



Australian Government

IP Australia

# Privacy Policy



## Revision History

Date	Amendments
02 December 2010	Policy approved by the Executive
21 March 2012	Revised document approved – updated links and text
05 March 2014	Revised document approved – compliance with legislative amendments
10 April 2014	Revised document approved – updated text
10 December 2018	Revised document approved – updated text
18 July 2019	Revised document approved – updated text
14 November 2019	Revised document approved – updated text
10 March 2022	Revised document approved – updated text
9 December 2024	Revised document approved – updated text
5 February 2026	Revised document approved – annual review process

## Contents

<b>About this Privacy Policy</b>	<b>5</b>
<b>IP Australia’s functions and activities</b>	<b>5</b>
<b>Application – Information covered by this policy</b>	<b>6</b>
<b>Collection of Personal Information</b>	<b>6</b>
<b>WHAT</b> kinds of personal information do we collect?	6
<b>WHY</b> do we collect personal information?	7
<b>HOW</b> do we collect personal information?	7
Indirect collection	7
Collection through online services and third-party platforms	8
Unsolicited Information	10
<b>Use of personal information</b>	<b>10</b>
Primary Uses	10
Secondary Uses	11
Use of personal information in Artificial Intelligence (AI) tools and Automated Decision Making Processes	11
<b>Disclosure of personal information</b>	<b>12</b>
Disclosures under IP Rights Legislation	12
Disclosures to Government and Associated Entities, Stakeholders	12
Disclosures to Service Providers	12
Overseas Disclosures	13
Further Disclosures of publicly available personal information	13
<b>Storage, Security and disposal of personal information</b>	<b>13</b>
Storage of Personal Information	13
Security of Personal Information	14
Disposal of Personal Information	14
<b>Anonymity and Pseudonymity</b>	<b>14</b>
<b>Access to, and correction of, Personal Information</b>	<b>14</b>
Request for access or correction	14
How we Respond	15
<b>Enquiries and Complaints about Privacy</b>	<b>15</b>

Complaints handling process	15
<b>Contact Us</b>	<b>15</b>

---

## About this Privacy Policy

This Privacy Policy outlines how IP Australia manages personal information in accordance with the *Privacy Act 1998* (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

IP Australia is committed to protecting the privacy of individuals and ensuring transparency in our information handling practices.

This privacy policy is reviewed annually by the Privacy Officers or when there is a significant change in our functions or information handling practices.

## IP Australia's functions and activities

IP Australia is the Australian Government agency responsible for administering Australia's Intellectual Property (**IP**) rights system, specifically trade marks, patents, designs and plant breeder's rights.

We collect, use and disclose personal information to exercise powers and perform functions under the:

- *Patents Act 1990*
- *Trade Marks Act 1995*
- *Designs Act 2003*
- *Plant Breeder's Rights Act 1994*
- *Wine Australia Act 2013 (in the process of resolving objections to determinations of geographical indications)*
- *Regulations made under those Acts.*

Some of these functions and activities include:

- processing applications, requests or notices related to IP rights and communicating with people about those rights
- maintaining records of IP right ownership and applications
- responding to general correspondence and customer enquiries and feedback
- communicating with stakeholders and the public including IP experts, IP offices, government agencies and research institutions
- Distributing relevant information to applicants, owners and mailing list subscribers.

Other general agency business functions and activities include:

- conducting market research and consultation processes
- managing employees and contractors, including managing performance and ensuring their health and safety
- verifying identity
- undertaking necessary criminal background checks for eligibility and ongoing suitability requirements
- managing the security of our systems, premises and information
- managing staff access to IT systems and tools
- handling complaints and feedback
- information sharing with other entities or the public where it is lawful to do so
- processing requests under legislation (e.g. Freedom of Information)
- supporting internal business operations such as planning, auditing, billing and service improvement

- participating in Committees and Boards, reference and working groups, and international IP forums
- undertaking research or providing education.

We also hold personal information on behalf of:

- the Trans-Tasman IP Attorneys Board (**the Board**), responsible for administering the regulatory and disciplinary regimes for patent attorneys in Australia and New Zealand and trade marks attorneys in Australia, and
- the Trans-Tasman Disciplinary Tribunal (**Tribunal**), responsible for deciding whether trade marks and patent attorneys have committed offences.

Please see the [Board's Privacy Policy](#) and the [Tribunal's Privacy Policy](#) for further information on how the Board and Tribunal respectively use and disclose personal information.

## Application – Information covered by this policy

This policy applies only to personal information, as defined under the Privacy Act, which is

*“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.”*

Examples of personal information include:

- your name or address;
- bank account details and credit card information;
- photos; and
- information about your opinions and what you like.

## Collection of Personal Information

**WHAT** kinds of personal information do we collect?

For **IP Rights Customers and third party stakeholders**, we may collect:

- **Identity and contact details:** name, date of birth, address, phone number, email address
- **IP-related data:** application details, address for service, information on ownership or opposition of IP right, claimed interests over IP rights, disciplinary records of patent/trade mark attorneys, personal information contained in relevant IP rights related commercial agreements (i.e. co-existence agreements, licenses, consents)
- **Financial details:** bank account, credit card, debts, bankruptcy checks
- **Business identifiers:** ABN, CAN, Tax File Numbers (TFNs)

For **IP Australia employees, job applicants and contractors**, we may collect:

- **Identity and contact details:** name, date of birth, nationality, address, phone number, email address, photographs, passport details, visas, citizenship or immigration status, government identifiers

- **Employment information:** occupation, qualifications and memberships, work history, referee reports, CVs, application for employment
- **Household information:** information about other people within your household, where relevant
- **Personnel and payroll records:** correspondence, performance and remuneration
- **Financial details:** bank account, credit card, debts, bankruptcy checks
- **Security and access records:** security clearances, police record checks, building and system access
- **WHS and health-related information**

Where relevant to our functions and activities such as for identity verification and criminal background checks for onboarding staff, we may collect **sensitive information** (a type of personal information) such as:

- **Health information**
- **Racial or ethnic origin**
- **Sexual orientation**
- **Criminal history and security assessments**
- **Biometric or genetic data**
- **Religious affiliation**

#### WHY do we collect personal information?

We aim to collect personal information only where necessary to perform our statutory functions and our general business activities. See 'IP Australia's functions and activities' above.

#### HOW do we collect personal information?

We generally collect your personal information **directly** through a range of channels, including when individuals:

- Contact us by phone, email, or in writing
- Use our website or webchat
- Subscribe to newsletters, mailing lists or participate in surveys
- Visit our offices or attend meetings (in person or virtual)
- Apply for a job or respond to stakeholder consultations
- Interact with us via social media or other web-related platforms such as Facebook, YouTube or LinkedIn
- Register and use the Online Services system to apply for and manage IP rights.

#### Indirect collection

In some cases, we may collect your personal information **indirectly** from your authorised representative, other government agencies; contractors or service providers acting on our behalf; or publicly available sources when:

- You have consented (e.g. survey participation);
- It is required or authorised by law (e.g. IP rights registration); or
- It is impractical or unreasonable to collect it directly from you.

We may also be provided with personal information from AGSVA to manage residual risks in relation to holding a national security clearance.

### Collection through online services and third-party platforms

To apply for IP Rights in Australia, you must register with our online services platform and accept the relevant terms and conditions. Personal information provided as part of registration is used to manage your account and process applications in accordance with the relevant Privacy Collection Notice and this Privacy Policy.

We may also collect personal information indirectly through third-party platforms to support service delivery, engagement and analytics. Some of these platforms can be accessed via IP Australia's website, social networking services, or as directed by IP Australia staff, and may collect limited personal information or use cookies. Key platforms include:

#### **Dynatrace application performance monitoring (APM) platform**

Our online services platform uses Dynatrace Application Performance Monitoring (APM) to monitor technical faults. This allows our systems support team to quickly rectify issues and identify improvements.

Dynatrace doesn't collect personally identifiable information.

#### **Clickstream data**

Clickstreams record your path when navigating a web page or the internet.

When you visit our website, our internet service provider (ISP) makes a record of your visit and logs your clickstream information.

We use this information to see what pages you've visited on our website. We analyse it to improve overall customer experience, establish priorities and allocate resources.

We don't identify you or your browsing activities, except if a law enforcement agency provides a warrant to inspect our ISP logs as part of an official investigation.

#### **Cookies**

A cookie is a short piece of data sent from a web server to a web browser on your computer or device when you visit a website. We use cookies to help co-ordinate your experience

We can't use cookies to find out names, email address or anything about your computer. We don't store or collect cookie information.

#### **Survey Monkey**

We use Survey Monkey to administer online surveys. These surveys use third party cookies.

The information collected by the cookies is not capable of identifying. It's only used

to ensure our surveys run effectively. We only use this information for statistical and maintenance purposes. For more information, see [Survey Monkey's Privacy Policy](#).

### **Qualtrics**

We use Qualtrics to administer online surveys. Qualtrics uses cookies for purposes such as:

- assisting you in navigating the website and product
- supporting registration, login, and feedback functionality
- analysing your use of Qualtrics products, services or applications, and
- assisting with promotional and marketing efforts including behavioural advertising

These surveys also use third party cookies.

You can find out how to amend your cookie setting to suit your preferences in [Qualtrics privacy statement](#) and [Qualtrics Cookie Statement](#).

### **Google Analytics**

We use Google Analytics to collect anonymous information about how you arrive at and interact with our website. Google uses first-party cookies and JavaScript code to collect this information.

Google Analytics doesn't track any application processes or procedures from online services.

You can opt out of [Google Analytics](#) by disabling or refusing the cookie or disabling JavaScript.

### **Eventbrite**

We coordinate our events through Eventbrite. Eventbrite facilitates the registration process and handles any personal information collected in accordance with their [Privacy Policy](#). They'll also provide your name, contact details and email address to us for the purpose of registration for the event.

### **Social Networking Services**

We use social networking services such as Facebook, YouTube, Instagram and LinkedIn to communicate with the public. When you interact with us on these platforms, we may collect your personal information to respond to enquiries or engage with stakeholders.

Please note:

- These platforms handle your personal information according to their own privacy policies
- They may store data outside Australia and use cookies or other tracking technologies
- Your use of these services is governed by the terms and conditions of each platform

### **SpendConsole**

We use SpendConsole, a cloud-based supplier invoice management and compliance system that supports Pan-European Public Procurement On-Line (PEPPOL) invoicing standards and provides some automation to IP Australia's Accounts Payable processes.

Personal information provided by suppliers will be stored in SpendConsole and used for the purposes of:

- processing and paying invoices received via any channel (including PEPPOL, email or mail)
- managing vendor information/records
- maintaining financial records.

### **Swift Digital**

We use Swift Digital, an email marketing platform, to manage subscriber lists and send targeted email communications to customers and IP Australia staff (for example, newsletters, event invitations and updates on IP matters).

When you subscribe to specific mailing lists for various IP products/events or opt in to participate in research, we will collect your personal information which may include your name, email address, telephone number, location, occupation, and areas of interest. These details are automatically added to the Swift Digital Platform.

This information is collected to enable the efficient delivery and management of tailored marketing communications, and may also be used internally for analysing engagement trends, reporting and ongoing improvement of communication strategies. Any external reports will not contain personal information.

You can opt out at any time using the unsubscribe link in our emails. Further details on how Swift Digital handles your personal information can be found in their [Platform Privacy and Spam Policy](#).

## **Unsolicited Information**

If we receive unsolicited personal information, we will assess whether it is necessary for our functions. If not, we will destroy or de-identify it in accordance with the Privacy Act and applicable National Archives of Australia Records Disposal Authority. For example, unsolicited information received by our Contact Centre may be retained as a Commonwealth record until it can be lawfully destroyed.

## **Use of personal information**

### **Primary Uses**

We use personal information for the primary purpose for which it is collected. This purpose is usually explained at the time of collection.

Personal information is used to support IP Australia's statutory functions and general

business activities.

Examples include:

- using information you provide to process your request relating to your IP rights,
- using information about applicants and IP rights to maintain publicly available IP rights registers,
- using your contact details to respond to questions you have asked,
- using information you have provided to assess your suitability for a job opportunity.

## Secondary Uses

We may use personal information for purposes other than the primary purpose of collection in some circumstances, such as if the individual has consented, the use is required or authorised by law, or if the individual would reasonably expect the information to be used in that way. Secondary purposes will also usually be explained at the time of collection.

Some examples of secondary uses are:

- Using transcripts of webchat interactions to improve service quality
- Using personal information to help ensure the health and safety of employees or contractors. In these instances, information is shared internally on a need-to-know basis and may be disclosed externally to other government bodies or health authorities where legally required.

## Use of personal information in Artificial Intelligence (AI) tools and Automated Decision-Making Processes

We may use Artificial Intelligence (AI) tools and Automated Decision Making (ADM) systems to support service delivery, improve operational efficiency in administering IP rights, and enhance user experience in customer service.

Where personal information is used in AI tools, we will endeavour to:

- Clearly identify the use of AI to users,
- Provide information about how personal information is handled
- Offer alternatives or human support where appropriate.

ADM processes are mostly used within IP Australia's internal systems to improve efficiency and consistency in our processes. There are several instances in which personal information is used in the ADM process. In those circumstances, we ensure that appropriate controls are in place to mitigate harm that may affect the rights or interests of an individual.

Our use of AI and ADM aligns with IP Australia's [AI Transparency Statement](#), the Australian Government's [Policy for the responsible use of AI in government](#), the [National Framework for AI Assurance](#), and the Commonwealth Ombudsman's [Automated Decision-Making – Better Practice Guide](#).

## Disclosure of personal information

We disclose personal information only for the primary purpose for which it was collected, or for secondary purposes if you have provided consent, you would reasonably expect the disclosure, or the disclosure is required or authorised by law.

### Disclosures under IP Rights Legislation

We disclose personal information about IP rights applicants, owners, and related parties as required under the legislation we administer. This includes:

- Publication on IP Rights databases, our website and Application Programming Interfaces (APIs), and
- participating in merit or judicial review proceedings in tribunals or courts or to institute proceedings in courts.

### Disclosures to Government and Associated Entities, Stakeholders

We may disclose personal information to other external parties such as:

- **Other Australian Government agencies** – in accordance with provided notices and as required or authorised by law (e.g. providing personnel records to the ATO or health information to Comcare)
- **Trans-Tasman IP Attorneys Board** – personal information of registered patent or trade mark attorneys that IP Australia considers relevant to the Board's functions.
- **Trans-Tasman IP Attorneys Disciplinary Tribunal** – personal information of registered attorneys involved in disciplinary proceedings
- **Consultation Groups** – Contact details of members of the Patents, Trade Marks, Plant Breeder's Rights Stakeholder groups.
- **Organisations upon request (e.g. research institutions, overseas IP Offices)** – We provide a variety of data products that are intended to suit the requirements of large companies, research organisations, libraries and overseas IP offices. This data includes personal information, such as names and addresses (postcode and country only), but does not include any sensitive information. IP Australia's Bulk Data Product Terms and Conditions within the Bulk Data Products Order Form prohibit the use of this data for creation of mailing lists or other marketing material.
- **Background Checking Partners** – for necessary police checks.

### Disclosures to Service Providers

We engage service providers to support our business operations including:

- Website hosting
- IT infrastructure and support
- Human resources systems
- External Audits

Where personal information is disclosed to service providers, we:

- Enter into contracts or MOUs that restrict use and disclosure to the agreed purpose
- Include specific privacy obligations to ensure compliance with APPs and secure handling of personal information.

Some service providers may store data in Australia or overseas. Where overseas disclosure occurs, we take reasonable steps to ensure appropriate privacy protections are in place.

### Overseas Disclosures

We disclose certain personal information to overseas recipients with consent, where authorised by or under law, or in accordance with an international treaty or convention, and in the following circumstances:

- When we publish IP rights-related personal information online in accordance with legislation, this information may be accessed globally.
- We file applications for IP rights, on behalf of applicants, with the International Bureau of WIPO (Geneva, Switzerland)
- We provide details of technical trainers to WIPO and ASEAN countries (i.e. name; date of birth; biographical details, including qualifications, education and experience; passport and visa details and citizenship)
- We share certain information about IP rights to overseas IP offices. It is not practicable to list all countries that we may disclose this information to, however, if you would like further information on this, please [contact us](#).
- We use contracted service providers to provide our Contact Centre and we use overseas-based service providers for IT and web hosting. If you provide personal information when you are using services such as our webchat and phone calls, our service providers will retain transcripts of the interaction and call recordings for the purpose of answering your enquiries, training and development to improve service delivery and to generate reports. Our service providers will store the information you provide in data centres located in Australia.
- We use a number of service providers to whom we disclose personal information. These include providers that host our website servers or provide us with IT services. They may store the information you provide in datacentres located in Australia or overseas.

### Further Disclosures of publicly available personal information

When we publish personal information on the internet or in online databases, that information may be accessed by any individual. We have no control over the subsequent use and disclosure of that personal information and is not accountable under the Privacy Act for any subsequent use of such information.

## Storage, Security and disposal of personal information

### Storage of Personal Information

- We store personal information securely using:
  - Electronic document and records management system
  - Databases and cloud platforms assessed as compliant with Australian Government security standards
  - Paper-based files in secure physical storage.

The storage of personal information is managed in accordance with the *Archives Act 1983*.

## Security of Personal Information

We take reasonable steps to protect personal information from loss, unauthorised access, modification or disclosure.

Our security practices include:

- Accessing records on a 'need-to-know' basis and subject to access controls and security clearances
- Secure storage of paper records in locked cabinets
- Clear-screen policy
- ICT protections on internal network, electronic records management system and databases such as firewalls, intrusion detection and prevention, antivirus software, user authentication
- Transactions made using online services are encrypted and monitored for misuse
- Use of Australian Signals Directorate-certified gateways for web services
- 24/7 surveillance of premises with logged access controls

If we become aware of a data breach or potential breach, we will respond in line with our Data Breach Assessment and Response Plan, which aligns with the Notifiable Data Breaches Scheme.

## Disposal of Personal Information

We dispose of personal information when it is no longer required for lawful purposes, unless:

- It forms part of a Commonwealth record
- Retention is required by law or court/tribunal order

Disposal is carried out securely and in accordance with approved records disposal authorities issued by the National Archives of Australia.

## Anonymity and Pseudonymity

Where practicable, you may interact with us anonymously or using a pseudonym – for example, when requesting general information or providing feedback. However, in some cases, such as registering IP rights, it may be impracticable to remain anonymous. We will inform you at the time of collection if identification is required or optional.

## Access to, and correction of, Personal Information

### Request for access or correction

Under the Privacy Act, you have the right to:

- request access to personal information that we hold about you
- request correction of your personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

You also have similar rights under the *Freedom of Information Act 1982* (Cth).

You can ask for access, or request correction, by contacting us (see the 'Contact us' section of this Privacy Policy).

## How we Respond

We will:

- acknowledge your request within **5 business days**
- provide a written response within **30 calendar days** after receiving your request which may include:
  - access to the requested information
  - a decision to refuse access or correction, with reasons
  - an update on progress advising you of any difficulties encountered in actioning your request including an expected timeframe for finalising your request.

Access may be refused in certain circumstances where IP Australia is required or authorised to do so by law.

## Enquiries and Complaints about Privacy

If you think we may have breached your privacy, or you are not satisfied with our response to your request, you may contact us to make a complaint (see the 'Contact us' section of this privacy policy).

If you are dissatisfied with our response, you may make a complaint in writing to the Office of the Australian Information Commissioner (OAIC). For more information, see the [OAIC website](#).

### Complaints handling process

We will acknowledge that we have received your enquiry/complaint within 5 business days.

We will usually respond to your privacy enquiry/complaint within 30 calendar days after the request is made, if you provide your contact details. These timeframes may be affected if the privacy complaint relates to a suspected data breach. In these instances, the resolution of the complaint will often be dependent on the finalisation of the data breach investigation. We will seek to agree an appropriate timeframe with you.

We are committed to quick and fair resolution of customer complaints and will ensure any privacy complaint is taken seriously. You will be treated professionally and respectfully at all times.

## Contact Us

To find out more about how we manage personal information, to make a complaint, or to request access to or correction of personal information, please contact our Privacy Officers via:

Email: [Privacy@ipaustralia.gov.au](mailto:Privacy@ipaustralia.gov.au)

Post: IP Australia

Attention: Privacy Officers  
PO Box 200  
Woden ACT 2606