Privacy Policy

October 2026

HPX Group Privacy Policy

The HPX Group is a professional services provider, bringing together Hamilton Locke, Source and Helios Salinger to provide exceptional legal, governance, risk, compliance and privacy services.

This Privacy Policy describes how all Australian companies in the HPX Group (**we**, **us**, **our**, **HPX Group**) handle personal information for the purposes of our obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**).

The Privacy Policy of Hamilton Locke New Zealand is available here.

1. Definitions

In this Privacy Policy:

Personal Information is defined in the Privacy Act to mean information or an opinion about an identified individual, or about 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.

Sensitive Information is a sub-set of Personal Information and is defined in the Privacy Act to mean information or an opinion about an individual's racial or ethnic origin; political opinions, religious or philosophical beliefs or affiliations; memberships of trade union, trade or professional association; sexual orientation or practices; criminal record; health information, genetic or biometric information, or biometric templates.

Website means each of the following websites, including any online store (eStore) operated through them:

(a) https://www.hpxgroup.com.au/

(b) https://www.hamiltonlocke.com.au/

(c) https://www.source.com.au/

(d) https://www.heliossalinger.com.au/

2. What kinds of Personal Information do we collect and hold?

We collect and hold a range of personal information in carrying out our business and functions. The kinds of Personal Information we collect and hold about you will depend on the nature of your relationship with us and the circumstances of a collection, including whether we collect the information from you as a client, service provider, supplier, job applicant or some other capacity.

2.1 Clients

If you are a client, a prospective client, or a representative of them, we may collect Personal Information about you or them related to the matter for which we have been engaged. This Personal Information may include:

(a) your name and contact details;

(b) job title, organisation or company name and employment information;

(c) identification information and documents such as your date of birth, gender, signature, passport, driver's license, Medicare card or other official identification document. Where additional proof of address is required as part of the identify verification process, we may also collect documents such as utility bills, bank statements or council rates notices;

(d) financial details, such as banking details, or credit/debit card information (if you provide them directly to us, however, typically your credit card information is processed by our payment service providers, and we do not have access to that information);

(e) communications between us and the history of, and your relationship with others involved in, the matter;

(f) information about your areas of interest, such as legal developments or events you are interested in hearing about from us; and

(g) other relevant Personal Information or Sensitive Information, depending on the nature of the matter or your engagement with us.

We are required to identify our clients and report certain transactions and suspicious matters to AUSTRAC under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML legislation**) when we provide designated services. We collect identification information and documents, and conduct relevant searches and enquiries, to comply with this obligation, including information about officers or directorships held, business activities and relationships, and the source of funds, as well as understanding the individuals who ultimately own or control the client, are beneficial owners or act on behalf of the client. We collect this information and conduct the required checks through public records and registries, as well as subscription services, but may also ask you to provide us with information and documents, including identification documents. We use a third-party service provider to assist us with these checks. If we cannot collect this information, we may not be able to act for you as a client.

2.2 Suppliers and service providers

If you are a contractor, supplier or service provider to us (such as IT service providers and marketing firms) or on behalf of our clients (such as barristers, experts, valuers, accountants and tax advisers), we may collect Personal Information about you, or your employees and contractors, such as:

(a) your name and contact details;

(b) your job title, job history, organisation or company name;

(c) financial details such as your bank account to make payments to you;

(d) information about performance of the contract or other arrangement between us; and

(e) communications between us.

2.3 Matter parties

If you are another party in respect of one of our client's matters, or if you represent such a party, we may collect Personal Information about you during the course of the matter. The type of information will depend on the nature of the matter, but is likely to include:

(a) your name and possibly contact details;

(b) the history of, and your relationship with others involved in, the matter; and

(c) communications between us.

2.4 Job applicants

If you apply for a job with us, we may collect Personal Information directly from you when you complete an online job application or through an external party, such as a recruitment agency. The information collected may include:

(a) your name and contact details;

(b) your resume, covering letter and academic transcript;

(c) information provided on your application form or resume, including education level, tertiary institution, language skills, jurisdictions you are qualified to practice in (if applicable), employment history and any other background information relating to your right to work in Australia;

(d) information provided to us during an interview or assessment;

(e) references from past referees, including past employers; and

(f) skills and background checks, which may include a criminal history check.

If you are or become an employee, the handling of your personal information may be exempt from the APPs if it is directly related to your current or former employment relationship with us.

2.5 General collection

If you contact us through our website, register to attend one of our seminars or other events, or subscribe to one of our publications, engage with us through social media or at an event, we will generally collect your name, contact details, and any other Personal Information you provide to us. We may also collect your health information (such as where you tell us your dietary preferences) and other Sensitive Information you provide to us, such as your religious beliefs or affiliations, or membership of a political, professional or trade association.

We will also collect Personal Information that you give to us in the course of our relationship. This information will depend on the nature of our relationship, but may include:

(a) information included in your requests for support;

(b) if you join our alumni program, your name and contact details, and your current employment; and

(c) calling line identification when you call us.

To the extent that it is relevant to the work we are undertaking for a client or a job applicant, we may also collect and hold personal information that is Sensitive Information. For example, we may collect health information about an individual, membership of a professional or trade association, membership of a trade union, religious beliefs or affiliations or criminal records.

3. Anonymity and use of pseudonyms

We provide tailored professional legal advice and related services. This means that, generally, you will have to identify yourself when dealing with us. However, there may be some circumstances, such as when you use our Website, that you may be able to deal with us anonymously or through a pseudonym. You do not have to provide us with your Personal Information, but this may mean we cannot provide our services or assistance to you.

4. How we collect Personal Information

In most circumstances, we will collect Personal Information about you directly from you, or if you are an employee, director or officer of a client or other organisation with whom we deal, from that organisation. There are some circumstances where it is unreasonable or impracticable for us to do so, and we will collect Personal Information from third parties, such as:

(a) associated businesses, government agencies, courts or tribunals, licensing bodies, local councils, referrers (such as other law firms, accountants, real estate agents, financial planners, insurers and business consultants);

(b) barristers, experts, and accountants we engage to provide services in respect of your matter;

(c) our client, or your legal representatives, where you are another party involved in a matter;

(d) service providers, including recruitment agencies, and identity verification and background check service providers;

(e) ratings and search agencies;

(f) referees and previous employers, when you provide references to us in the course of a job application;

(g) other third parties that you refer us to;

(h) publicly available records and subscription services, such as company and other public registers and registries, court records and other sources; and

(i) social media and online searches.

Where you provide us with the personal information of an individual, you must make that individual aware that we are collecting their personal information and refer them to this Privacy Policy. You must only provide Sensitive Information about another individual where you have that individual's consent to do so.

5. Purposes of collection, use, disclosure and holding personal information

We collect, hold, use and disclose Personal Information for the purpose for which it was collected and otherwise as permitted under the Privacy Act. This includes:

(a) to supply our products and services;

(b) to conduct conflict checks, verify identity, and undertake other searches and checks (including for example to undertake PEXA checks, KYC and CDD checks, AFSL-related checks, criminal history checks and bankruptcy checks) to comply with our legal, professional and insurance obligations;

(c) to respond to your enquiry and communicate with you about your enquiry;

(d) to verify and process payments;

(e) to comply with our legal, professional and insurance obligations;

(f) for our administrative and risk management purposes, and internal record keeping;

(g) for the prevention of fraud and other criminal activities;

(h) to provide you with support and deal with any complaints or feedback you have;

(i) to perform research and analysis and improve or develop our products or services;

(j) to measure and report on the effectiveness of our advertising and marketing campaigns, including by sharing information with analytics and advertising platforms as described in the Websites section of this Privacy Policy;

(k) to manage and develop our relationships with our clients, potential clients, service providers, suppliers and contractors;

(l) to consider job applicants for current and future employment;

(m) to market our services, improve data quality, and for business development and direct marketing purposes; and

(n) carrying out our functions and activities as a professional legal service and compliance services provider.

We may use and disclose your personal information for other purposes required or authorised by or under law (including purposes for which you have provided your consent).

6. Disclosure of personal information to third parties

We may disclose your Personal Information to third parties for the purposes outlined above, in the course of carrying out our services or conducting our business. These third parties may include, where appropriate:

(a) our related companies within the HPX Group, and entities with which we have licensing or other partnership agreements or arrangements with (including Hamilton Locke (NZ) Limited);

(b) financial institutions for payment processing and fraud detection and management;

(c) credit reference agencies, so far as it relates to clients who instruct their credit card issuer to cancel payment to us without having first provided an acceptable reason to us;

(d) our service providers, including our outsourced identity verification and fraud prevention service providers, back-office service providers (for services such as IT support, word processing and billing assistance), data storage, marketing, promotional and market research agencies and external business advisers (such as auditors);

(e) regulators and law enforcement agencies, where required by law;

(f) in the case of a sale of our business (in whole or in part) to the purchaser (as an asset of the business); and

(g) if you are a job applicant, referees whose details you provide to us.

Our business works closely with other organisations, such as government departments and agencies, other law firms, barristers, accountants, real estate agents, financial planners, insurers, local business and industry networks, business and industry alliances, auditors and other consultants. We routinely disclose Personal Information to these third parties where it is reasonably necessary for them to assist us to provide our legal services to you, or to enable them to provide related service offerings that you have requested.

We may also disclose your personal information to other third parties and for other purposes where we are required or authorised by or under law to do so (including where you have provided your consent).

7. Direct marketing

We may use your Personal Information so we can contact you with information about our products and services, events, activities and legal developments and insights that may be of interest to you.

We may contact you by email, mail or telephone. You can let us know at any time if you no longer wish to receive these communications, by contacting us (using the contact details at the end of this policy) or using the opt-out/unsubscribe facility in our communications.

If you are a client or have otherwise expressed interest and provided us with your contact details, we may send emails to you with information about legal developments (such as publications, alerts and newsletters) and marketing our services (such as seminar invitations).

8. Websites and eStore

When you access our Websites (including our eStore), we may collect information from and about your device including:

(a) your Internet Protocol (IP) address;

(b) browser type;

(c) language preference;

(d) referring site;

(e) the date and time of each visitor request;

(f) Website usage statistics, such as the pages viewed, and the length of time viewed; and

(g) where you have identified yourself to us (for example, by completing a form, making an enquiry, or making a purchase), information collected by tracking pixels linking your device or browser activity on our Websites to you, for the purposes described in the Tracking Pixels section below.

Where we collect only the information described in paragraphs (a) to (g) above and you have not identified yourself to us, we generally cannot identify you from this information alone. However, where you have identified yourself (for example, by making a purchase through our eStore, completing a form, or logging in), the information described above may be linked to you and will be treated as Personal Information. Where that information is not linked to an identified individual, it will be used and disclosed by us in aggregated or de-identified form only, for purposes including statistical analysis, website and eStore development, and measuring the effectiveness of our marketing.

We also use cookies, tags and similar technologies on our Websites (including our eStore) to display personalised content, serve relevant advertising, measure the performance of our marketing campaigns, and store your preferences on your computer. On our eStore, these technologies are enabled by default when you visit the site.

A cookie is a string of information stored on your device which is used to identify a unique visitor. We use cookies to help identify and track visitors, their usage of the Website, and their website access preferences.

You can manage your cookie and tag preferences, or opt out of or limit use of non-essential cookies and similar technologies, by configuring your browser or device settings or by contacting us using the details set out at the end of this Privacy Policy.

Google Analytics

We use Google Analytics to understand how people use our Websites and eStore. This involves cookies and tags that collect information about your browsing activity. You can opt out of Google's advertising features through your Google account settings, browser add-ons (including the Google Analytics Opt-out Browser Add-on, available at tools.google.com/dlpage/gaoptout) or your device's privacy settings. Google provides various tools and options to control how your data is used for advertising purposes. You can learn more about how Google uses your data and your available options on Google's privacy pages. However, if you choose to disable or restrict cookies or tags, you may not experience optimum performance of our Websites or eStore, and some personalised features may not be available to you.

9. Tracking Pixels

What are tracking pixels?

A tracking pixel (sometimes called a web beacon) is a small, often invisible, piece of code embedded in our Websites, in our emails, or on third-party websites or platforms. It lets us and our service providers know when you have visited a page or opened a message and can allow information about your visit to be shared with the relevant analytics, marketing or customer relationship management provider.

Limiting tracking pixels

You may be able to limit tracking pixels by adjusting your browser or device settings, or by using any opt-out tools that our service providers make available. You may also contact us using the details set out at the end of this Privacy Policy if you require assistance managing your preferences. However, if you disable tracking pixels, some personalised features may not be available to you.

eStore analytics and advertising measurement

Where you browse or make a purchase through our eStore, the following additional information may be collected by us or on our behalf through cookies, tags and similar technologies:

(a) page-view and device data (such as pages visited, browser type, screen resolution and referring URL);

(b) product browsing behaviour (such as items viewed, searches performed and categories browsed);

(c) completed purchase details, including order value, items purchased and a transaction or order identifier;

(d) an advertising-click identifier that links your purchase or site visit back to a specific advertisement; and

(e) a cryptographic hash of your email address, which is shared with Google as part of its "enhanced conversions" feature to measure advertising effectiveness. Although this value is derived from your email address using a one-way hashing process, both we and Google are capable of re-identifying you from it (for example, by matching the hash to a known account). We therefore treat this hashed identifier as Personal Information.

This information is collected and shared with Google (via its analytics and advertising services) for the purposes of:

(a) measuring and reporting on the performance of our advertising campaigns;

(b) understanding how visitors interact with our eStore;

(c) attributing purchases to specific advertising channels; and

(d) optimising the content and targeting of our advertising.

A record of your consent preferences and a consent-state snapshot is recorded with each order.

We may in the future enable similar analytics and advertising measurement through additional platforms (such as Meta and LinkedIn). Where we do so, this Privacy Policy will apply to the information collected through those platforms in the same way, and we will update this section where practical. Updated details of the platforms in use can be obtained by contacting our Privacy Officer.

10. Overseas disclosure

Some of our service providers are located outside Australia. As a result, Personal Information collected and held by us may be transferred to recipients in other countries. In particular, we may disclose Personal Information to our service providers located in India and The Philippines, so that they can provide us with services in connection with the operation of our business, such as financial administration and related services. Some of our marketing, analytics and customer relationship management service providers who use tracking pixels may also be based, or store or process data, overseas.

Where your matter is international in nature, we may need to disclose your Personal Information to third parties based overseas. The countries in which these overseas recipients may be located will depend upon the individual circumstances of your matter.

11. How we hold, store and protect Personal Information

We generally hold Personal Information in computer systems, including computer systems operated for us by our service providers. We do maintain some paper records which contain Personal Information. We take reasonable steps to protect Personal Information from misuse, interference, loss, and from unauthorised access, modification or disclosure. This includes taking appropriate security measures to protect access to our premises and physical files, and to electronic materials, and requiring our service providers to do so.

12. Requests for access and correction

You have a right to request access to your Personal Information we hold and request its correction if it is inaccurate, out of date, incomplete, irrelevant or misleading. You may do so by contacting our Privacy Officer at the details below.

We take reasonable steps to ensure that your Personal Information we hold is accurate, complete and up to date. However, we encourage you to tell us if your Personal Information changes or if you believe or suspect it may not be correct.

We will respond to all requests for access to or correction of your Personal Information within a reasonable period.

In most cases, we will comply with such requests. If, for whatever reason, we do not, we will give you written reasons why. We may charge an access fee to cover the cost of retrieving the information and supplying it to you. For further information, please contact us at the address below.

13. Complaints and concerns

Please contact us at the address below if you would like any further information, or have any concerns or complaints about the manner in which we have collected or handled your personal information, or would like to complain about a breach of the APPs. We will respond to complaints within a reasonable period of time (usually 30 days).

If you are not satisfied with our response, you can contact us to discuss your concerns or lodge a complaint with the Office of the Australian Information Commissioner at oaic.gov.au, calling 1300 363 992 or emailing enquiries@oaic.gov.au.

14. Contact

If you would like more information about the way we manage personal information, would like to request access to or correction of personal information that we hold about you, or wish to make a complaint, please contact:

Privacy Officer
HPX Group
Level 37, 180 George Street
Sydney NSW 2000

P: (02) 8072 8271

E: privacy@hpxgroup.com.au

15. Changes to our privacy policy

From time to time, it may be necessary for us to review and revise our Privacy Policy. We may notify you about changes to this Privacy Policy by posting an updated version on our Website. We encourage you to check our Website from time to time to ensure you are familiar with our latest Privacy Policy.

This Policy was last updated in October 2026.