DATA AND CYBER SECURITY FOR LAW PRACTICES

Document last updated on 10 November 2025

Knowing how to safely handle and store data is more important than ever in our rapidly growing information economy. This is all the more true for law practices who hold large amounts of personal information about clients and others, such as in the form of passports, driver's licences and bank account details, which may be accessible electronically.

Solicitors have a duty to their clients to maintain the confidentiality of client information. But what does this mean for law practices providing legal services in a context of continually changing and emerging technologies? The Law Society and Lawcover provide the following outline of solicitors' obligations with respect to collecting and handling personal information and mitigating cyber risk.

HOW DO I SAFEGUARD THE DATA MY LAW PRACTICE COLLECTS AND HOLDS?

Having good data management systems and processes can protect you and your clients' personal information from unauthorised access, disclosure and loss.

The Law Society and Lawcover have developed resources to assist law practices in this regard: https://www.lawsociety.com.au/professional-development/cyber-security-resources.

Solicitors can also refer to Lawcover's extensive library of resources on their website: https://www.lawcover.com.au/cyber-resources/.

WHAT SHOULD I DO IF I FALL VICTIM TO A CYBERCRIME EVENT?

Good data security management includes having a clear policy and procedure for reporting data breaches. If your law practice is targeted by cybercrime, you should:

1. Call 1800 BREACH (1800 273 224) or email lawcyber@cbp.com.au.
2. If the cybercrime relates to trust money, report the incident to the Law Society's Trust Accounts Department by emailing tad@lawsociety.com.au, who can then guide you further about the appropriate steps to take to mitigate risk.
3. Where applicable, comply with your obligations to notify an 'eligible data breach' under the *Privacy Act 1988* (Cth) (**the Privacy Act**). This is discussed further below.
4. Report the incident to www.cyber.gov.au/report and 'iDcare'.

WHAT OBLIGATIONS DO LAW PRACTICES HAVE IN COLLECTING AND HOLDING 'PERSONAL INFORMATION'?

OBLIGATIONS UNDER LEGAL PROFESSION LEGISLATION

All legal practitioners in NSW have a duty not to disclose any information that is confidential to a client unless otherwise permitted by the Legal Profession Uniform Law Australian Solicitors' Conduct Rules (**the Conduct Rules**) [rule 9 of the Conduct Rules].

OBLIGATIONS UNDER THE *PRIVACY ACT 1988* (CTH)

Some law practices may have additional obligations in the collection and handling of clients' personal information, prescribed by the Privacy Act 1988 (Cth) (the Privacy Act). For those law practices where obligations under the Privacy Act apply, care should be taken to ensure that any personal information it collects and holds, whether of a client or third party, is protected from unauthorised access, disclosure and loss. It is important to note that obligations under the Privacy Act apply irrespective of whether personal information is confidential information (i.e., whether the personal information is publicly available information). If your law practice has obligations under the Privacy Act, then it must ensure that any personal information it collects and holds is protected from unauthorised access and disclosure, and loss.

The scope and application of the Privacy Act is discussed below.

The Privacy Act

Regardless of size or structure, law practices to which any of the following conditions apply, which may include sole practitioners, law firms and incorporated legal practices, have responsibilities under the Privacy Act.

- Have an annual turnover in excess of $3 million
- Are a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**AML/CTF Act**), in which case the Privacy Act will apply from 1 July 2026*
- Hold tax file numbers (**TFN**) of individuals
- Hold health information about an individual and are deemed to be providing a 'health service'

See sections 6, 6C, 6D and 6E of the Privacy Act and the *AML/CTF Act*.

What types of 'personal information' is regulated by the Privacy Act?

'Personal information' is broadly defined in the Privacy Act. It is information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Common examples of personal information collected by law practices include a person's name, signature, home address, email address, telephone number, date of birth, bank account details, tax file number, medical records and employment details. File notes written about a client, or information contained in an email chain could also be deemed personal information, as the definition under the Privacy Act includes an opinion about an identified individual or an individual who is reasonably identifiable.

The handling of an employee's personal information is exempt from the Privacy Act if it is directly related to the employee's current or former employment relationship (i.e., if the employee's personal information is part of their 'employee record' – see definition in s6 of the Privacy Act). The Privacy Act only applies to an employee record if the information is used for a purpose not directly related to the employment relationship.

Where applicable, what obligations do law practices have under the Privacy Act?

The Australian Privacy Principles

Law practices that have an annual turnover in excess of $3 million are considered 'APP entities' under the Privacy Act, and all APP entities must comply with the requirements of the Australian Privacy Principles (see section 15 of the Privacy Act).

The Australian Privacy Principles (**APP**) are a set of legally binding principles which set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

There are 13 APPs, and they are categorised under five key sections:

Part 1 – Consideration of personal information privacy

- APP 1 – Open and transparent management of personal information
- APP2 – Anonymity and pseudonymity

Part 2 – Collection of personal information

- APP 3 – Collection of solicited personal information
- APP 4 – Dealing with unsolicited information
- APP 5 – Notification of the collection of personal information

Part 3 – Dealing with personal information

- APP 6 – Use or disclosure of personal information
- APP 7 – Direct marketing
- APP 8 – Cross-border disclosure of personal information
- APP 9 – Adoption, use or disclosure of government related identifiers

Part 4 – Integrity of personal information

- APP 10 – Quality of personal information
- APP 11 – Security of personal information

Part 5 – Access to, and correction of, personal information

- APP 12 – Access to personal information
- APP 13 – Correction of personal information

The APP guidelines published by the Office of the Australian Information Commissioner (**OAIC**) outline the mandatory requirements of the APPs, how the OAIC interprets the APPs, and matters the OAIC may take into account when exercising its functions and powers under the Privacy Act.

File number recipients

Irrespective of whether a law practice is an APP entity, if it collects and holds TFNs of individuals, then it must comply with those parts of the Privacy Act that deal with the handling of tax file number records (see sections 13, 17 and 18 of the Privacy Act).

The Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under s 17 of the Privacy Act regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

MANAGING CYBER RISK

ELIGIBLE DATA BREACH

Law practices with obligations under the Privacy Act must notify affected individuals and the OAIC about an 'eligible data breach'.

An eligible data breach occurs when there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds and which is:

- likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.

Law practices that suspect an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

LAWCOVER GROUP CYBER RISK POLICY

Lawcover purchases a group cyber risk insurance policy for the benefit of its insured law practices. The Lawcover Group Cyber risk policy provides crisis assistance and protection from losses to a limit of $50,000.

This policy has been tailored specifically for law practices and sits adjacent to the Lawcover professional indemnity insurance policy.

This policy is available for all insured law practices.

EDUCATIONAL RESOURCES

Practitioners seeking to learn more or update their knowledge on Australian privacy laws and cyber risk management can do so by enrolling in the Law Society's Australian Privacy Principles module and Cyber risk masterclass. Courses are available through LawInform and count towards solicitors' CPD requirements.