PRIVACY POLICY

Personal Information

The *Privacy Act 1988* (Cth) defines personal information as information or an opinion about an identified individual (or an individual who is reasonably identifiable). In this context, it does not matter whether the information or opinion is true or not, nor does it matter how the information or opinion is recorded.

Examples of personal information include:

- Basic contact information (such as names, addresses and phone numbers).
- Gender.
- Date and place of birth.
- Information about relationships, including past and current family members, employees, employers, co-workers, lenders and acquaintances.
- Financial information, such as income, asset and debt details and past and current personal and corporate insolvency.
- Third party identifiers, such as bank account and customer numbers.
- Past and current employment information.
- Credit information, including credit reports.
- Personal identification documents.
- Videos, audio recordings, photographs and/or social media account posts.
- Australian and/or foreign residency information, including citizenships.

Examples of particularly sensitive personal information include health information; racial or ethnic origin; political opinions, religious belief and/or political or religious affiliations; gender, gender identity and/or sexual preferences; criminal records; and genetic information.

Sometimes, for example where there is a known risk of family violence, even a current residential address may fairly be regarded as sensitive.

What personal information do we collect?

We routinely collect personal information when we conduct our business, including when we deliver legal services to clients and purchase goods or services from our suppliers.

We always collect basic contact information about our clients and suppliers. The main reason for this is that common sense dictates and sometimes Australian law requires that we verify client and supplier identity. This is particularly the case in relation to property (including financial) transactions.

The other types of personal information we collect varies according to context, including the nature of the legal services we are asked to provide and our obligations at law such as under taxation and/or anti-money laundering legislation. Examples include:

- When we are asked to provide advice regarding workers compensation or other types of personal injuries claims, we will usually request disclosure of and/or access to detailed, past and current family, employment and health information.

- When a client asks us to recover a debt or defend debt recovery action or provide restructuring or personal or corporate insolvency advice, we will usually request disclosure of and/or access to sensitive financial (including taxation) information and sometimes to finance applications and credit history reports.

- When we act in relation to land transactions, we are usually required by law to collect detailed personal information (including sensitive information) to verify identity and correctly determine taxation liabilities.

- We often discuss sensitive information in connection with discrimination and related industrial law claims.

Why do we collect personal information?

We collect personal information for three main reasons:

- To provide quality, effective and efficient legal services to our clients.

- To run and market our business efficiently and effectively.

- To comply with Australian law.

How do we collect personal information?

We often collect personal information directly from the individual or organisation concerned. For example, if we need your telephone number we will ask you for it directly, or if an email we send to you bounces we will contact you by phone to confirm the correct address.

Other ways we may receive personal information include via:

- Public registers and databases, such as the Personal Property Securities Register, ASIC Connect, and Access Canberra.

- Paid search providers, such as InfoTrack.

- Other professionals, such as accountants, finance brokers, insurance brokers and financial planners.

- Other lawyers, when they communicate with us in connection with work we are engaged to perform.

- Subpoenas, notices for non-party production and disclosure during litigation.

- Witnesses and relatives.

- Banks and other financial institutions, insurance companies and government agencies.

- Other professionals and clients, when they refer us work.

Information Management

We manage the personal information we collect using common sense, reasonable access and security controls and with due regard to our professional duties and other obligations under Australian law. For example:

- We take steps to ensure that our knowledge of privacy-related issues and relevant laws remains current, and that we apply best practice wherever possible.

- We take reasonable steps to ensure that we avoid making common information technology-related security mistakes.
- We read the terms and conditions and privacy and security policies of our suppliers to satisfy ourselves that we are dealing with appropriately skilled, privacy-aware organisations.
- We conduct periodic, internal privacy and security checks.
- We have written policies, including business systems and information technology policies, to guide our staff.
- Privacy and security awareness is a routine part of new staff induction.

Disclosure

Australian law requires us to respect and maintain the confidences of our clients. This means that we may only disclose the substance of conversations we have with our clients, correspondence we engage in with our clients and client documents in limited circumstances. It also means that we must manage client files with an appropriate degree of sensitivity.

When clients provide information to us for the dominant purpose of obtaining legal advice, legal professional privilege will usually also apply. This special rule of law means that we cannot disclose the information without client consent unless another law or a Court compels us to do so.

Sometimes, we may not be able to complete the work you have asked us to perform if you withhold consent to necessary or reasonable disclosure of your personal information. For example, we may not be able to attend to a necessary government registration or file documents at Court, if you do not authorise us to provide the government or Court with your full name and current address.

We may be required to disclose personal information (or may seek your consent to disclose personal information) in a variety of contexts. Examples include necessary or reasonable disclosures to:

- Courts and Tribunals.
- Government and non-government agencies, such as to ASIC, Access Canberra, the Office of State Revenue or the Australian Taxation Office.
- Paid search providers.
- Where you are negotiating a transaction or involved in a dispute, to other parties and/or their solicitors.
- Internally to our staff.
- Our suppliers where, for instance, a disbursement will be invoiced directly to you,
- Other service providers or referral partners, so that we may appropriately complete work you have asked us to perform (for example, other solicitors, barristers, experts, accountants, insurers etc).
- Third parties who supply financial, administrative, information technology or other services to our business.

How and where do we hold personal information?

We are a virtual law firm. We hire virtual office space in Canberra City, ACT, which we use to see clients and hold meetings. Our staff work remotely from the locations most convenient to them from time to time, which may include a home office, public place or day office space. We prefer to conduct business with minimal environmental impact, and train and expect our staff to:

- maintain paperless client files;

- store all client-related information in matter files created in our preferred practice management software; and

- only use the hardware and storage systems we allocate or approve, in connection with their work, and to avoid using portable storage devices such as external hard drives;

and we maintain and enforce appropriate internal policies on topics including business systems and information technology security. Those policies provide relevant guidance to our staff, including instruction regarding effective, basic information security controls and common sense privacy procedures.

This 'New Law' business model creates significant opportunity for us to improve efficiency, reduce cost and modernise the way we deliver traditional legal services . However, there are also several risks for you to consider and we recommend that you return to our website to read our Technology Disclosure for further information.

Some of the changes you will experience as a client of our firm include:

- Incoming paper correspondence is scanned and uploaded into our practice management software. The paper is then securely destroyed and recycled.

- Our solicitors will still makes notes about conversations, but generally these will be electronically created in the first instance rather than being handwritten. As with incoming, paper correspondence, handwritten notes are scanned and uploaded into our practice management software before the paper is securely destroyed and recycled.

- In other words, we generally only hold paper records of personal information for brief periods of time (we do not archive paper records).

- All client-related emails we receive are saved into our practice management software. Although local data files may exist on local hardware, these do not serve as a primary record.

- It is firm policy not to delete any client-related text or other instant messages received on smartphones and other devices. All staff are taught to export these forms of communication from their device so the information can be stored in our practice management software.

Although the systems we have in place should mean that a full copy of all client-related information is contained in our practice management software, it is inevitable that information will also be stored electronically on multiple devices located in multiple places. Despite that our staff are instructed not to intentionally store any business-related information on local hardware/devices, there will always be a local footprint of some description.

We will take all reasonable steps to ensure that all personal information we hold is secure from any unauthorised access, misuse or disclosure. However, we do not guarantee that personal information cannot be accessed by an unauthorised person (e.g. a hacker) or that unauthorised disclosures will not occur.

Correcting personal information

Where we become aware that personal information we hold is not accurate, complete or current, we will take appropriate and reasonable steps to correct it.

You may ask for your personal information to be corrected by contacting the solicitor acting for you or by emailing privacy@namadgilegal.com.au.

Please note that we may request proof of identity before acting on your request.

Accessing your personal information.

You may ask for access your personal information by contacting the solicitor acting for you or by emailing privacy@namadgilegal.com.au.

Sometimes we may decline to facilitate access. For example, where:

- it is impractical to facilitate access, or your request is unreasonable.
- facilitating access would have an unreasonable impact on the privacy or safety of another person or would compromise our professional obligations; or
- the law permits or requires us to deny you access.

However generally speaking, we will endeavour to grant you access as soon as possible in the circumstances, at a mutually convenient time and place.

Please note that we may request proof of identity before facilitating access.

We may charge a fee for reasonable costs incurred in responding to an access request. The fee (if any) will be disclosed in advance.

Complaints

Please email any privacy related complaints to privacy@namadgilegal.com.au or post written complaints to the attention of the Privacy Officer (Managing Director) at our current postal address.

We will do our best to resolve your concerns to your reasonable satisfaction within a reasonable time.

In the unlikely event that we are unable to resolve your concerns, you may be able to complain externally to organisations such as the Law Society of the Australian Capital Territory or the Office of the Australian Information Commissioner.

Changes to this policy

We may update, modify or remove this policy at any time and from time to time.

Any updates and modifications will be published on our website.

This policy was last updated in June 2018.

If you have any comments on the policy, please contact privacy@namadgilegal.com.au.