

Privacy Policy - Singapore

1. Our Commitment to your Privacy

The CEO Institute (Singapore) and its related entities understand that it is an individual's right to keep their personal data private.

We are committed to protecting and maintaining the privacy, accuracy and security of personal data that we hold about members, prospective members and other individuals who engage with The CEO Institute.

2. Privacy Laws that Apply to us

This policy applies to The CEO Institute's activities in Singapore and to personal data handled in Singapore.

We are bound by the Personal Data Protection Act 2012 of Singapore (PDPA) and the data protection obligations it contains, including obligations relating to consent, notification, purpose limitation, access and correction, accuracy, protection, retention, transfer limitation, data breach notification and accountability.

The PDPA also contains a separate set of provisions relating to the national Do Not Call (DNC) Registry.

3. What is "personal data"?

Under the PDPA, personal data is any data, whether true or not, about an individual who can be identified from that data or from that data and other information to which an organisation has or is likely to have access.

This privacy policy explains how we collect, use, disclose and protect personal data.

4. What Personal Information We Collect

We collect personal data about:

- Members, prospective members and associates, and their businesses, before and during their association with The CEO Institute
- Job applicants, staff members, volunteers and contractors
- Chairs, speakers, partners and other service providers
- Other people who come into contact with The CEO Institute

The types of personal data we may collect include:

- Identification and contact details such as name, title, postal address, email address, telephone numbers and country of residence
- Professional and business information such as job title, organisation, industry sector, professional experience, qualifications and areas of interest



- Membership and programme information such as membership status, syndicate or programme participation, attendance at events, feedback and preferences
- Billing and payment information such as billing contact, payment method and limited payment details
- Information you provide in surveys, feedback forms, online enquiries or during conversations with us
- Any other personal data that you choose to provide to us in connection with our programmes, events and services

We only collect personal data that is reasonably necessary for our functions and activities.

5. How we Collect Personal Information

We collect personal data in a variety of ways, including:

- Application, registration and consent forms completed in hard copy or online
- Online portals and digital forms on our website or other platforms
- Face-to-face or video meetings and interviews
- Surveys, feedback forms and evaluation tools
- Telephone calls and other voice communications
- Email, messaging platforms and other written correspondence
- Event registration and attendance systems
- Our website and digital platforms, including cookies and similar technologies where consented or permitted by law

Where we collect personal data through our website or digital channels, we may also collect technical information such as device type, browser type and usage patterns, which helps us improve our services. Where required, we will treat such information as personal data.

6. Personal data provided by third parties

In some circumstances we may receive personal data about you from a third party. For example:

- A referral from an existing member, Chair, staff member or sales representative
- Another organisation that partners with us on a programme or event
- Publicly available sources such as LinkedIn, professional directories or your organisation's website

Where it is reasonable to do so, we will notify you that we have received your personal data from a third party and explain how we will handle it.



7. Sensitive personal data and special categories

While the PDPA does not use the same "sensitive data" terminology as some other regimes, we treat certain types of information as more sensitive. This includes information relating to health, criminal records, children, and any information that you identify as particularly confidential.

We only collect this type of information where it is reasonably necessary for our functions and activities, where you have given consent, or where the law permits or requires it.

Unless you agree otherwise, or the law allows, we use and disclose this kind of information only for the purpose for which it was provided or for a directly related secondary purpose.

8. Photographs and Video

When you attend functions and events organised by The CEO Institute, you may be photographed or filmed. Unless you raise an objection at the time, you are taken to consent to your image being used and reproduced in The CEO Institute's publications, marketing material, websites, social media channels and other promotional material.

If you do not wish to be photographed or filmed, please tell us or the event organiser at the time.

9. Purposes for which we collect, use and disclose personal data

We collect, use and disclose personal data for the following purposes:

- To assess and process membership applications and renewals
- To administer memberships, programmes, syndicates and events, including in-person and virtual programmes
- To keep members and stakeholders informed about matters relating to their membership, programmes and The CEO Institute's activities
- To plan, deliver and improve our professional development offerings, thought leadership and member services
- To maintain member directories, contact lists and networking tools where part of the value of membership
- To manage our relationships with Chairs, speakers, sponsors, partners and suppliers
- To communicate with you about events, news, research, surveys and other information that may be relevant to you
- To manage billing, payments, accounting and reporting
- To perform internal administration, governance, risk management and business planning
- To satisfy legal and regulatory obligations and to discharge our duty of care
- Any other purpose that we have notified to you at or before the time your personal data is collected, or that is reasonably related to the purposes above



We will notify you of the purposes for which we are collecting, using and disclosing your personal data, and we will only do so for purposes that a reasonable person would consider appropriate in the circumstances.

10. Consent

We generally collect, use and disclose personal data based on your consent. Consent may be given expressly, for example in writing or online, or may be implied from your conduct where it is reasonable to do so.

By providing personal data to us, engaging with us, or using our services, you consent to our collection, use and disclosure of your personal data in accordance with this policy and any specific notices that we give you.

You may withdraw your consent at any time, subject to legal or contractual restrictions and reasonable notice. If you withdraw consent, this may affect our ability to provide certain services to you.

11. Direct marketing and the Do Not Call Registry

We may use your personal data to send you information about The CEO Institute's programmes, events, publications, surveys and other offerings that we believe may be relevant to you.

For marketing messages sent by email or other electronic means, you can opt out at any time by using the unsubscribe facility in the message or by contacting us.

If we send marketing messages to Singapore telephone numbers by voice call, text message or fax that fall within the scope of the PDPA Do Not Call (DNC) provisions, we will do so in compliance with those provisions. In particular, we will either obtain your clear and unambiguous consent or check the relevant DNC Register before sending such messages.

12. Disclosure of personal data in Singapore

We may disclose personal data to:

- Legal and regulatory authorities where we are legally obliged to do so
- Chairs, facilitators, expert speakers and other professionals engaged in delivering our programmes and events
- Service providers who support our operations, such as event venues, IT and cloud service providers, marketing and communications providers, and professional advisers
- Recipients of The CEO Institute's publications, including newsletters and member updates, where this involves limited contact details
- Member organisations and peer contacts where introductions and networking are part of the value we provide
- Anyone you authorise us to disclose information to
- Related entities and business partners of The CEO Institute, where this supports the delivery of programmes and services

We do not sell personal data.



13. Cross-border transfers of personal data

The CEO Institute operates across several countries. For the purposes described in this policy, we may transfer personal data from Singapore to recipients in:

- Australia
- New Zealand
- Other countries or territories where The CEO Institute has members, Chairs, events or service providers

When we transfer personal data outside Singapore, we will comply with the PDPA's Transfer Limitation Obligation. In practical terms, this means we will take reasonable steps to ensure that the recipient provides a standard of protection for the personal data that is at least comparable to the protection under the PDPA, for example by using appropriate contractual safeguards, intra-group policies or other legally enforceable obligations.

14. Management and security of personal data

We take reasonable security measures to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

These measures include:

- Physical security for paper records, including secure offices and locked storage
- Password-protected access to electronic records and systems
- Role-based access controls so that staff and contractors only access personal data needed for their role
- Use of reputable cloud and IT service providers with appropriate safeguards
- Staff training and confidentiality obligations
- Procedures to respond to suspected or actual data breaches, including notification to affected individuals and the Personal Data Protection Commission (PDPC) where required by law

Personal data is held on The CEO Institute's systems and those of our service providers, which may be in Singapore or overseas.

15. Retention of personal data

We retain personal data only for as long as it is reasonably necessary to fulfil the purposes for which it was collected, or as required by applicable laws and regulations.

When personal data is no longer required, we will delete, anonymise or securely destroy it.

16. Access and correction requests

You have the right to request access to personal data that The CEO Institute holds about you, and to request correction of any personal data that you believe is inaccurate, incomplete or out of date, subject to the exceptions set out in the PDPA.



You can make a request by contacting us using the details in section 18. We may need to verify your identity and may charge a reasonable fee for providing access, in line with the PDPA. If we are unable to provide access or make a correction, we will explain why, subject to any legal restrictions.

17. Credit card details

Credit card details that you provide for programme joining fees or other payments are processed securely using the STRIPE platform or other secure payment gateways that we may use from time to time. We do not store full credit card details in a form that is accessible for general use once the transaction has been completed, except where required for lawful record-keeping.

18. How to contact us

If you have any questions about this policy, wish to request access to or correction of your personal data, or wish to withdraw consent, please contact our Data Protection Officer or Country Director:

Country Director
The CEO Institute (Singapore)
105 Cecil St,
#18-18, The Octagon,
Singapore 069534.

We may update these contact details on our website from time to time.

19. Complaints

If you have a concern or complaint about how we have handled your personal data, please contact our Data Protection Officer in writing using the details below and provide details of your concern.

The Chief Executive Officer
The CEO Institute Pty Limited
PO Box 297
Glen Iris
VIC 3146
Australia

We will investigate your complaint and aim to respond in writing within a reasonable period.

If you are not satisfied with our response, you may contact the Personal Data Protection Commission (PDPC) in Singapore for further guidance or to lodge a complaint.

20. Changes to this policy

We may review and update this Singapore Privacy Policy from time to time to reflect changes in law or our practices.

The current version will always be available on our website and will state the date it last took effect.

