions are being utilised, personal information should be protected through techniques such as anonymisation and aggregation, reducing privacy risks while maintaining utility.

*Embedding privacy into data warehouse architecture will support safe and compliant use of personal information*

# PBD IN DATA WAREHOUSES

---

Data warehouses serve as central repositories that integrate information from multiple source systems, supporting critical functions such as reporting and analytics.

Embedding PbD principles into data warehousing allows organisations to utilise large datasets while safeguarding individual privacy—an approach that reflects the PbD principle of “Positive-sum thinking.”

## Strategies to Implement PbD When Setting Up a Data Warehouse

- 1 Integrate Privacy Requirements into Data Architecture:** Design the data warehouse with built-in privacy controls, ensuring that data anonymisation and pseudonymisation capabilities are in place and applied appropriately to ingested datasets.
- 2 Define Access Controls and Data Permissions:** Establish clear access rights for teams interacting with the data warehouse, and consider whether all teams require access to raw data or only need reporting capabilities. Where access to raw datasets is necessary, ensure that permissions align with operational needs. When setting up reporting capabilities, consider implementing robust aggregation standards so that insights about a specific individual cannot be inferred. Personal information collected with user consent should be restricted to teams directly involved in fulfilling the intended purpose.
- 3 Implement Data Retention and Deletion Policies:** Indefinite retention of personal information introduces unnecessary risks, including increased storage costs and potential inaccuracies in data-driven insights. Develop a structured retention and deletion schedule to manage data lifecycle effectively and implement controls to ensure timely deletion when required.
- 4 Monitor and Audit Data Usage:** Establish robust processes for tracking data access and usage within the warehouse. This includes monitoring activities such as data edits, downloads, and sharing. Any suspicious actions should be promptly investigated, as they may indicate potential data breaches. Proactive monitoring strengthens security and reinforces organisational accountability.

## BEST PRACTICE TIP

---

Organisations should aim to have clarity on the lineage of the personal information stored in a data warehouse.

This includes the personal information's source system and understanding any notices that may have been provided to individuals at the time of the information's collection and the terms of any consent that may have been provided.

Having this information will allow an organisation to easily assess whether proposed uses of the information following ingestion are within the individual's reasonable expectations.

# CONCLUSION

---

## Privacy by Design as a Strategic Mindset

As cyber incidents and data breaches continue to rise, public awareness and scrutiny of data practices have never been higher. Australians are increasingly questioning how their personal information is collected, stored, and shared, prompting regulators – particularly the Office of the Australian Information Commissioner (OAIC) – to strengthen oversight and enforcement. Globally, jurisdictions are expanding privacy regimes and enhancing regulatory powers, underscoring the imperative for organisations to take privacy and data protection seriously.

This guide has introduced key principles of PbD, along with foundational steps that an organisation can consider taking to integrate a privacy-first mindset into everyday business operations. Implementing this guidance and committing to PbD will help organisations build consumer trust, avoid regulatory penalties, and navigate the evolving regulatory landscape with confidence.

If you have any questions about how implementing PbD in your organisation – please reach out. We are here to help.

Reach out for an obligation-free, no-cost consultation with our privacy professionals.

Email [hello@privacy108.com.au](mailto:hello@privacy108.com.au) to get started

# How Privacy 108 Can Help

Privacy 108 has supported organisations across multiple industries implement PbD and set up sustainable privacy practices. We provide practical, legally-informed advice tailored to the unique needs of organisations at different stages of their privacy maturity journey.

## Our services include:

- Developing privacy management programs
- Conducting privacy baseline reviews and data governance (including data minimisation) audits
- Conducting privacy impact assessments
- Providing expert guidance on privacy-related legal matters
- Drafting and enhancing privacy policies and notices
- Implementing privacy by design principles
- Recommending and integrating privacy-enhancing technologies
- Delivering customised privacy training and awareness programs

## You might also like

The following guides are available for free:

[Managing Vendor Privacy Risk](#)

[Privacy Considerations for Marketing Teams](#)

You may also like our Vendor Risk Management Guide. Get your free copy [here](#).

---



**Privacy108**  
We Protect Privacy