Privacy Policy

Introduction

Precise Background Services Pty Ltd as trustee of the Precise Background Services Trust ("**us**", "**our**" or "**we**") are committed to protecting the privacy of your Personal Information.

This Privacy Policy tells you how we will handle your Personal Information in accordance with the *Privacy Act* 1988 (Cth) ("**Privacy Act**"). If you use our Services to submit a national police check, we will also comply with the Australian Privacy Principles ("**APPs**").

Please note that any information that is not Personal Information that we collect, process or otherwise use will not be governed by this Privacy Policy.

All capitalised terms in this Privacy Policy have the meaning given to that term in the Schedule "Definitions" unless the context requires otherwise.

1. When does this Privacy Policy apply to me?

This Privacy Policy applies when you visit the Site or use any of our Services. By visiting the Site or by using any of our Services, you agree to the terms of this Privacy Policy. You should not access the Site or use any of our Services if you do not agree with this Privacy Policy.

If you do not allow us to collect all the Personal Information we reasonably request, we may not be able to deliver any of our Services to you.

While you have a right not to identify yourself to us (for example by using a pseudonym), given the nature of the Services we provide, we may not be able to provide you with our Services.

2. What Personal Information do we collect?

We collect and use Personal Information from you using our Services. We may also collect your Personal Information from third parties if you consent to us doing so, or we are required or authorised under an Australian law to collect the information from a third-party. The specific type of Personal Information that we collect will depend on the reasons for, or circumstances of its collection and may include, but is not limited to, the following:

- **User information:** name, telephone, date of birth, phone number, email address, identity documents (including passport, drivers licence and Medicare card) and residential and postal address;
- **Criminal history information:** including charges, good behaviour bonds, pending matters awaiting court hearing or past convictions, and other reports from law enforcement bodies – all criminal history information is Sensitive Information;
- **Payment and transactional information:** banking, credit card or debit card details, billing information, Device information and Technical Usage Data; and
- **Enquiries, communications and social media:** information contained in any enquiry you submit to us regarding our Portal or any of our Services, communication content, metadata associated with communications and information about you shared by social media portals (if you communicate with us by way of a social media portal that we use).

We will only collect, hold, and use your Sensitive Information with your informed consent and if such information is reasonably necessary for, or directly related to, one or more of our Services, or otherwise in accordance with the Privacy Act.

If we receive unsolicited Personal Information from you or a third-party, we will determine whether we are entitled to collect such information in accordance with the Privacy Act or the APPs. If we determine that we are not entitled to do so, we will destroy the information or ensure that the information is de-identified as soon as practicable.

3. How do we collect Personal Information?

We may collect your Personal Information directly from you or in the course of our dealings with you. For example, we collect Personal Information from you or about you from:

- your use of any of our Services;
- correspondence between you and us;
- external sources like the Australian Criminal Intelligence Commission and other governmental agencies from which we source information from in the provision of our Services;
- visits to and submissions you make on our Site;
- your interactions with our electronic direct mail and/or emails from our marketing campaigns (such as clicks on links included in these emails); and
- registration and forms you may fill in for our marketing-related activities and events.

In some instances, we may receive Personal Information about you from third parties, including our related entities, government agencies and regulatory authorities. We may also receive Personal Information about you from your authorised third parties and publicly available sources.

4. Why do we collect, hold and use Personal Information?

We collect, hold and use your Personal Information for the purposes of providing you with access and usage of the Portal and the Services, which include (without limitation):

- confirming your identity – for example, to confirm that the person making the application and giving consent and the identity of the subject of the check are the same;
- providing you with our Services – for example, we need to collect Personal Information (e.g. names, date of birth, address history) from you to order a check;
- ongoing client relationship management purposes;
- offering, promoting, advertising, marketing and selling relevant and suitable Services to you;
- sending you relevant notifications, electronic direct mail, email marketing campaigns and/or newsletters;
- any other purposes identified at the time of collecting your Personal Information;
- developing and improving our business and/or any of our Services;

- for monitoring, research and analysis in relation to our business, the Portal and any of our Services;
- involving you in market research, gauging customer satisfaction and seeking feedback;
- performing and supplying any of our Services to you;
- managing our relationship with you (including maintaining a user profile), communicating with you, identifying you when you contact us, responding to your enquiries and keeping records;
- processing payments you have authorised;
- complying with all of our legal obligations to you and to third parties (including, without limitation, any governmental authority.
- ensuring the security of our Services and maintaining back-ups of our database(s);
- where we reasonably suspect that unlawful activity has been, is being or may be engaged in and the use or disclosure is a necessary part of our investigation or in reporting the matter to the relevant authorities;
- in the preparation for, or conduct of, court proceedings or in an administrative or out-of-court procedure (or the implementation of orders of a court or tribunal or on behalf of an enforcement body);
- for the purpose of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice; and
- where we reasonably believe that use or disclosure is necessary to lessen or prevent a serious, immediate threat to someone's health or safety or the public's health or safety.

Where we wish to use or disclose your Personal Information for other purposes, we will obtain your consent.

5. Will my Personal Information be disclosed to third parties?

We may need to disclose your Personal Information to third parties, including:

- to our related entities as necessary for the provision of any of our Services or to enable them to provide any of the service offerings that you have requested;
- to government agencies to enable relevant registrations, notifications and/or lodgements in connection with the Portal and/or our Services (in the case of an Australian nationally coordinated criminal history check, this includes the Australian Criminal Intelligence Commission), who may pass your Personal Information on to other law enforcement bodies;
- to a person that you have authorised to use the Portal or any of our Services on your behalf;
- if you enable third party applications to be used in conjunction with the Portal and/or any of our Services, to those third party applications;
- to our partners, contractors, suppliers, subcontractors and service providers, including without limitation our suppliers of IT based solutions that assist us in providing any of our Services, distributors of direct marketing communications, marketing agencies, insurers and external business advisors, but only to the extent that they have contractual obligation to keep your Personal Information confidential and protected;
-

- in accordance with requirements or authorisations under applicable laws or to comply with our legal obligations; and

- to any other persons that you would reasonably expect us to disclose to for purposes contemplated by the Services or this Privacy Policy.

We take reasonable steps to ensure that third party recipients are obliged to protect the privacy and security of your Personal Information and use it only for the purpose for which it is disclosed.

6. Will my Personal Information be transferred internationally?

Disclosure to third parties overseas

To the extent we are permitted by law and by any government agency we engage with in the provision of the Services, occasionally, we may be required to disclose your Personal Information to third parties outside of Australia in connection with the provision of Services or other purpose permitted by the Privacy Act. If we make such disclosure, we will take reasonable steps to ensure that those third parties, in whichever jurisdiction, adhere to the APPs.

7. How do we hold and store Personal Information?

Your Personal Information is held and stored on paper and/or by electronic means. We have physical, electronic and procedural safeguards in place to protect your Personal Information and take reasonable steps (including by the use of industry-standard, physical procedural and technical security measures and encryption) to ensure that your Personal Information is protected from misuse, interference, loss and unauthorised access, modification and disclosure, including:

- Implementing and maintaining an information security policy that governs, the type or class of information that the policy applies to, information security roles and responsibilities relating to Personal Information, security clearance requirements and our employees' and contractors' responsibilities, configuration and change control, technical access controls, staff training, networking and connections to other systems, physical security (including media security), and incident management;

- Securing our computer systems by maintaining an appropriately configured gateway environment (including firewalls), restricting file system permissions, updating and patching operating systems, running up-to-date anti-virus software;

- Protecting your digital Personal Information using internal and external firewalls. We encrypt and/or pseudonymise Data wherever possible. All access to your Personal Information including databases requires password access that meets industry complexity standards;

- Restricting access to Personal Information to staff and contractors whose job description requires access. Our employees and contractors are contractually obliged to maintain the confidentiality of any Personal Information held by us;

- Implementing multi-factor authentication safeguards wherever possible and appropriate;

- Storing Personal Information within secure facilities. We also require our storage contractors to implement privacy safeguards;

- Regularly training our staff on privacy and data protection procedures.

However, regardless of any security measures used, we cannot guarantee the absolute protection and security of any Personal Information stored with us or with any third parties, and therefore you should be aware of the inherent risks of loss and unauthorised access, use, modification or disclosure involved in disclosing your Personal Information.

8. How long will my Personal Information be retained?

We will retain your Personal Information only for as long it is required for any of the purposes set out in this Privacy Policy or for any other lawful purpose. We will retain your Personal Information for the time periods required by law, and in respect of certain Services, as long as required by the government agencies we engage to provide those Services.

We use secure methods to destroy or de-identify your Personal Information when it is no longer needed or legally required to be retained. Paper records are sent for secure destruction.

Electronic records may be archived to alternative storage and are subject to the procedural safeguards described above.

9. What direct marketing will be undertaken?

We may use and disclose your Personal Information (but not your Sensitive Information) for the purpose of direct marketing to you by way of a direct mail, email, SMS, MMS, targeted digital advertising or any other means of marketing communication, where:

- you have consented to us doing so; or
- it is otherwise permitted by law.

You may opt out of direct marketing communications at any time by contacting us or by using opt-out facilities set out in the direct marketing communications.

10. Will I be able to access and control my Personal Information?

You have a right to request access to or correction of your Personal Information held by us. If you wish to access, correct or update any Personal Information that we hold about you, please contact us via the details below in section 13.

We will respond to your request within one month of you making the request and give you access in the manner you requested unless it is unreasonable or impracticable for us to do so. Before we accept your request, we will need to use reasonable methods to verify your identity.

There may be reasons why we cannot give you access to the information that you have requested, or we refuse to correct your Personal Information (for example, it is commercially sensitive or if it also contains someone else's personal information) provided such refusal is permitted by law or permitted under any contractual arrangement we have with any government agency in providing the Services. In these instances, we will let you know these reasons in writing. To assist us to keep our records up to date, please notify us of any changes to your Personal Information.

11. Can I withdraw my consent to hold my Personal Information?

You have a right to withdraw your consent to us using your Personal Information at any time. Please note that by withdrawing your consent, we may no longer be able to provide you with access to our Services.

Please contact us via the details below if you would like to make such a request. We will process a request within one month. We will use secure methods to destroy or de-identify your Personal Information when it is no longer needed or legally required to be retained.

12. Will I have the opportunity to provide feedback?

From time to time, you may have the option to participate in surveys or provide feedback intended to improve any of our Services which may involve providing additional Personal Information. Your participation in such activities is subject to your consent.

13. Who do I contact if I have a complaint?

We have procedures in place for dealing with complaints and concerns about our practices in relation to the Privacy Act, the APPs, and any alleged breach of this Privacy Policy. We will respond to your complaint in accordance with the relevant provisions of the APPs. For further information, please contact us using the details below:

Privacy Officer
Level 27, 101 Collins Street, Melbourne, Victoria, 3000
Email: support@precisebackground.com
Phone: 1300 557 556

If you are not satisfied with our response to your complaint, or you consider that we may have breached the APPs or the Privacy Act, a complaint may be made to the Office of the Australian Information Commissioner (**OAIC**). The OAIC can be contacted by telephone using contact details below or by using the contact details on the OAIC website.

Office of the Australian Information Commissioner

Phone:	1300 363 992
Teletypewriter (TTY):	133 677 then ask for 1300 363 992.
Speak and Listen users:	1300 555 727 then ask for 1300 363 992

14. Will this Privacy Policy change?

We may update our Privacy Policy from time to time by either notifying you of a change to our Privacy Policy and providing you with the updated Privacy Policy or publishing a new version on our Portal.

Our Privacy Policy was last updated on **4 February 2024**.

By continuing to use our Site or otherwise continuing to use our Services, you accept this Privacy Policy as it applies from time to time.

15. Schedule - Definitions

"**Data**" means any data inputted by you or with your authority through the use of the Services and includes, without limitation, data owned or supplied by you or data which may otherwise be generated, compiled, arranged or developed by you in using the Services pursuant to these Terms of Use.

"**Device**" means any type of device including a computer, mobile phone, tablet or console that meets the minimum specifications required to access to the Portal and/or use any of our Services.

"**Device Information**" means Data that can be automatically collected from any device used to access the Portal and/or any of our Services, including your Device type, your Device's network connections, your Device's name, your Device's IP address, information about your Device's web browser and the internet connection used to access the Portal or any of our Services, Geolocation Information, information about apps downloaded to your Device and biometric Data (such as Touch ID/Fingerprint).

"**Geolocation Information**" means information that identifies your location by using longitude and latitude coordinates obtained through GPS, Wi-Fi or cell Portal triangulation.

"**Portal**' means the 'PBS Portal' being the cloud-based background check software.

"**Personal Information**" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained and includes Sensitive Information (unless stated otherwise);

"**Sensitive Information**" means: (a) Personal Information that is also information about an individual's racial or ethnic origin, political opinions, membership of a political association, philosophical beliefs, religious beliefs or affiliations, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record; (b) health information (as defined in section 6FA of the Privacy Act) about an individual; (c) genetic information about an individual that is not otherwise health information (as defined in section 6FA of the Privacy Act); (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

"**Services**" means any and all services provided by us from time to time, including the Site and Portal.

"**Site**" means the website operating from the domain at "precisebackground.com" or such other domains used by us from time to time for access to this site or any other sites or provision of any of our Services.

"**Technical Usage Data**" means information we collect from your Device that you use to access the Portal or any of our Services such as what you have searched for and viewed on the Portal, the length of your visit and the way you use any of our Services, including your IP address, statistics regarding how pages are loaded or viewed, the website you viewed before coming to the Portal and other usage and browsing information collected through cookies.

"**User**" means a user of the Portal and/or any of our Services, as the context requires.