YPOL LAWYERS

PRIVACY POLICY

Approved by YPOL Pty Limited's Board of Directors
Date: **April 2024**

Table of Contents

PRIVACY POLICY

We recognise the importance of privacy to our clients and are committed to protecting your personal information. We are subject to the *Privacy Act* 1988 (Cth) and to professional obligations regarding confidentiality.

The following is an outline of how we collect, hold, use and disclose personal information. This document also outlines what constitutes a data breach and what action YPOL will take to identify, report and review any breaches that may occur.

1. Personal Information

YPOL Lawyers collects and holds personal information from various sources in the ordinary course of fulfilling our duties to the court, our clients and shareholders and through the achievement of its strategy and objectives. This includes collecting and holding personal information pertaining to:

- clients and potential clients;
- suppliers and consultants; and
- applicants for employment.

"Personal Information" is defined in the Privacy Act 1988 (Cth) as information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

The main types of personal information we collect may include:

- Names and contact details including phone numbers, postal and/or residential addresses and email addresses;
- Information that can identify you, including date of birth or residence status; drivers licence number, passport details, marital status and photographs;
- any facts or opinions that are connected to an enquiry that we are conducting on behalf of a client or potential client to provide legal services effectively; and
- any other personal information that is provided through a website, mobile application or other on-line platform belonging to Slater and Gordon or as otherwise requested by us or provided by you.

In some cases, you might need to give us personal information about other people – such as when you have an authorised representative. In those situations, we're relying on you to tell those people that you're giving us their details, and to let them know about this Policy. In addition, if you provide us with third party personal information then you warrant to us that you have the third party's consent to do this.

With your permission, sometimes we may also need to collect sensitive information. Sensitive information is a subset of personal information that is given a higher level of protection under the Australian Privacy Principles. Sensitive information includes personal information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices

- criminal record
- biometric information that is to be used for certain purposes
- biometric templates.

The personal information (including sensitive information) collected or held by YPOL Lawyers will be referred to in this policy as "personal information".

2. Collection

We generally collect and hold the following types of personal information:

- Information provided by clients for the purpose of seeking our advice.
- Information about other persons that we collect for the purpose of acting for our clients.

We only collect personal information by lawful and fair means. We also take reasonable steps to ensure the personal information collected is accurate, up-to-date and complete.

Sometimes we may collect personal information about a client that is publicly available – for example, from social media or public registers e.g. Australian Securities and Investments Commission (ASIC), Australian Business Register (ABR).

If we receive personal information from third parties, we will protect it as set out in this policy.

3. Marketing

We use personal information to provide information on legal developments, corporate news or event invitations to clients or contacts. This includes personal information which has been collected from you and would reasonably be expected to be used in direct marketing. If we have collected personal information about you from a third party, it will only be used for direct marketing if you have not opted out of it. Sensitive information will only be disclosed with your consent. We do not purchase marketing lists or sell personal information.

4. Use and disclosure

YPOL Lawyers use the personal information we collect to represent our clients and for related administrative or legal purposes. We may disclose personal information we hold to barristers or experts retained in client matters or to third party contractors engaged to carry out specific tasks such as photocopying or filing of court documents. Reasonable steps are taken to ensure the information which is used or disclosed is relevant, accurate, up-to-date and complete.

If we collect, hold or use personal information in ways other than as stated in this policy, we will ensure we do so pursuant to the requirements of the Privacy Act. YPOL Lawyers retains personal information for as long as it is necessary to fulfil the purposes outlined above and as otherwise specified in applicable record retention policies and procedures. At the conclusion of legal matters, we are required to keep legal files for a minimum period of 7 years from the closure of a legal file unless we are instructed to the contrary. In some cases, we may be required to retain documents for a longer period of time (e.g., documents that inform the making of a Will). We will also retain personal information for the purposes of ongoing legal and regulatory compliance as well as for establishing, exercising or defending legal proceedings.

5 Security

We take reasonable steps to protect personal information that we hold from misuse, interference, loss, unauthorised access, modification or disclosure. YPOL Lawyers operate within a remote hosted working environment. We have two factor authentication when accessing the network and data is encrypted in transit and at rest. Our data is hosted on Microsoft servers located in Australia. Our premises are only accessible via security pass which

is administered by the Office Manager. We take reasonable steps to destroy and de-identify personal information which we no longer require and regularly monitor our information handling practices.

We make all directors and staff aware of their obligations to protect personal information. We take reasonable steps to ensure all directors and staff are compliant with the Australian Privacy Principles and any registered Australian Privacy Principle code we are bound by.

6 Access to Personal Information

Information may be accessed by personnel within YPOL Lawyers. All personnel within YPOL are bound by confidentiality laws and standards that govern the legal profession within Australia and to comply with the Australian Privacy Principles.

In the course of providing legal services and conducting the effective management of our business, disclosure to third party professionals and service providers may occur (e.g., barristers, document reproduction service providers, disbursement funders, IT service providers and debt recovery agents). We have contractual arrangements in place with all of our third-party professionals and service providers to protect personal information from unauthorised use or disclosure.

If you wish to access your personal information, you should make a request in writing to the Privacy Officer.

7 Identifying a data breach

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.
- unauthorised access to personal information by an employee.
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person.
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

8 Consequences of data breach

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation. Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud.
- identity theft causing financial loss or emotional and psychological harm.
- family violence.
- physical harm or intimidation.

- Negative impact on YPOL's reputation for privacy protection.

9 Notifiable Data Breaches

The notifiable data breach scheme (NDB scheme) requires YPOL to notify individuals and the Commissioner of certain data breaches. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

10 YPOL's Data Breach response plan

- **Please see appendix A**

11 YPOL Data breach checklist

- **Appendix B**

A quick response to a data breach is critical to effectively managing a breach.

Access

If you wish to request access to personal information that we hold about you or seek to correct such information, please contact our Privacy Officer at:

Privacy Officer

YPOL Lawyers

Level 4, 1 Chifley Square

Sydney NSW 2000

Email: enquiry@ypol.com.au

We will respond to the request for access within a reasonable period. Charges may apply if you are given access to the personal information.

Complaints

If you wish to make a complaint about a breach of the Australian Privacy Principles or any registered Australian Privacy Principle Code we are bound by, please contact our Privacy Officer. We will respond to the complaint within a reasonable period.

Appendix A

Identify the data breach	A data breach is unauthorised disclosure of information, or loss of information, that YPOL holds	Examples of data breaches include: • loss or theft of physical devices **(**such as laptops and storage devices) or paper records that contain personal information - this type of breach would require immediate escalation • unauthorised access to personal information by an employee • inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person • disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.
Contain	Immediately take action to contain the breach	For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.
	Assessing these questions may help identify strategies to contain a data breach	How did the data breach occur? Is the information still being shared? Who has access to the information? What can be done to secure the information?
Assess	An assessment of the data breach can help an entity understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.	The type of personal information involved in the data breach The circumstances of the data breach, including its cause and extent The nature of the harm to affected individuals or businesses

Notify	**Line Manager** **Office Manager** **IT support** **Directors**	Consider: • the obligations of the entity under the NDB scheme. Entities are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm. • other circumstances in which individuals should be notified. For example, your entity may not have obligations under the NDB scheme but have processes in place to notify affected individuals in certain circumstances. • how notification should occur, including: • what information is provided in the notification? • how the notification will be provided to individuals o who is responsible for notifying individuals and creating the notification. • who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified. • where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public. • whether the incident triggers reporting obligations to other entities.
Document		**See Appendix B**
Review	Once the above steps have been taken, a review will need to be taken.	This might involve: • a security review including a root cause analysis of the data breach. • a prevention plan to prevent similar incidents in future. • audits to ensure the prevention plan is implemented. • a review of policies and procedures and changes to reflect the lessons learned from the review. • changes to employee selection and training practices • a review of service delivery partners that were involved in the breach.