

# Commercial Insights

## Privacy Awareness Week 2023

Over the past 12 months we have observed a seismic shift in the focus on the privacy landscape in Australia and across the globe, with several high profile and large scale data breaches shining a spotlight on how individuals, business and governments treat and store personal information. Privacy is at the forefront of individuals' minds. It is an opportune time to remind organisations to continue to review their privacy practices and ensure that appropriate controls and measures are in place to protect the personal information with which they have been entrusted.

With the plethora of information available on data protection, privacy policies and technological protections, it can be overwhelming as a business owner to know how to protect the personal information that your entity collects, uses, discloses and holds. The theme of the 2023 Privacy Awareness Week is '**Privacy 101: Back to Basics**', a fitting theme in today's increasingly digital world. In many ways, privacy practices have failed to keep up with the pace of technology which has exposed extraordinary challenges in protecting individuals' privacy. The Back to Basics theme reminds us that despite the rapid growth and expansion of the digital world, the fundamentals of privacy have not changed and it is important not to lose sight of the basics in protecting personal information.

The Australian privacy regulator and facilitator of Privacy Awareness Week, the Office of the Australian Information Commissioner (**OAIC**), has provided the following tips for businesses to ensure that the personal information they collect, handle and store is kept safe and secure:

1. **Know your obligations** – it is vital to understand your organisation's privacy obligations and to ensure privacy is closely considered as your business systems and practices evolve. Privacy should not be a 'tick box exercise'. Instead it is an integral element that needs to be thoroughly considered at the inception of a project and at regular intervals. It is also important to understand the permissions you have received from customers for using their data and how they expect you to handle their personal information. This is integral to building trust with your customers.
2. **Have a privacy plan** – one of the best ways to develop a culture of privacy in your business is to have a privacy management plan in place and to establish robust privacy practices. This will ensure you set, achieve and regularly review your privacy practices, while also keeping compliant with your privacy obligations and meeting community expectations.
3. **Appoint privacy champions** – assigning a senior staff member to have overall responsibility for privacy is another key ingredient to developing a culture of privacy in an organisation, from the top down. Good privacy governance and leadership demonstrates a commitment to protecting personal information. It

is also important to appoint day-to-day managers of privacy matters and set out clear reporting lines and transparency so that senior management are regularly informed of any potential privacy issues.

4. **Assess privacy risks** – mitigating privacy risks is much easier than responding to an actual or suspected data breach. It is key to plan and assess early. Undertake privacy impact assessments for new projects to identify privacy impacts on individuals, especially when the project involves new technology, information handling pathways or systems.
5. **Only collect or keep the personal information that you need** – only collect the personal information that is reasonably necessary to carry out your business functions or activities. It is equally important to destroy or de-identify information that is no longer needed for the purposes for which it was collected. Over-collection and prolonged storage of unnecessary personal information increases the risk of a data breach and can undermine customers' trust.
6. **Secure personal information** – ensure secure systems are in place to protect personal information from misuse, loss and unauthorised access or disclosure. Failure to have adequate protections means that your business is not complying with its privacy obligations, and may result in financial or reputational loss for your business and customers.
7. **Simplify your privacy policy** – the main reason consumers do not read privacy policies is because often they are too long and complex. Make sure your privacy policy is written in plain English, is easy to understand, and reflects your current privacy practices.
8. **Train your staff** – your employees should understand the expectations around handling personal information in their roles and not just by reference to general principles. Privacy training should be tailored to your organisation and form part of inductions for new staff, service providers and contractors, with refreshers held at regular intervals.
9. **Prepare for data breaches** – have a clear and practical data breach response plan in place so that staff know what to do if a suspected data breach arises. Time is of the essence in investigating and responding, and mitigating any loss, in a suspected data breach, so having access to a practical data breach response plan is critical to effectively managing a breach should it occur.
10. **Review your practices** – central to good privacy management is being proactive and planning for future challenges and risks. Privacy related policies, systems and workflow should be continually reviewed and updated to ensure they are fit for purpose and responsive to evolving risks.

All staff, whether employees or contractors, permanent, casual or part-time, share the responsibility of protecting personal information. The principles outlined above are timeless. Bringing the focus back to fundamental basics will help you be a privacy champion and embed a culture of privacy in your organisation.

It is important to note that Privacy law reform is on the way. Ensuring privacy is embedded in the culture of your organisation will make adopting and adhering to any future changes much easier.

Further information on Privacy Awareness Week 2023 and tips on protecting privacy is available [here](#).

This article was written by Special Counsel Hayley Bowman, with the assistance of Solicitor Meg Ryan and Legal Assistant Matt Watson. Meridian Lawyers is experienced in advising clients on their privacy and data security obligations, including managing responses to data breaches and developing privacy training materials. If you have any questions about your current obligations regarding the collection, use, handling or storage, of personal information in Australia or steps you can be taking in advance of the introduction of the revised privacy laws, please contact Special Counsel [Hayley Bowman](mailto:hbowman@meridianlawyers.com.au) or Principal [Mark Fitzgerald](mailto:mfitzgerald@meridianlawyers.com.au).



**Hayley Bowman**

**Special Counsel**

+61 3 9810 6723

[hbowman@meridianlawyers.com.au](mailto:hbowman@meridianlawyers.com.au)



**Mark Fitzgerald**

**Principal**

+61 3 9810 6767

[mfitzgerald@meridianlawyers.com.au](mailto:mfitzgerald@meridianlawyers.com.au)

Disclaimer: This information is current as of April 2023. This article does not constitute legal advice and does not give rise to any solicitor/client relationship between Meridian Lawyers and the reader. Professional legal advice should be sought before acting or relying upon the content of this article.