Data Privacy Policy

OMNIA AUDIT V1 APRIL 2023

Our Commitment

Omnia Audit Pty Ltd (Omnia Audit, Us, Our, We) is committed to providing you with the highest levels of client service. We recognise that your privacy is very important to you. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) sets out a number of the Australian Privacy Principles (APPs). Our aim is to both support and ensure that we comply with these principles. Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner at http://www.oaic.gov.au This Privacy Policy discloses the purpose, and how the personal information that you provide to our representatives and us is collected, used, held, disclosed and disseminated. We encourage you to check our website regularly for any updates to our Privacy Policy.

Your Personal Information

Omnia Audit is subject to certain legislative and regulatory requirements under the Corporations Act and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. These may require us to obtain personal information about you including:

- your name, contact details,
- your occupation.

How We Collect Personal Information

In circumstances where Omnia Audit collects personal information directly from you or from third parties once authorisation has been provided by you. You have the right to refuse us authorisation to collect such information from a third party.

How We Use Your Personal Information

Primarily, your personal information is used so that we may provide advice to you. We may also use the information that is related to this primary purpose and it is reasonable for you to expect the information to be disclosed.

From time to time, we may provide you with direct marketing material. If, at any time, you do not wish to receive this information please tell us. We will endeavour to meet your request within two (2) weeks. We maintain a Register for those individuals not wanting direct marketing material.

When We May Disclose Your Personal Information

In line with modern business practices common to many institutions and to meet your specific needs we may disclose your personal information to the following organisations:

- compliance consultants;
- contractors or temporary staff to handle workloads during peak periods;
- mailing houses;
- insurance reference bureaus;
- your professional advisers, including your solicitor as authorised by you;
- information technology service providers;
- a potential purchaser/organisation involved in the proposed sale of our business for the purpose of due diligence, corporate re-organisation and transfer of all or part of the assets of our business. disclosure will be made in confidence and it will be a condition of that disclosure that no personal information will be used or disclosed by them;
- a new owner of our business that will require the transfer of your personal information;
- government and regulatory authorities, as required or authorised by law.

Our employees and any outsourcing companies or third-party contractors that we engage are obliged to respect the confidentiality of any personal information held by Omnia Audit.

As members of general insurance professional associations, we are required to meet an accepted standard of care. From time to time, we may need to provide these associations with access to your personal information to ensure that we are meeting our compliance requirements.

The Corporations Act 2001 (Cth) has provided the Australian Securities and Investments Commission with the authority to inspect certain personal information that is kept on our files about you.

We may collect information about you for the purpose of reporting to AUSTRAC under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

Omnia Audit takes its obligations to protect your personal information seriously, this includes when we operate throughout Australia and overseas. In some circumstances we may need to obtain your prior consent if it is likely that disclosure of personal information will be made to an overseas recipient.

How We Store and Secure Your Personal Information

We keep your personal information in your client files or electronically. These files are accessible to authorised personnel only and are appropriately secured. Access to same is subject to meeting confidentiality requirements.

Personal information is treated as confidential information and sensitive information is treated as highly confidential.

It is a legislative requirement to keep all personal information and records for a minimum of 7 years. Should you cease to be a client of ours, we will maintain your personal information on or off site in a secure manner for a period of 7 years after the date of our termination. After this, the information will be destroyed.

Ensure Your Personal Information Is Correct

Omnia Audit takes all reasonable precautions to ensure that the personal information we collect, use and disclose is accurate, complete and up-to date. To ensure we can maintain this level of accuracy and completeness, we recommend that you:

- make sure that the personal information that you provide us is clear, accurate and free from mis-statement;
- if there are any errors in your personal information to inform us as soon as practicable; and
- update us with any changes to your personal information as soon as possible.

If you provide inaccurate or incomplete information then we may not be able to provide you with the products or services you are seeking and/or our advice to you may be compromised.

Access To Your Personal Information

You have a right to access your personal information, subject to certain exceptions allowed by law. We ask that you provide your request for access in writing (for security reasons) and we will provide you with access to that personal information. Access to the requested personal information may include:

- providing you with copies;
- providing you with the opportunity for inspection; or
- providing you with a summary.

If charges are applicable in providing access to you, we will disclose these charges to you prior to providing you with the information.

Some exceptions exist where we will not provide you with access to your personal information. These includes circumstances where:

- providing access would pose a serious threat to the life or health of a person;
- providing access would have an unreasonable impact on the privacy of others;
- the request for access is frivolous or vexatious;
- the information is related to existing or anticipated legal proceedings between us and would not be discoverable in those proceedings;
- providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
- providing access would be unlawful;
- denying access is required or authorised by or under law;
- providing access would be likely to prejudice certain operations by or on behalf of an enforcement body or an enforcement body requests that access not be provided on the grounds of national security.

Should we refuse you access to your personal information, we will provide you with a written explanation for that refusal.

Using Government Identifiers

Although in certain circumstances we are required to collect government identifiers such as your tax file number or Medicare number, we do not use or disclose this information other than when required or authorised by law or unless you have voluntarily consented to disclose this information to any third party.

Dealing With Us Anonymously

You can deal with us anonymously where it is lawful and practicable to do so. For example, if you telephone requesting our postal address.

Your Sensitive Information

Without your consent we will not collect information about you that reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs or afflations, membership of professional or trade association, membership of a trade union, details of health, disability, sexual orientation, or criminal record.

This is subject to some exceptions including when:

- collection is required by law; and
- the information is necessary for the establishment, exercise or defence of a legal claim.

Our Website

Our website may provide links to third party websites. The use of your information by these third-party sites is not within our control and we cannot accept responsibility for the conduct of these organisations. Other websites are not subject to our privacy standards. You will need to contact or review those websites directly to ascertain their privacy policies.

You may register with us to receive newsletters and other information. By doing so, your name and email address will be collected and stored on our database. We take care to ensure that the personal information you give us on our website is protected. For example, our website has electronic security systems in place, including the use of firewalls and data encryption.

If you do not wish to receive any further information from us, or you wish to update your registration details, please email your request to us. We will endeavour to meet your request within 5 working days.

Our Website may utilise cookies to provide you with a better user experience. Cookies also allow us to identify your browser while you are using our site – they do not identify you. If you do not wish to receive cookies, you can instruct your web browser to refuse them.

Complaints Resolutions

Please contact our Privacy Officer if you wish to complain about any breach or potential breach of your privacy rights. Your complaint will be responded to within 7 days. If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Australian Information Commissioner (OAIC).

Privacy Officer: Jacob Solly
Phone: +61 2 9030 0010

Spam Policy

Spam is a generic term used to describe electronic 'junk mail'- unwanted messages sent to a person's email account or mobile phone. In Australia, spam is defined as 'unsolicited commercial electronic messages'.

The Australian Communications and Media Authority (ACMA) is responsible for enforcing the provisions of the Spam Act 2003 (Cth) (the Spam Act). Additional information about the Spam Act and the ACMA's role is available from: www.acma.gov.au 'Electronic messaging' covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone. Omnia Audit complies with the provisions of the Spam Page 4 of 4 Act when sending commercial electronic messages. Equally importantly, Omnia Audit makes sure that our practices are in accordance with the APPs in all activities where they deal with personal information.

Internal procedure for dealing with complaints

The three key steps Omnia Audit follows:

1. CONSENT

Only commercial electronic messages are sent with the addressee's consent – either express or inferred consent.

2. IDENTIFY

Electronic messages will include clear and accurate information about the person and the Omnia Audit representative that is responsible for sending the commercial electronic message.

3. UNSUBSCRIBE

We ensure that a functional unsubscribe facility is included in all our commercial electronic messages and deal with unsubscribe requests promptly.

Comply with the law regarding viral messages

Omnia Audit ensures that Commercial Communications that include a Forwarding Facility contain a clear recommendation that the Recipient should only forward the Commercial Communication to persons with whom they have a relationship, where that relationship means that person could be said to have consented to receiving Commercial Communications.

Comply with the age sensitive content of commercial communication

Where the content of a Commercial Communications seeks to promote or inspire interaction with a product, service or event that is age sensitive, Omnia Audit takes reasonable steps to ensure that such content is sent to Recipients who are legally entitled to use or participate in the product service or event.

Complaints resolutions

The Spam Act specifies that the person's consent has been withdrawn within five working days from the date that an unsubscribe request was sent (in the case of electronic unsubscribe messages) or delivered (in the case of unsubscribe messages sent by post or other means). Please contact our Privacy Officer if you wish to complain about any breach or potential breach of your privacy rights. Your complaint will be responded to within 7 days. If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Australian Information Commissioner or the Australian Communications and Media Authority.

Privacy Officer: Jacob Solly
Phone: +61 2 9030 0010