PRIVACY BY DESIGN

Purpose of guidance

This resource is designed to provide an overview to Victorian public sector organisations (**organisations**) on Privacy by Design (**PbD**). It discusses the benefits of PbD and the steps an organisation can take to implement it.

What is Privacy by Design?

PbD[1] is an approach to proactively embedding privacy into the design and development of a program that involves any collection, use, or disclosure of personal information. PbD aims to ensure privacy is considered before, at the start of, and throughout the development and implementation of a program.

In this resource, program refers to an organisation's information systems, business processes, practices, services, and the range of projects the organisation undertakes.

Organisations increasingly use digital technologies to understand the public better and achieve better outcomes for them, to improve services for the public, and to find creative solutions to policy issues. Organisations collect, use and disclose significant amounts of personal information to achieve these objectives, consequently it is important that an organisation implements good privacy practices.

There are many benefits to both organisations and the public when PbD principles are considered:

- PbD minimises the privacy risks associated with handling personal information. There is a reduced risk of an organisation breaching its privacy obligations under the *Privacy and Data Protection Act 2014* (**PDP Act**), and any other applicable privacy laws as the organisation proactively identifies the privacy risks associated with a program and takes steps to address them.

- PbD shifts the privacy focus from compliance to prevention as it helps an organisation design, manage, and implement initiatives in a way that respects and protects an individual's privacy rights. Privacy protection is viewed as an asset, not just a compliance measure.

- PbD increases awareness of privacy across an organisation and facilitates cultural change in the way that programs are developed and implemented.

- PbD helps build public trust in an organisation's ability to handle personal information appropriately as it demonstrates that the organisation prioritises privacy and values the personal information it holds.

- PbD can be cost effective as it enables an organisation to identify and address any potential privacy problems early as opposed to retroactively building privacy into programs that already exist. Not only can data breaches have significant financial impacts to an organisation, they can also erode the public's trust in the organisation's information handling practices and affect the organisation's reputation.

Implementing Privacy by Design

There are a range of factors that influence how an organisation implements PbD, including the nature and size of the organisation, the amount of personal information handled by the organisation, and the resources available to the organisation. Importantly, the measures that an organisation implements should be anchored in a respect for individual's personal information.

Steps that an organisation can take to embed a PbD approach across the organisation include:

- Mandating privacy impact assessments (**PIAs**) for programs that involve collection, use and disclosure of personal information. An organisation will find it easier to build privacy into programs once it has identified privacy risks and developed appropriate risk mitigation strategies.[2]

- Consulting the Privacy Officer on all programs that involve handling personal information, or ensuring the Privacy Officer is involved in the development of such programs.

- Ensuring appropriate security measures are implemented throughout the program's lifecycle to protect personal information. For example, for ICT systems, measures could include:

    - Collecting only the minimum amount of information required for the program to avoid risks associated with overcollection of information.

    - Implementing access controls to ensure only the right individuals have access to the information held in the system.

    - Periodically testing the program to ensure privacy and security measures are operating efficiently and ensuring access to the system can be audited.

    - Having a clear process for destroying or de-identifying personal information once it is no longer needed for the program.

- Building a culture of privacy across the organisation:

    - Conducting regular training and awareness sessions on privacy obligations for employees under the PDP Act, and the role they play in ensuring the organisation handles personal information appropriately.

    - Incorporated privacy education into staff induction processes.

    - Ensuring executive and senior management take the lead in promoting good privacy practices.

    - Creating key roles and responsibilities for privacy management, including making a senior staff member with overall accountability for privacy, and appointing a privacy officer to handle privacy queries and complaints.

- Promoting openness and transparency to help build public trust in the organisation's ability to handle personal information appropriately:

    - Having privacy policies that are easily accessible, current, and clearly explain how the organisation manages personal information.

- Providing detailed, easy-to-understand collection notices when collecting personal information from individuals.[3]

PbD enables organisations to approach privacy in productive ways that centre on prevention rather than remediation. It means that privacy concerns are identified and mitigated early and comprehensively in an environment where privacy is not the inevitable loser in a zero-sum game.

The payoff is significant: improved relationships with the public, better satisfaction and trust, support for ICT initiatives, cost savings, reduced legal liabilities and more efficient public sector operations.

PbD sets the scene for a culture of privacy where privacy is woven into the fabric of day-to-day organisational practices such that it becomes a part of business as usual activities that sustain and promote public value.

---

[1] Dr Ann Cavoukian developed the concept of Privacy by Design and the seven foundational principles underpinning the approach.
[2] Detailed guidance on PIAs is available on OVIC's website here: https://ovic.vic.gov.au/privacy/privacy-impact-assessment/.
[3] Detailed guidance on privacy policies and collection notices is available on OVIC's website here: https://ovic.vic.gov.au/privacy/privacy-policies/ and here: https://ovic.vic.gov.au/privacy/collection-notices/.