

National Credit Insurance (Brokers) Pty Ltd

Privacy Policy

Effective: 16th October 2023

This policy sets out how National Credit Insurance (Brokers) Pty Ltd (**NCI**) ABN 68 008 090 702 and any registered business names thereof will manage personal information that we deal with in providing services to our clients.

NCI are bound by the Privacy Act 1988 (as amended by the Privacy Amendment (Enhancing Privacy Protection Act 2012 and the Notifiable Data Breaches Act 2017)) (the **Act**) and must comply with obligations outlined in the Act. This policy does not limit or exclude any of your rights under the Act. If you wish to seek further information on the Act, see www.oaic.gov.au

Personal Information

Personal information refers to any information or opinion, whether true or not, about a living individual that can reasonably allow the individual to be identified.

If you are an individual who is either based in or a resident of Australia, the European Union or the United Kingdom, subject to applicable Privacy Laws, we will not process sensitive information about you unless we have received your express consent to the processing of this information.

How we collect personal information

We collect personal information where:

- You provide that personal information to us, including via our website and any related service, through any registration or subscription process, through any contact with us (e.g, telephone or email), or when you buy our services and products.
- Information is publicly available or acquired from a third party.
- You authorise us to contact such third parties for the purposes of providing you with the services that you have requested.

Why we collect, use and disclose personal information

- Process applications for credit limits on behalf of our clients to obtain trade credit insurance on their debtors.
- Review existing applications for insurance.
- Assess personal guarantees (current and prospective) for provision of NCI services.
- Processing and analysing applications for credit limits to provide recommendations and opinions.
- Undertake debt collection services.
- Compiling Credit Reports.
- Reviewing personal guarantees to assist in collection of client's debt recovery.
- Business development purposes and direct marketing.
- Managing and responding to your requests and queries, including complaints.
- Internal and external audit being conducted.

Legal basis for using your information if based in European Union or United Kingdom

If you are an individual who is either based in or a resident of the European Union or the United Kingdom, we will only collect, use and share your personal information where we are satisfied that we have an appropriate legal basis to do this. We will make sure that we only use your personal information for the purposes set out above and where we are satisfied:

- We need to use your personal information to perform a contract or take steps to enter into a contract with you;
- We need to use your personal information for our legitimate interest as a commercial organisation. For example, we may collect your personal details so that we can respond to enquiries submitted via our website. In all such cases, we will look after your information at all times in a way that is proportionate and respects your privacy rights and you have a right to object to processing as explained in the "accuracy, access and correction of your personal information" section of this Privacy Policy below;
- We need to use your personal information to comply with a relevant legal or regulatory obligation that we have; or
- We have your consent to using your personal information for a particular activity.

Identification

In circumstances where required for us to operate our business we will ask for your identification.

It is likely it will be impractical for us to interact with you without some form of identification. For example we will not be able to open a trade credit insurance account or debt collection recovery account without obtaining identification details.

Personal information collected

The type of personal data we may collect from you includes:

- Name;
- Mobile phone number;
- Residential phone number;
- Office phone number;
- Residential address;
- Postal Address;
- Email Address;
- Age / Date of birth;
- Gender;
- Occupation;
- Driver's license number.

We will make reasonable effort to ensure the personal data collected is accurate and complete.

Use and disclosure of personal information

We may disclose your personal data for:

- The purpose to which it was provided to us;
- Purposes which are directly related to the purpose it was provided for; and
- Any other purposes to which you may have consented.

Further we may use and disclose personal information where any of the following occurs:

- You would reasonably expect that your information would be disclosed;
- We are required by law to provide your personal information to a government agency or other organisation;
- The disclosure of the information will prevent or lessen a serious threat to somebody's life or health;
- The disclosure of the information is reasonably necessary for the enforcement of criminal law or action against serious misconduct.

Disclosure to Credit Reporting Bodies (CRB's)

We may disclose your personal information to a CRB in accordance with the permitted disclosures as defined in the Act to the following CRB's:

Equifax Australia Information Services and Solutions Pty Ltd
GPO Box 964, North Sydney, NSW, 2059
Ph: 13 83 32
<https://www.equifax.com.au/privacy>

Illion
PO Box 7405 St Kilda Rd, Melbourne, VIC, 3004
Ph: 13 23 33
<https://www.illion.com.au/privacy-policy/>

A copy of the CRB's credit reporting policy will be available from their website listed above. We can provide a hard copy on request.

Your obligations when we provide you with personal information

If we give you, or provide you access to, the personal information of any individual, you must only use it:

- For the purposes we have agreed to; and
- In compliance with the Act and this privacy policy.

Use of personal information for direct marketing

When we collect your personal information, e.g., via email, post, SMS, app notification, telephone or targeted online advertisements, we may use your personal information to send you direct marketing communications about our insurance products or our related services. We limit direct marketing to a reasonable and proportionate level, and to send you communications which we believe may be of interest to you, based on the information we have about you.

You can choose to opt-out with respect to direct marketing. If you choose to opt out of direct marketing correspondence we will record this on our opt-out register.

You may opt-out of direct marketing at any time by emailing us at:
info@nci.com.au

Or you may click 'unsubscribe' at the bottom of any electronic marketing materials you receive from us.

Overseas data transfers

We may transfer personal data held about you outside Australia if permitted by law to countries including but not limited to New Zealand, Asia and United Kingdom.

We may use cloud computing solutions or data storage located overseas in which case information may be stored, under our control, on computer servers located outside Australia.

Some of the third party service providers to whom we disclose personal information are located in countries outside of your country of residence, for example, Australia (or, in relation to New Zealand, outside New Zealand, or in relation to Singapore, outside Singapore) such as Malaysia, the Philippines, Vietnam, the United Kingdom, the European Union and the United States of America. In this regard, unless exempted by applicable Privacy Laws, we will either (a) seek your express or implied consent to do so prior to the transfer of your personal information overseas or (b) we will take reasonable steps to ensure that the overseas recipient does not breach the Privacy Laws applicable in relation to your personal information. Transfer of your personal information will only be made for one or more of the purposes specified in this Privacy Policy.

When we take reasonable steps, we will ensure that transfers of personal information are in accordance with applicable law and carefully managed to protect your privacy rights. We will ensure transfers are limited to either countries which are recognised as providing an adequate level of legal protection or where we can be satisfied that alternative arrangements are in place to protect your privacy rights. To this end:

- Where we transfer your personal information either outside our group of companies or to third parties who help provide our services, we obtain contractual commitments from them to protect your personal information; or
- where we receive requests for information from law enforcement or regulators, we carefully validate these requests before any personal information are disclosed.

You have a right to contact us for more information about the safeguards we have put in place (including a copy of relevant contractual commitments) to ensure the adequate protection of your personal information when this is transferred as mentioned above.

Your obligations when you provide personal information of others

You must not provide us with personal information (including any sensitive information) of any other individual unless you have the express or implied consent of that individual to do so. If you do provide us with such information about another individual, before doing so you:

- must tell that individual that you will be providing their information to us; and
- warrant that you have that individual's consent to provide their information to us.

If you have not done this, you must tell us before you provide any third party information.

Your obligations when we provide you with personal information

If we give you, or provide you access to, the personal information of any individual, you must only use it:

- for the purposes we have agreed to; and
- in compliance with applicable Privacy Laws and this Privacy Policy.

You must also ensure that your agents, advisers, employees and contractors meet the above requirements.

How personal information is secured

Your information may be held in an electronic or non-electronic form. We take reasonable steps to protect any personal information that we hold from misuse, interference and loss, and from unauthorised access, alteration and disclosure by:

- Password protection;
- Restricting access physically and electronically;
- Destruction and de-identification of the personal data once it is no longer required;
- Staff training in relation to handling personal data;
- Destruction of personal data that is unsolicited and which we were not permitted to collect, as soon as practicable.

However, data protection measures are never completely secure and, despite the measures we have put in place, we cannot guarantee the security of your personal information. You must take care to ensure you protect your personal information (for example, by protecting any usernames and passwords). You should notify us as soon as possible if you become aware of any security breaches. We will where required by applicable Privacy Law, notify you of any material security breach concerning your personal information as as soon as reasonably possible.

Links to third party sites

Our website may contain links to other third party websites. We do not endorse or otherwise accept responsibility for the content or privacy practices of those websites or any products or services offered on them. We recommend that you check the privacy policies of these third party websites to find out how these third parties may collect and deal with your personal information.

Use of cookies

We use cookies (an alphanumeric identifier that we transfer to your company's hard drive) which help provide additional functionality to the site or to help us analyse site usage more accurately. In all cases in which cookies are used, the cookie will not collect personal information without your consent. You can disable cookies by turning them off in your browser settings, however, our website may not function properly if you do so.

If you follow a link from our website to another website, please be aware that the owner of the other website will have their own privacy and cookie policies for their site. We recommend you read their policies, as we are not responsible or liable for what happens at their website.

Accuracy, access and correction of your personal information

We take reasonable steps to ensure that your personal information is accurate, complete and up to date whenever we collect, use or disclose it. However, we also rely on you to advise us of any changes to your personal information.

You are entitled to access personal information we hold about you. Should we hold personal information that is inaccurate, out of date, incomplete, irrelevant,

misleading or incorrect you have the right to make us aware of this fact and request that it be corrected. There are exemptions under the Act which may apply to personal information access and correction requests.

We are unable to provide you with access that is unlawful.

We require that you provide identification to verify the correct person is requesting the information or the change to the information. We will not charge you for making a request, however if reasonable we may charge you with the costs associated with complying with an information request.

We will respond to your request as soon as practicable, normally within 30 days in the manner you requested.

Requests for access to and/or correction of personal data held by us, should be made in writing addressed to:

The Privacy Officer

National Credit Insurance (Brokers) Pty Ltd
Level 2, 165 Grenfell Street, Adelaide, South Australia, 5000
Email: Privacyofficer@nci.com.au
Ph: 08 8228 4800

If we refuse access or correction to the information, written notice will be provided to you setting out:

1. The reasons for refusal (except where the grounds for the refusal would make it unreasonable to do so); and
2. The mechanisms available to complain about the refusal; and
3. Any other matter prescribed by the regulations.

Where your request is granted we will notify any relevant third parties we have disclosed the information to of the correction, where necessary and required.

Additional rights for individual based in or a resident of the European Union or United Kingdom

If you are an individual based in or a resident of the European Union or the United Kingdom, there are additional rights available to you. Please see below detailed rights including rights of access, erasures, rectification and portability of your personal data.

Right	What this means
Access	You can ask us to: • Confirm whether we are processing your personal information; • Give you a copy of that data; and • Provide you with other information about your personal information such as what data we have, what we use it for, who we disclose it to, whether we transfer it abroad and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, and where we got your data from, to the extent that information has not already been provided to you in this Privacy Policy.

Rectification You can ask us to rectify inaccurate personal information. We may seek to verify the accuracy of the data before rectifying it.

Erasure You can ask us to erase your personal information, but only where:

- it is no longer needed for the purposes for which it was collected; or
- you have withdrawn your consent (where the data processing was based on consent); or
- following a successful right to object (see 'Objection' below); or
- it has been processed unlawfully; or
- to comply with a legal obligation to which we are subject.

We are not required to comply with your request to erase your personal information if the processing of your personal information is necessary:

- for compliance with a legal obligation; or
- for the establishment, exercise or defence of legal claims.

Restriction You can ask us to restrict (i.e. keep but not use) your personal information, but only where:

- its accuracy is contested (see 'Rectification' above), to allow us to verify its accuracy; or
- the processing is unlawful, but you do not want it erased; or
- it is no longer needed for the purposes for which it was collected, but we still need it to establish, exercise or defend legal claims; or
- you have exercised the right to object, and verification of overriding grounds is pending.

We can continue to use your personal information following a request for restriction, where:

- we have your consent;
- to establish, exercise or defend legal claims; or
- to protect the rights of another natural or legal person.

Portability You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, but only where:

- the processing is based on your consent or on the performance of a contract with you; and
- the processing is carried out by automated means.

Objection You can object to any processing of your personal information which has our 'legitimate interests' as its legal basis, if you believe your fundamental rights and freedoms outweigh our legitimate interests.

Once you have objected, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms.

International
Transfer

You can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside of the European Economic Area or UK. We may redact data transfer agreements or related documents (i.e. obscure certain information contained within these documents) for reasons of commercial sensitivity.

Supervisory
Authority

You have a right to lodge a complaint with your local supervisory authority about our processing of your personal information. For example, in the UK, the supervisory authority for data protection is the ICO (<https://ico.org.uk/>). We ask that you please attempt to resolve any issues with us first, although you have a right to contact your supervisory authority at any time.

If you wish to access any of the above - mentioned rights, we may ask you for additional information to confirm your identity and for security purposes, in particular before disclosing personal information to you.

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality we owe to others, or if we are legally entitled to deal with the request in a different way.

Your consent and rights

By visiting our website, applying for or purchasing our products and services, you consent to the collection, use and disclosure of your information and other activities as specified in this privacy policy.

Administration of personal information

You may refuse or withdraw your consent for the collection, use and/or disclosure of your personal information in our possession by giving us reasonable notice so long as there are no legal or contractual restrictions preventing you from doing so. If you withdraw your consent for us to use your personal information for your insurance matters, this will affect our ability to provide you with the products and services that you asked for or have with us.

If the purpose for which your personal information is collected is no longer served by the retention of such data, or when the retention is no longer necessary for any other legal or business purpose, we will ensure that the hard copy of your personal information will be completely destroyed and electronic personal information as much as possible.

Complaints and queries

If you have a complaint or require further information about how NCI manage your personal data, please contact NCI's Privacy Officer on the contact details above.

You will need to provide us with sufficient details regarding your complaint together with any supporting evidence and information.

We will provide you with a receipt of acknowledgement as soon as practicable, normally within 30 days in the manner you requested.

In dealing with your complaint we may need to consult another credit provider or third party.

If we fail to deal with your complaint in a manner you feel is appropriate you may choose to make a complaint to the Information Commissioner below or by completing a Privacy Complaint Form available from their website:

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001

Email: enquiries@oaic.gov.au

Website: www.oaic.gov.au

Telephone: 1300 363 992

Facsimile: 02 9284 9666

Notification of serious harm

The National Data Breaches (NDB) Scheme applies to eligible data breaches that occur on or after 22nd February 2018.

A data breach occurs when personal information held by us is lost or subjected to unauthorised access or disclosure. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

If we suspect an eligible data breach may have occurred we will undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm.

The assessment will be completed within 30 calendar days after the day we became aware of the grounds (or information) that caused us to suspect an eligible data breach. If the assessment finds the data breach is likely to result in serious harm and we have not been able to prevent the likely risk of serious harm with remedial action, we will:

1. Notify the individual/s at likely risk of serious harm; and
2. Notify the Information Commissioner of the breach.

Changes to privacy policy and notice

We may amend this Privacy Policy at any time. A current version will be available by following the 'privacy policy' link located at the bottom of our website homepage at <http://www.nci.com.au>