Australian Government
Office of the Australian Information Commissioner

Updated December 2017

Business resource 18: Privacy

Privacy and start-up businesses

If you're establishing a start-up it's vital to understand how you can benefit from good privacy practice, and the obligations that may apply to your business under the *Privacy Act 1988* (Cth) (Privacy Act) now, or in the future.

Why is good privacy practice essential for your start-up?

There are significant reputational and commercial benefits that flow from good privacy practice. In fact, it's increasingly critical to customer trust. When people are confident about how your start-up will handle their personal information, they are more likely to trust the product or service you offer, leading to improved business performance. Similarly, privacy is increasingly acting as a commercial differentiator amongst competitors.

Conversely, there are a number of risks associated with privacy practices that don't meet customer and community expectations. These risks include:

- reputational damage, which can jeopardise funding and scaling
- the need to redesign products, services and processes to retrofit privacy management down the line, which can increase costs and cause delays
- regulatory scrutiny, which can lead to increased compliance obligations
- public sanctions for *breaching the Privacy Act.*

The Privacy Act provides rights to individuals about how their personal information is used and managed. It also places responsibilities on most businesses. If your start-up is a small business (turnover of $3 million or less per annum) the Privacy Act may not apply to you yet. But ask yourself; do you plan for your business to stay small, or to grow?

If you're planning for growth or acquisition, you need to adopt a 'Privacy by Design' approach to your products and services. This means building the management of privacy risks into the design specifications of technologies, business practices and physical infrastructures from the beginning, rather than bolting it on later.

Below are some tips on how you can do this.

What does good privacy practice involve?

Privacy is not about secrecy. It is about being transparent about how you handle personal information and giving individuals confidence that it will be managed securely and appropriately.

> The Australian Privacy Principles (APPs) in the Privacy Act set out the minimum expectations of the community in relation to how you handle their personal information. When your organisation is covered by the Privacy Act, they are also legally binding.

'Personal information' is any information or an opinion about an individual who can be reasonably identified from that information or opinion. Information that might not be personal information by itself can become personal information when it is linked to other available information to identify an individual. This may, depending on context, include a person's name, date of birth, phone number, bank account details or commentary about a person, and, in the age of big data, may also include information like a person's web browsing history or online purchases.

The standards in the APPs are generally framed as requiring businesses to do what is 'reasonable' in the circumstances. This means they are flexible and can be tailored to your particular business model, products and services.

Below are some privacy tips based on aspects of the APPs that are particularly relevant to start-ups. For a summary of all of the APPs you can refer to the OAIC's *APP quick reference tool*; and the *APP guidelines* set out in detail how the OAIC interprets the APPs.

Tips for good privacy practice

Design your products or services to minimise, manage or eliminate privacy risks: Adopting a Privacy by Design approach is the most efficient and effective way to protect privacy. You need to think about privacy from the beginning – it's more costly and burdensome to do it later. See below for further information on Privacy by Design. (See APP 1.2)

Develop a privacy policy and make it publicly available (eg on your website): Being open and transparent about how you handle personal information is essential for consumer trust. The OAIC's *Guide to developing a privacy policy* will assist you to develop a policy. (See APP 1.1)

Collect and retain de-identified data where possible: Consider whether you could collect de-identified information instead of personal information. Personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. It involves removing or altering information that identifies an individual or is reasonably likely to do so (see the OAIC's *De-identification of data and information* business resource for more information).

If you do need to collect information that could identify individuals (e.g. because a law says you have to), minimise the amount you collect to what you actually need for your business, and de-identify or destroy it when you no longer need it. You should also consider the risk that de-identified information will be re-identified if it is going to be integrated with other data sets, or shared with third parties. (See APP 3.2 and APP 11.2)

Get the individual's consent for new uses and sharing of personal information: Only use or disclose personal information for the purpose you collected it, or for a related purpose that the individual would expect (See APP 6). If you want to use personal information you have collected for an unrelated purpose, it's best practice to get the individual's consent or de-identify the information.

Check the privacy practices of third parties with which you share personal information: If a third party mishandles data you gave it, you may still bear the commercial and reputational damage. Before sharing data, make sure your commercial arrangements (such as a contract) cover how personal information will be handled. This is particularly important if the third party is located offshore. (See APP 8 and the OAIC's *Sending personal information overseas* business resource for more information).

Collect personal information directly: Collect information lawfully and fairly. Collect information and any consent you need directly from the individual, unless it is unreasonable or impractical to do so. (See APPs 3.5, 3.6)

Notify individuals when you collect their personal information: When you collect personal information about individuals, notify them or make them aware of the collection (ideally beforehand). Notification should include how and why the information is collected, and who the information may be disclosed to. (See APP 5)

Protect the personal information you hold: Analyse the potential physical and digital threats to the security of the personal information you hold, and take steps to mitigate these threats. This may include (but is not limited to) implementing software and network security, access controls, and password management. (See APP 11). Human error is a large source of security breaches so you also need to ensure your staff are adequately trained. The OAIC's *Guide to securing personal information* contains further guidance on protecting personal information.

Be prepared for a data breach: Once your products or services go live, have a data breach response plan in place. Where there is a risk of serious harm to the people whose personal information has been compromised, consider notifying affected individuals and the OAIC. The OAIC's *Guide to developing a data breach response plan* will help you develop a data breach response plan.

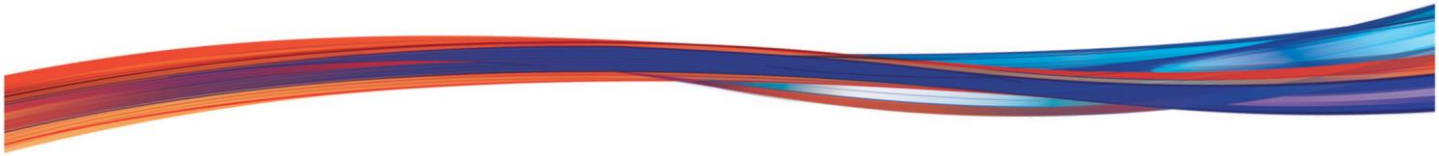
Practice good privacy governance: Implement operational practices and procedures that support your privacy policies. The OAIC's *Privacy management framework* provides advice on how businesses can implement good privacy practices in their day-to-day operations. (See APP 1.2)

Privacy by Design

Privacy by Design is a process for embedding good privacy practices into the design specifications of technologies, business practices and physical infrastructures. That means building in privacy up front – right into the design specifications and architecture of new systems and processes. It is more effective and efficient to manage privacy risks proactively, rather than to retrospectively alter a product or service to address privacy issues that come to light.

In order to build privacy in, you need to understand the privacy impacts. Privacy impact assessments (PIAs) are the best way to do this. A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating those impacts. Completing a PIA can be straightforward – the important thing is to turn your mind to the privacy risks.

Each PIA will vary depending on the nature and extent of personal information that is involved in a project. However, there are some general principles that consistently apply to PIAs:



- A PIA is not just a basic compliance check – it also needs to consider the privacy risks and mitigation strategies for a project.
- A PIA should be done at a stage that is early enough for it to influence how the project proceeds (e.g. at the planning and design or business case stage).
- A PIA should evolve with a project. Effective PIAs will contemplate privacy risks that might arise if a project expands in scale or scope. When the project changes, the PIA should be revisited and updated.
- A PIA should incorporate feedback on privacy risks from stakeholders that might be interested or affected by a project.
- A PIA will map how information is collected as part of a project, and once it is collected, how the information will flow (who can access it, how it will be stored, what it will be used for, etc.).
- Using the information flow map, a PIA should identify any privacy issues and suggest ways that the privacy risks can be managed, minimised or eliminated.

The OAIC's *Guide to undertaking privacy impact assessments* will assist you in undertaking a PIA.

Start-ups and the Privacy Act

For some start-ups privacy issues also pose the risk of non-compliance with the Privacy Act. Whether a start-up is legally required to comply with the APPs and the Privacy Act will depend on the type and scale of its business.

The Privacy Act will generally apply to a start-up once its annual turnover is greater than $3 million.

However, start-ups that undertake the following activities will also need to comply with the Privacy Act:

- collect Know Your Customer information in order to comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. See the OAIC's AML/CTF privacy resource for more info
- participate in Australia's credit reporting system, for example by providing consumer credit reports or exchanging data with a credit bureau. See the OAIC's credit reporting fact sheets for more info
- provide health services, such as a product/service that tracks and holds health data. See the OAIC's series of resources for health service providers for more information.

More detailed guidance on whether the Privacy Act applies to a particular start-up is available in the OAIC's *Privacy Business Resource 10: Does my small business need to comply with the Privacy Act?*

It is important to remember that whether or not the Privacy Act applies to your start-up can change over time, especially if your business grows. Even if your start-up is not required to comply with the Privacy Act now, it may need to in the future.

For example:

- an app developer might not collect personal information as part of the initial version of an app, but builds this capability into an update of the app and then sells the information collected
- your start-up might be acquired by a larger organisation that passes the $3 million annual turnover threshold

- your start-up might scale its business and pass the $3 million annual turnover threshold.

Practising Privacy by Design is the best way to 'future proof' yourself from additional costs and redevelopment work that will be necessary once your business attracts these legal obligations.

The Commissioner has various regulatory powers to ensure compliance with the Privacy Act, including seeking a civil penalty of up to $2.1 million for serious or repeated breaches. The OAIC will also generally make public any regulatory action it has taken.

Other laws that might apply to your start-up

There are also other privacy-related legal requirements outside of the Privacy Act that may apply depending on your start-up's business practices:

- the Telecommunications Consumer Protection Code, if your start-up is a telecommunications provider
- the Spam Act and the Do Not Call Register Act, if your start-up markets to customers directly. See the OAIC's Spam Act business resource for more info on when these laws apply
- the Payment Card Industry Data Security Standard, if your start-up accepts, transmits or stores data from your customers' payment cards.

If your start-up operates or transacts with customers overseas, then you may also need to comply with laws in those jurisdictions. While some jurisdictions have similar laws, they may impose additional obligations. For example, the EU General Data Protection Regulation is due to commence in 2018 and will make PIAs compulsory in some circumstances, and require organisations to notify data breaches.

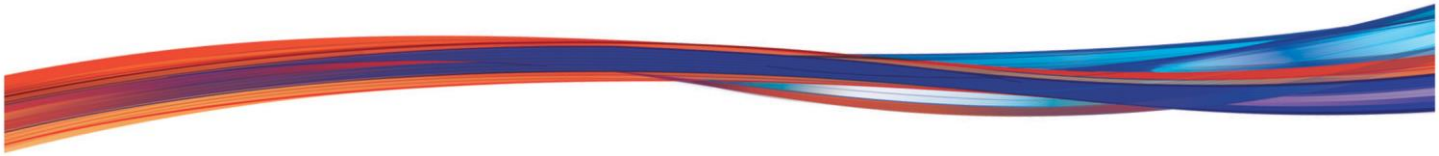
Additional resources

In addition to those already mentioned, the OAIC has a range of other privacy resources that help you comply with the APPs. The *Mobile privacy: a better practice guide for mobile app developers* may be particularly relevant for start-ups that intend to use a mobile app.

You can subscribe to the OAIC's newsletter, OAICnet, which provides news about the OAIC's activities, publications and other information.

In addition to the OAIC's *Guide to securing personal information*, you may find the following resources on information security useful:

- the Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Intrusions*, which provides guidance on protecting government and business networks from cyber attacks
- the Computer Emergency Response Team (CERT) Australia, which is a government agency that provides cyber security advice and support to small businesses
- the list of cyber security firms that are accredited by the Council of Registered Ethical Security Testers (CREST) when you are preventing or responding to information security breaches
- the United States Federal Trade Commission's Start with Security guidance, which includes guidance and lessons learned from law enforcement actions the FTC has taken in the US.



For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

Or visit our website www.oaic.gov.au