Fact Sheet May 2020

Privacy by design

Privacy by design ensures that good privacy practices are built into your organisation's decision-making, as well as the design and structure of your information systems, business processes, products and services.

This means that you consider privacy at all stages of initiatives, from conception through to the development and implementation phases. By developing an organisation-wide awareness of privacy, a privacy by design approach shifts the focus to preventing privacy-related issues, rather than simply complying with privacy laws.

Embedding privacy by design into your organisation's practices will also help you to meet community expectations around how public agencies handle personal information.

The key principles

Privacy by design is built around seven key principles[1]:

1. Proactive not reactive, preventative not remedial

Take a proactive approach, anticipating risks and preventing privacy-invasive events before they occur.

2. Privacy as a default setting

Automatically protect personal information in IT systems and business practices as the default.

3. Privacy embedded into design

Embed privacy into the design of any systems, services, products and business practices. You should ensure that privacy becomes one of the core functions of any system or service.

4. Full functionality: positive-sum not zero-sum

Incorporate all legitimate interests and objectives in a 'win-win' manner, not through a 'zero-sum' (either/or) approach. This will avoid unnecessary trade-offs, such as privacy versus security, demonstrating that it is possible to have both.

5. End-to-end security – full lifecycle protection

Put in place strong security measures throughout the 'lifecycle' of the information involved. Process personal information securely and then destroy it securely when you no longer need it.

6. Visibility and transparency – keep it open

Ensure that whatever business practice or technology you use operates according to the stated promises and objectives and is independently verifiable. Make people fully aware of the personal information being collected, and for what purpose.

7. Respect for user privacy – keep it user centric

Keep the interest of individuals paramount in the design and implementation of any system or service. You can do this by offering strong privacy defaults and user-friendly options, as well as ensuring appropriate notice is given.

Privacy by design has become an internationally accepted framework for protecting privacy. It has also been incorporated into Article 25 of the *European Union General Data Protection Regulation* (GDPR), which has made "data protection by design and default" a mandatory requirement in the European Union and the United Kingdom.

NSW privacy legislation

In NSW, the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) continue to provide the overarching privacy framework.

Both the PPIP Act and HRIP Act are principles based and focus on the collecting, holding, using or disclosing of personal and health information. You are obliged to comply with the requirements of these Acts. You may also need to check if there are privacy provisions in other applicable legislation that you need to consider.

How to implement privacy by design

How you implement privacy by design will vary according to the systems you use, the types of projects you undertake, as well as the extent to which you deal with personal information.

[1] Information and Privacy Commissioner of Ontario (2009) Privacy by Design: The 7 Foundational Principles (https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf)

The following general strategies can help to embed a privacy by design approach in your organisation:

- As a matter of course, consider whether a Privacy Impact Assessment is needed when you are starting a new project or making changes to an existing one
- Minimise the amount of personal information that you process: only collect and use what you need for your purposes
- Use and store personal information at the highest possible level of aggregation and with the least possible detail
- If possible, pseudonymise personal information. You should also store personal information from different sources in separate databases, and these databases should not be linked unless this is necessary for your purposes. This will help to prevent an individual's identity being inferred
- Adopt a 'plain language' policy for any public documents so that people easily understand what you are doing with their personal information
- Publish the contact details of the people in your organisation who are responsible for privacy and data protection and link to your Privacy Management Plan
- Create and improve security features in your systems. You may be able to use privacy-enhancing technologies
- Ensure that personal information is automatically protected in your IT systems, services, products and/or business practices, so that individuals do not have to take any specific action to protect their privacy
- When you use other systems, services or products, make sure you only use those whose designers and manufacturers take into account privacy considerations. You should consider whether the contracts with these parties include a requirement for the third party to comply with the PPIP Act and/or HRIP Act.

Privacy Impact Assessments (PIA)

A PIA helps to identify and minimise the privacy risks of changes to services or policies and new projects. A PIA is an important privacy by design process that assists compliance with privacy obligations and delivers benefits to organisations.

A PIA should involve an assessment of:

- Positive and adverse privacy impacts including community reaction
- Compliance with privacy and other relevant legislation
- Controls that mitigate any identified risks

The IPC has published a Guide to Privacy Impact Assessments in NSW

A PIA may not always be required for a project. By contrast, privacy by design is a broader concept, as it applies organisationally and requires you to take privacy considerations into account in every aspect of your work.

Privacy enhancing technologies (PET)

In some instances, you may be able to use privacy enhancing technologies to minimise the use of personal information and increase data security. These include tools such as encryption, private search functions in databases and protocols for anonymous communications. PETs can help to reduce privacy risks in your IT systems and to fulfil your obligations under privacy laws.

While PETs have a role to play in protecting privacy, they are often used as an add-on to existing IT systems (rather than as part of the design of the system itself). PETs will be most effective when they are considered as one part of a broader information governance strategy, where other technical and policy measures are also used to ensure the secure handling of personal information throughout an organisation and its systems[2].

Further resources

The UK Information Commissioner's Office is regularly updating its guidance on data protection by design and default under the GDPR. Click here for more information.

While the GDPR does not apply to most NSW public sector agencies, its requirements around data protection by design and default provide useful examples of the ways in which organisations can build privacy protections into the design of their systems and processes.

For more information

If you would like further advice about privacy by design, we encourage you to contact us. Before doing so, we suggest you review our fact sheet, The Role of the Privacy Commissioner: Consulting the IPC on Initiatives and Projects.

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

[2] European Union Agency for Network and Information Security (2014) Privacy and Data Protection by Design- from policy to engineering (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design)