

Privacy Policy

Steelwork Compliance Australia Pty Ltd ABN 37 601 117 051 (SCA) is committed to providing quality services to you and this policy outlines our ongoing obligations to you in respect of how we manage your personal information. This Privacy Policy applies to Steel Compliance Australia Pty Ltd and its parent company Australian Steel Institute Limited (**ASI**).

SCA provides quality compliance certification for the supply, fabrication and erection of structural steelwork to be used in Australia. **ASI** is the peak membership body representing and serving Australia's steel industry. **ASI** provides advocacy, advisory, bookshop and library services as well as industry publications, technical presentations, seminars and conferences to both its members and the general public.

We have adopted the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Cth) (the Privacy Act). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of your personal information.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at www.oaic.gov.au.

This Privacy Policy may be updated or amended at any time without notice in order to ensure compliance with the Privacy Act or to better reflect the way our business processes comply with this Privacy Policy. The current Privacy Policy is available at any time on our website or by contacting the Privacy Officer.

Privacy Policy enquiries

If you have any queries or complaints about our Privacy Policy please contact us at:

Steelwork Compliance Australia Pty Ltd 37 601 117 051
Privacy Officer
Level 3 Building 3, 20 Bridge Street, Pymble NSW 2073, Australia.
PO Box 197, Macquarie Park BC NSW 1670, Australia
sca@scacompliance.com.au
+61 (0)2 8748 0180

The Australian Privacy Principles (APPs)

APP1: Open and transparent management of personal information

This Privacy Policy is available on our website www.scacompliance.com.au and can be obtained by emailing or writing to the Privacy Officer at the address shown above.

What is personal information and why do we collect it?

Personal information is information or an opinion that identifies an individual. Examples of personal information we collect include: names, addresses, phone numbers, email addresses, job titles.

This personal information is obtained in many ways including correspondence, telephone and facsimile and email; via our website www.scacompliance.com.au and other associated websites including steel.org.au, learn.steel.org.au and innovate.steel.org.au; from your website, from media and publications, from other publicly available sources, and from third parties.

We collect your personal information for the primary purpose of providing our services to you and providing information to our members and the general public. We may also use your personal information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure.

When we collect personal information we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained
- For a secondary purpose that is directly related to the primary purpose
- With your consent; or
- Where required or authorised by law.

Third Parties

Where reasonable and practicable to do so, we will collect your personal information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

Disclosure of personal information

Your personal information may be disclosed in a number of circumstances including the following:

- To third parties where you consent to the use or disclosure; and
- Where required or authorised by law.

Security of personal information

Your personal information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure.

When your personal information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your personal information. However, most of the personal information is or will be stored in our databases which will be kept by us for a minimum of 7 years.

APP2: Anonymity and pseudonymity

If you want to communicate with us on a particular matter you may ask to remain anonymous or use a pseudonym. However, if we are unable to verify your membership or your authority to act on behalf of a member, our services may be restricted and we may be unable to assist with passwords or other security matters or technical services like internet access.

APP3: Collection of solicited personal information

We collect the personal information that is reasonably necessary for us to efficiently, professionally and relevantly provide you with our services and to give you the ease of access and opportunities to access the services we may have available from time to time. It may include personal and business information, a completed form or application, record of a credit card payment, photographs or video footage at an event.

We try to collect your personal information directly from you. If we have collected your personal data from another source then we will tell you where it came from and why.

Incorporated entities may provide us with personal information about relevant employees who represent them in their dealings with us. The entity (through its authorised representative) can change those individual details at any time and we rely on that entity to ensure that information about its representatives is current.

APP4: Dealing with unsolicited personal information

If we are provided with unsolicited personal information (for example, misdirected mail, unsolicited emails, unsolicited employment application) which we would not otherwise request or use, we will make reasonable efforts to delete, destroy or de-identify the record. Where it is impracticable to do so, we will take all reasonable steps to protect the personal information against loss, unauthorised access, use, modification, disclosure or other misuse.

APP5: Notification of the collection of personal information

If we collect personal information from you, you will receive or have access to a Personal Information Collection Notice. This Collection Notice is available on our website www.scacompliance.com.au and forms part of the terms and conditions for membership, events and other services.

APP6: Use or disclosure of personal information

If we hold your personal information for a particular purpose (the 'primary purpose') we cannot use it for any other reason (a 'secondary purpose') unless you have consented to, or you would have reasonably expected it to be used for, that secondary purpose.

APP7: Direct marketing

The Privacy Act and the APPs prohibit the use or disclosure of personal information for the purpose of direct marketing unless we have collected the personal information directly from you and you would reasonably expect us to use it for that purpose. We will always provide you with an easy way by telephone, email or an online link to request us not to send all or particular marketing material.

APP8: Cross-border disclosure of personal information

In some circumstances your personal information may be disclosed to related membership bodies in other countries but may only be used for purposes which you would reasonably expect. Further, overseas parties may provide software, IT and data storage services to **SCA** or **ASI** and consequently have access to your personal information.

We will take all reasonable steps to ensure that those service providers which may have access to your personal information adopt the high standards of data security required by the Privacy Act.

APP9: Adoption, use or disclosure of government related identifiers

SCA may request, record and use government identifiers (e.g. tax file numbers) for legitimate purposes in the conduct of its business as permitted by law.

SCA does not use government identifiers (e.g. tax file numbers, Medicare numbers) for the purposes of identification of individuals in our membership or contact databases.

APP10-13: Quality, security, access and correction of personal information

ASI will take all reasonable steps to ensure that your personal information is accurate, up-to-date, complete and relevant and that it is safe from misuse, interference, loss, unauthorised access, modification or disclosure. In particular, credit card and other financial information is stored securely and promptly deleted or destroyed once the relevant transaction has been completed. This information is not stored in our online systems or otherwise for future transactions.

You can request **SCA** to access, verify, amend or remove your personal information by contacting the Privacy Officer using the details above. Members or authorised representatives of members can also access, update and modify personal information held in respect of their membership via our online member portal or by email to sca@scacompliance.com.au.

If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you. We commit to actioning your request as promptly as possible (subject to any legal or compliance obligations).

In order to protect your personal information we may require identification from you before releasing the requested information.

There is no charge for these services but we may charge an administrative fee for providing a copy of your personal information.

Notifiable data breaches

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the Notifiable Data Breaches (NDB) scheme in Australia with effect from 22 February 2018.

If a data breach occurs involving personal information, **SCA** is required to contain the breach, reduce any potential harm and take remedial action. It must also make an assessment of the breach, investigate the incident and evaluate whether the breach is likely to result in serious harm to any individual affected. If so, **SCA** is required to notify the Australian Information Commissioner as well as notify affected individuals, and take action to prevent further breaches.

Date of publication: 15-May-2020