

InfoTrack Privacy Policy

InfoTrack Pty Limited ABN 36 092 724 251 (“**InfoTrack**” or “**we**”, “**our**” or “**us**”) is bound by the *Privacy Act 1988* (Cth) (as amended), including the Australian Privacy Principles (“**Privacy Act**”). This Privacy Policy sets out how we treat the personal information that we collect, use and disclose and our procedures regarding the handling of personal and sensitive information, including the collection, use, disclosure and storage of information, as well as the right of individuals to access and correct that information.

From time to time, we may revise or update this Privacy Policy or our information handling practices. If we do so, the revised Privacy Policy will be published on our websites, www.infotrack.com.au and www.infotrackgo.com

InfoTrack may collect personal information in order to conduct our business, to provide and market our services and to meet our legal obligations. By using our website or our services, or by providing any personal information to us, you consent to the collection, use and disclosure of your personal information as set out in this Privacy Policy.

The performance of our functions and activities, including our collection, use, storage, retention, security and disclosure of your personal information is in accordance with all relevant privacy laws including the Privacy Act and the *Australian Crime Commission Act 2002* (“**ACC Act**”).

The types of personal information we collect and hold

The types of personal information we may collect and hold includes (but is not limited to) personal information about:

- clients, business associates and potential clients and their employees;
- suppliers and their employees; and
- prospective employees and contractors.

Personal information that we collect and hold may include:

- your name, address, contact telephone number and other contact details such as your email address;
- payment information (such as credit card or bank details);
- other personal information required to provide our services in specific cases, for example certain information to complete property transactions, if relevant;
- details required to obtain National Coordinated Criminal History Checks supplied by the Australian Criminal Intelligence Commission (“**ACIC**”) and the National Police Checking Service (“**NPCS**”), such as all names the Applicant has previously been known by, date of birth, residential history, biometric information, demographic information, information relating to an Applicant’s check purpose and information or opinion relating to an Applicant’s current or previous application process; and

- details of your use of our products or services.

You are not obliged to provide personal information to InfoTrack. However, in many cases, if you do not provide your personal information to us, we may not be able to supply the relevant product or service that you have requested from us.

In some circumstances, you may provide to us, and we may collect from you, personal information about a third party. Where you provide the personal information of a third party, you must ensure that the third party is aware of this Privacy Policy, understands it and agrees to accept it.

If it is necessary to provide specific services to you, we may collect sensitive information about you. Under the Privacy Act, “sensitive information” includes but is not limited to information or an opinion about an individual’s racial or ethnic origin, religious belief, or criminal record and also includes health information about an individual. However, we will only collect sensitive information from you if you agree to provide it to us, you authorise us to obtain it from a third party or where the collection of the information is required or authorised by or under an Australian law or a Court/Tribunal order or otherwise where the collection is not prohibited under the Privacy Act. We will only use sensitive information in accordance with the Privacy Act and for the purpose for which it is provided.

How personal information is collected and held by us

We collect personal information in the following ways:

- when you fill in and return to us a signed client form;
- when you submit personal information through our website (such as when you send us a message or fill out a form);
- in person, for example, when you engage with our HelpDesk and Property Services teams;
- when you connect to a third party or connect to our services via a third party, for example, an integration partner; and
- in the course of providing services to you.

We may also collect information about you from third party suppliers and government database services.

We are committed to protecting your personal information and take steps to protect your personal information against loss, unauthorised access, use modification or disclosure, including, for example:

- firewalls implemented across all office networks and sites;
- anti-virus software deployed on all workstations;
- cyber security training for all employees at point of onboarding and throughout the year;
- imposing restrictions on physical access to paper files;
- requiring any third parties engaged by InfoTrack to provide appropriate

- assurances to handle your personal information in a manner consistent with the Privacy Act; and
- taking reasonable steps to destroy or de-identify personal information after we no longer need it for our business or to comply with the law.

InfoTrack operates an Information Security Management System (“**ISMS**”) with full consideration of the ISO27001:2013 standard and with the support of our senior management. ISMS contains various policies which outline the security management measures we have applied to protect your personal information and safeguard against unauthorised access and unnecessary retention of your personal information in our systems. All employees and any contractors of InfoTrack must comply with our ISMS.

Staff accessing our system must pass appropriate security clearance requirements and access to systems are centrally restricted and monitored, including the use of suitable password protection measures.

All personal information we collect from you is stored in a secured location in Australia on infrastructure managed by InfoTrack. Data is encrypted during transit using current TLS protocol and stored encrypted at rest using AES-256 encryption.

Collection of personal information through website activity

Information that may identify you as a user may be gathered during your access with our website.

Our website includes pages that use ‘cookies’. A cookie is a unique identification number that allows the server to identify and interact more effectively with your computer. The cookie assists us in identifying what our users find interesting on our website.

A cookie will be allocated each time you use our website. The cookie does not identify you as an individual in our data collection process, however it does identify your Internet Service Provider.

You can configure your web browser to refuse cookies. If you do so, you may not be able to use all or part of our website.

Adoption, use and disclosure of government related identifiers

InfoTrack, or its related body corporates in the ATI Group, may collect some personal information that is a government related identifier.

Personal information from identity documents may be provided to the document issuer or official record holder via third party systems for the purpose of confirming

your identity, for example, the Australian Government's Document Verification Service (“**DVS**”). Where InfoTrack does collect government related identifiers, they are maintained on a separate database for audit and compliance purposes.

InfoTrack may use or disclose a government related identifier where:

- it is reasonably necessary for InfoTrack to verify the identity of the individual for the purposes of our business activities or functions; or
- as required or authorised by law or in accordance with the order of a Court or Tribunal, or where it is otherwise permitted to do so under the Privacy Act.

The purposes for which we collect, hold, use and disclose personal information

We collect, hold, use and disclose personal information for a variety of business purposes including:

- to provide the products or services you have requested from us;
- to process payments;
- to improve our business, products and services;
- to promote our business to you;
- to market other InfoTrack services or products to you;
- to handle and respond to your enquiries, complaints or concerns; and
- to provide personal information to third parties as set out in this Privacy Policy.

Direct marketing

We also collect, hold, use and disclose your personal information to:

- notify you about the details of new services and products offered by us;
- notify you of the details of meetings, events and seminars that may be of interest to InfoTrack customers and clients;
- send you our newsletters and other marketing publications;
- administer our databases for client service, marketing and financial accounting purposes; and
- to comply with our legal requirements regarding the collection and retention of information concerning the products and services that we provide.

If you do not wish to disclose your personal information for the purpose of direct marketing or you would like to opt-out of receiving direct marketing communications, you can do so by contacting the InfoTrack Privacy Officer using the contact details set out below, or by following the instructions to unsubscribe which are contained in a communication that you receive from us.

Who do we disclose personal information to?

The ATI Group and Related Companies

The ATI Group includes our parent company ATI Global Pty Ltd and its subsidiaries, LEAP Legal Software Pty Ltd, InfoTrack Group Pty Ltd and their subsidiaries, including CreditorWatch Holdings Pty Limited and its subsidiaries, CNCNA Pty Ltd (trading as eCompanies), InfoTrack Limited (NZ), InfoTrack Group Limited (UK) and its subsidiaries, and LotSearch Pty Ltd. Different companies within the ATI Group provide different services.

The ATI Group may share information with our integration partners to ensure the smooth running of the services which we, and they, provide. These partners include Sympli Pty Ltd, Practice Evolve Group Pty Ltd and its subsidiaries, Legal Software Developments Pty Ltd and its subsidiaries, and other partners as mentioned on our website and updated from time to time. At times, we may need to provide personal information to them to help them run their businesses or for reporting purposes. We may also share your personal information within the wider ATI Group and with our service providers for the purposes outlined above.

Third Party Service Providers

We may disclose your personal information to third party service providers who assist us in providing the services you request, including public authorities and providers of information services.

We may also disclose your personal information to third parties who work with us in our business to promote, market or improve the services that we provide, including:

- providers of customer relations management database services and marketing database services;
- marketing consultants, promotion companies and website hosts; and
- consultants and professional advisers.

We may also combine your personal information with information available from other sources, including the entities mentioned above, to help us provide better services to you.

Where we do share information with third parties, we require that there are contracts in place that only allow use and disclosure of personal information to provide the service and that protect your personal information in accordance with the Privacy Act.

Otherwise, we will disclose personal information to others if you've given us permission, or if the disclosure relates to the main purpose for which we collected the information and you would reasonably expect us to do so.

ACIC, NPCS and Nationally Coordinated Criminal History Checks

A specific third party service provider who we may disclose personal information to

is ACIC and NPCS, for the purposes of obtaining National Coordinated Criminal History Checks. Should ACIC and NPCS conduct audits upon us from time to time, we may also collect and provide data to them for the purposes of compliance with such audits.

ACIC and NPCS use this personal information to disclose to us police information relating to you, including Nationally Coordinated Criminal History Checks, to update records held about you and for law enforcement, including purposes set out in the ACC Act.

Our relationship with ACIC and NPCS as a third party service provider is governed by a contractual arrangement, such contract being the *Agreement for controlled access by duly Accredited Bodies to Nationally Coordinated Criminal History Checks*.

Data collected for the purposes of obtaining National Coordinated Criminal History Checks from ACIC and NPCS is held by us for no less than 12 months, but no more than 15 months, following collection.

The Privacy Act and ACC Act authorise and apply to us in relation to the collection, use, storage, security and disclosure of your personal information for the purpose of this service.

National Police Checking Service (NPCS)

GPO Box 1936, Canberra City ACT 2601

NPCS@acic.gov.au

(02) 6268 7000

Disclosure of personal information to overseas recipients

We do not presently disclose personal information to any organisations located overseas; however, we do disclose information in Australia, for the purposes described above, to some multinational organisations that are located both in Australia and overseas, including the United Kingdom, the United States and New Zealand.

With respect to Nationally Coordinated Criminal History Checks provided by ACIC and NPCS, no data collected for the purposes of this service will ever be transferred or stored outside of Australia, unless InfoTrack applies for, and is granted, a Permitted Offshore Transfer arrangement with the ACIC.

European Union – General Data Protection Regulation (GDPR)

If you are a resident of the European Union for the purposes of the GDPR, then in addition to what is set out above, the following applies to you.

InfoTrack is a data controller and processor for the purposes of the GDPR and by your consenting to this Privacy Policy, InfoTrack is able to process your Personal Information in accordance with this Privacy Policy.

In providing services to you, InfoTrack may make use of a number of automated processes using your Personal Information and your activity on our site as tracked by us, in order to provide more tailored and relevant services to you.

In addition to your rights set out above, you may update or rectify any of your Personal Information that we hold about you, in the manner described in the “How you can access your personal information” paragraph above.

How we handle requests to access your personal information

You have a right to request access to your personal information which we hold about you. You can make such a request by contacting the InfoTrack Privacy Officer using the contact details set out in this policy.

We will respond to any such request for access as soon as reasonably practicable. Where access is to be given, we will provide you with a copy or details of your personal information in the manner requested by you where it is reasonable and practicable to do so.

We will not charge you a fee for making a request to access your personal information. However, we may charge you a reasonable fee for giving you access to your personal information.

In some cases, we may refuse to give you access to the information you have requested or only give you access to certain information. If we do this, we will provide you with a written statement setting out our reasons for refusal, except where it would be unreasonable to do so.

How we handle requests to correct your personal information

We will take such steps (if any) as are reasonable in the circumstances to make sure that the personal information we collect, use or disclose is accurate, complete, up to date and relevant.

If you believe the personal information we hold about you is inaccurate, irrelevant, out of date or incomplete, you can ask us to update or correct it. To do so, please contact us using the contact details listed below. Our Helpdesk or Sales staff can generally assist with updating your personal information immediately over the phone, however if you are unhappy with the handling of your request to update or correct your personal information, you may request that the matter be escalated to our Privacy Officer for further review.

If we refuse your request to correct your personal information, we will let you know why. You also have the right to request that a statement be associated with your personal information that says you believe it is inaccurate, incomplete, irrelevant, misleading or out of date.

How to contact us or make a complaint

If you have any questions about this Privacy Policy, if you wish to correct or update information we hold about you or if you wish to request access to your personal information or make a complaint about a breach by InfoTrack of the Australian Privacy Principles (including the way we have collected, disclosed or used your personal information), please contact our Privacy Officer by post, email or phone via the below details:

InfoTrack Privacy Officer
GPO Box 4029 Sydney NSW 2001
legal@infotrack.com.au
1800 738 524

When you make the complaint please identify yourself, including your contact details, provide a brief description of the matter and why you think InfoTrack has mishandled your information, and how you would like us to resolve the matter.

We will then acknowledge, investigate and respond to any complaint as soon as practicable, but within a period of no more than 30 days. You can call us at any time during this period to check on the status of your complaint. We will take reasonable steps to remedy any failure to comply with our privacy obligations, however if you are unhappy with the handling of your complaint by our Privacy Officer, you may let us know that you would like the matter to be escalated for further internal review.

If you are still unhappy with our handling of the complaint, you may contact the Office of the Australian Information Commissioner at <https://www.oaic.gov.au/>

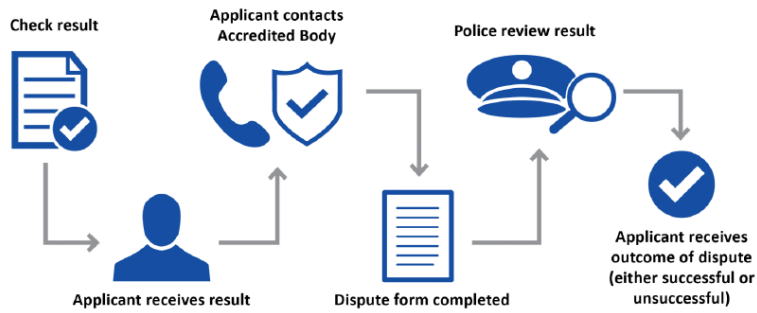
Nationally Coordinated Criminal History Check Disputes

If you believe there is an error or problem dispute regarding a Nationally Coordinated Criminal History Check result, as supplied by ACIC and NPCCS, please contact us via the above details to raise a dispute and provide us with any additional information and supporting evidence.

We will action and escalate all raised disputes by completing a Dispute form on your behalf and providing this form, together with any additional supporting documentation provided by you, to NPCCS. The relevant police agency and NPCCS will then review the dispute and provide a dispute outcome (and where possible, reasoning for the outcome) which we will share with you.

The period of time to resolve a dispute process can vary depending on the complexity of the matter.

DISPUTES



Last update: 20 April 2020