



Quanta Services Australia

PRIVACY POLICY

Quanta Services Australia Pty Ltd ABN 11 164 311 997 (**Quanta**), Consolidated Power Projects Australia Pty Ltd ABN 18 075 411 219, Nacap Pty Ltd ABN 33 006 306 994, Quanta Power Australia Pty Ltd ABN 79 617 859 739 and Enscope Pty Ltd ABN 38 136 478 030 (**Quanta Group, we, our, us**) performs energy infrastructure construction throughout Australia. We recognise and respect the importance of your privacy and that you have a right to control how your Personal Information is collected and used by us.

This Privacy Policy applies to all your dealings with us. By visiting or using our Online Platforms, enquiring about (or using) our Services or otherwise communicating with us, you accept the terms of this Privacy Policy and consent to the collection, use and disclosure of your Personal Information by us as described in this Privacy Policy.

The purpose of this Privacy Policy is to provide you with information on how we collect, use, store and disclose your Personal Information. If you require any further information about our privacy practices, we welcome you to get in touch with us using the contact details set out in section 16 of this Privacy Policy below.

1 Definitions

In this Privacy Policy:

APPs means the Australian Privacy Principles under the Privacy Act which govern the standards, rights and obligations around the collection, use and disclosure of Personal Information, privacy governance and accountability, integrity and correction of Personal Information and the rights of individuals to access their Personal Information.

Online Platforms means the online platforms we operate including quantaservicesaustralia.com, enscope.com.au, nacap.com.au and conpower.com.au and any of our other websites or social media pages (including LinkedIn) managed by us.

Personal Information has the meaning given to it under the Privacy Act.

Privacy Act means the *Privacy Act 1988* (Cth), as amended from time to time.

Privacy Officer means our first point of contact for all privacy related inquiries and matters, who can be contacted using the details set out in section 16 below.

Privacy Policy means this document setting out the policy of the Quanta Group relating to the privacy and handling of your Personal Information.

Sensitive Information has the meaning given to it under the Privacy Act.

Services means the works and services provided by us to our customers, being the provision of specialised contracting services to the energy, gas, oil, communications, electrical and renewable power industries and defense base projects.

2 What is Personal Information?

Personal Information is defined in the Privacy Act as information or opinion about an identified individual (or an individual who is reasonably identifiable) whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not.

Sensitive Information is a subset of Personal Information that is afforded higher levels of protection under the Privacy Act. It includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record or health information.

3 Types of Personal Information we collect

In order to carry out our Services, we often need to collect your Personal Information. If we do not collect the Personal



Information or if any of the Personal Information you provide is incomplete or inaccurate, we may not be able to provide the Services or those Services may be compromised.

Depending on the nature of the Services we provide, the Personal Information we collect may include:

- (a) contact details (such as your name, date of birth, address, email and phone details);
- (b) health information;
- (c) information required for you to do business with us including bank account details, credit card information and any other relevant financial information;
- (d) information on prior dealings with us;
- (e) official records that are relevant to our functions or activities, for example records relating to land ownership;
- (f) information that allows us to be satisfied that an individual is authorised to undertake a role or particular activities, for example copies of licences and certificates;
- (g) information that allows us to assess employment applications, for example employment histories, educational qualifications, reference checks and, where relevant, police checks;
- (h) information required for you to work for us including bank account details, tax file numbers, passport details, visa permits (for travel, residency and work entitlement) and any other relevant employment information; and
- (i) any other Personal Information relevant to the Services we provide.

4 How we collect Personal Information

We will always aim to collect Personal Information directly from you, where practicable. We may also sometimes collect Personal Information through:

- (a) our Online Platforms (including your interactions with us on our social media platforms);
- (b) indirect forms such as emails, face-to-face meetings, business cards, resumes and telephone conversations;
- (c) entering into and performing contracts for Services; and
- (d) third party service providers.

Personal Information collected will be relevant and limited to what is necessary in relation to the purposes for which they are used and disclosed.

From time to time, we may collect Personal Information about you from third parties, public sources and as otherwise permitted by law. However, please note that we will typically only collect Sensitive Information (including health information) with your consent and directly from you, where possible.

We only collect and handle your Personal Information that is provided by you, with your consent or where otherwise permitted by law. We will assume that you have consented to us collecting all information that is provided to us in accordance with this Privacy Policy unless you tell us otherwise at the time you provide it to us.

Please note that if you provide us with Personal Information about a third party, you represent to us that the person agrees to us collecting and handling their Personal Information in accordance with this Privacy Policy, and we will collect it on this basis.

5 Use of Personal Information

Our main purposes for collecting, holding, using and disclosing Personal Information include, but are not limited to, the following:

- (a) to supply Services to our customers;



- (b) to notify our customers about our new or existing Services;
- (c) to distribute material and general information relating to our Services;
- (d) to obtain products and services from our suppliers;
- (e) to respond to enquiries from existing or prospective customers seeking information about our Services;
- (f) to enforce agreements between you and us;
- (g) to undertake research and surveys and analyse statistical information;
- (h) to comply with contractual, legislative and policy requirements including in relation to occupational health and safety and environmental matters;
- (i) to improve our Services;
- (j) legal compliance purposes – we may hold Personal Information to fulfill our legal obligations, respond to legal requests and comply with legal requirements;
- (k) dispute resolution purposes – in the event of disputes, claims or disagreements, we may retain Personal Information to facilitate resolution;
- (l) financial records purposes – Personal Information may be held for financial record keeping including tax compliance;
- (m) user account management purposes – Personal Information is retained to manage user accounts, including login credentials and transaction history;
- (n) marketing purposes – Personal Information may be used to for marketing of Services, eg. LinkedIn announcements;
- (o) archiving and backup purposes – Personal Information may be included in backups and archives to ensure data integrity and disaster recovery;
- (p) employment and recruitment purposes; and
- (q) as otherwise permitted or required by law.

6 Disclosure of Personal Information

We will generally only use or disclose your Personal Information for the purpose for which it was collected (known as the "primary purpose"). This might be to provide you with our Services. We may, however, also use or disclose Personal Information for another purpose related to the primary purpose where you would reasonably expect it to be used or disclosed for such related purpose (known as the "secondary purpose") or with your consent (which may be express or implied).

We often disclose Personal Information to:

- (a) related companies or our joint venture partners;
- (b) suppliers and service providers;
- (c) our customers or prospective clients (for example 'verification of competency' or other similar information); and
- (d) our contractors or agents.

Sometimes, we may be required to disclose your Personal Information to other third parties in certain circumstances including:

- (a) where disclosure is required or permitted by law;



- (b) if disclosure will prevent or lessen a serious or imminent threat to someone's life or health; or
- (c) where it is reasonably necessary for an enforcement related activity.

With regard to Sensitive Information (which includes your health information), we will only ever use or disclose your Sensitive Information with your consent, for the primary purpose for which it was collected or for another purpose directly related to the primary purpose where you would reasonably expect it to be used or disclosed for such a directly related purpose.

The Quanta Group are Australian companies owned by Quanta Services Inc., which has headquarters in the United States of America. The Quanta Group may also carry out projects in foreign countries. In both of these situations, we may disclose Personal Information off-shore where it is necessary to do so for the purpose of managing our affairs or otherwise as permitted by law.

If information has to be disclosed overseas, the overseas recipient may not be subject to privacy obligations or to any principles similar to the APPs. In these situations, we will generally take reasonable steps to have the overseas recipient comply with the APPs. However, we may not take such steps and will not be responsible for the subsequent handling of the Personal Information which we have disclosed if you have agreed that we may disclose the information overseas without taking such steps, if the recipient is subject to a law or binding scheme substantially similar to the APPs which can be enforced by you, or if the disclosure is required or authorised by the Privacy Act or the law.

7 Storage and security

We take security of your Personal Information seriously. Your Personal Information is stored in a manner that strives to protect it from misuse and loss and from unauthorised access, modification or disclosure. Those who work with us are aware of the importance we place on protecting your privacy and their role in helping us to do so.

When the Personal Information that we collect is no longer required, we will remove or de-identify the Personal Information as soon as reasonably possible. We may, however, retain Personal Information for as long as is necessary to comply with any applicable law, for the prevention of fraud, for insurance and governance purposes, in our IT back-up, for the collection of any monies owed and to resolve disputes.

Here are some examples of the things we do to protect your information.

Method	Examples
Staff obligations and training	<ul style="list-style-type: none">• We regularly train and assess our staff in how to keep your Personal Information safe and secure.• Our staff are required to keep your Personal Information secure at all times, and are bound by internal processes and policies that confirm this.• Access to Personal Information is controlled through access and identity management systems.• We have security professionals who monitor and respond to (potential) security events across our network.
System security	<ul style="list-style-type: none">• We store your Personal Information in secured systems.• We have technology that prevents malicious software or viruses and unauthorised persons from accessing our systems.



Method	Examples
Services providers and overseas transfers	<ul style="list-style-type: none">• When we send information overseas or use service providers that handle or store data, we require them to take steps to keep your information safe and use it appropriately.• We control where information is stored and who has access to it.
Building security	We use a mix of ID cards, alarms, cameras, guards and other controls to protect our offices and buildings.
Our websites and apps	When you log into our Online Platforms, we encrypt data sent from your computer or device to our system so no-one else can access it.
Destroying or de-identifying data when no longer required	<ul style="list-style-type: none">• We aim to keep Personal Information only for as long as we need for our business or to comply with the law.• When we no longer need Personal Information, we take active steps to destroy or de-identify it.

8 Access to and correction of Personal Information

You are always welcome to request that we provide you with access to the Personal Information we hold about you by contacting us using the details listed in section 16 below. Generally, we will provide you with access to the information unless applicable laws allow us to refuse, or prevent us from giving you, access to the Personal Information we hold about you. We will never unreasonably refuse requests to access Personal Information.

Where we agree to provide you with access to your Personal Information, sometimes we may make this conditional on us recovering our reasonable costs of doing so. No fee will be incurred for requesting access, but if your request for access is accepted, you will be notified of the fee payable (if any) for providing access if you choose to proceed with your access request.

You may also lodge a request to correct Personal Information we hold about you if you believe it is inaccurate, incomplete, irrelevant, misleading or out of date. There is no fee for doing this. To do so, please contact us at the contact details listed in section 16 below.

9 Direct marketing

Like most businesses, marketing is important to our continued success and viability. We may use Personal Information we hold about you, from time to time, to send marketing materials. Generally, we only do so where you consent or where allowed by applicable laws. Our communications to you may be sent in various forms such as by post or by electronic means (including email and SMS).

If you wish to cease receiving this marketing information, please contact us directly on the contact details listed in section 16 below asking to be removed from our mailing lists, or use the "unsubscribe" or "update your preferences" facilities included in all our marketing communications.

Please be assured that we will never use your Sensitive Information for direct marketing purposes.



10 Our Online Platforms

We sometimes use cookie technology on our Online Platforms. Cookies are pieces of information that a website transfers to your computer's hard disk for record keeping purposes and are a necessary part of facilitating online transactions. Most web browsers are set to accept cookies. We use them because cookies are useful to estimate our number of visitors and determine overall traffic patterns through our websites.

We may also collect statistical information regarding the use of our Online Platforms, including the domains from which website users visit, IP addresses, the dates and times of visits, activities undertaken on our Online Platforms and other clickstream data. In addition, we sometimes use web beacon technology to monitor internet activity on our websites. A web beacon is a clear-pixel image that generates an anonymous de-identified notice of a website's visit when viewed. A web beacon usually works in conjunction with a cookie.

If you do not wish to receive any cookies you may set your browser to refuse cookies. However, this may mean you will not be able to take full advantage of the services on our Online Platforms. If you set your browser to refuse cookies, a web beacon may still be able to generate a notice of your visit but it will not be associated with the information contained in cookies.

11 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 about you by third parties. In such cases, we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party and about your rights under this Privacy Policy.

Our Online Platforms may sometimes contain links to other websites operated by third parties for your convenience. We cannot provide any guarantees regarding third-parties' information handling policies or the content of third-party websites you may visit. Before disclosing your Personal Information on any other platform, we recommend that you examine the terms and conditions and privacy policy of the relevant platform. Please note that we are not responsible for any practices on linked platforms that might breach your privacy.

12 Employment, contractors and recruitment

If you send us an application to be considered for an advertised position (or unsolicited), this information may be used to assess your application or suitability for employment with us. This information may be disclosed to our related bodies corporate, joint venture and alliance partners and service providers for purposes such as considering your application, aptitude and psychological testing or other human resources management activities.

As part of the application process, you may be asked for your consent to the use and disclosure of certain Personal Information about pre-employment testing. We may also ask you to consent to the disclosure of your Personal Information to those people who you nominated to provide references. A refusal to provide any of this information, or to consent to its proposed disclosure, may affect the success of the application.

We will handle the Personal Information of contractors in accordance with the APPs.

This Privacy Policy does not apply to our handling of information about our employees. Our handling of employee records is exempt from the APPs under the Privacy Act if the act or practice is directly related to:

- either a current or former employment relationship between us and the individual; and
- an employee record held by us relating to the individual.

For information about our practices relating to employee records, please contact us at the contact details listed in section 16 below.

13 Notifiable data breaches

A notifiable data breach scheme is currently in place in Australia. We are committed to adhering to this scheme as an important step in preventing and managing serious privacy breaches.



A "data breach" means unauthorised access to, or disclosure, alteration, loss, or destruction of, Personal Information or an action that prevents us from accessing Personal Information on either a temporary or permanent basis. An "eligible data breach", in accordance with the Privacy Act, occurs when there is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates and we are unable to prevent the likely risk of serious harm with remedial action.

We, including all our people, take breaches of privacy very seriously. If we suspect a privacy breach has occurred, our priority is to contain and assess the suspected breach. In doing so, we will:

- (a) take any necessary immediate action to contain the breach and reduce the risk of harm;
- (b) determine the cause and extent of the breach;
- (c) consider the types of information involved, including whether the personal information is sensitive in nature;
- (d) analyse the nature of the harm that may be caused to affected individuals;
- (e) consider the person or body that has obtained or may obtain personal information as a result of the breach (if known); and
- (f) determine whether the Personal Information is protected by a security measure.

If we believe an eligible data breach has occurred we will, as soon as practicable, notify the Commissioner and all affected individuals or, if it is not possible to notify affected individuals, provide public notice of the breach (in a manner that protects the identity of affected individuals).

14 General Data Protection Regulation

We welcome the General Data Protection Regulation (**GDPR**) as an important step forward in encouraging high standards of personal data security. Australian businesses of any size may need to comply if they have an establishment in the European Union (**EU**), if they offer goods and services in the EU (irrespective of whether a payment is required), or if they monitor the behaviour of individuals in the EU (where that behaviour takes place in the EU).

Under the GDPR and the *Data Protection Act 2018* (UK), we may have some additional obligations with respect to the processing of "personal data" collected from residents of the EU and/or United Kingdom (**UK**). The meaning of personal data is similar to Personal Information – however, it is broader as it includes any information relating to an identified or identifiable natural person.

Where required, we will take appropriate steps to ensure that the personal data of EU and/or UK residents is:

- (a) processed lawfully, fairly and in a transparent manner;
- (b) collected for legitimate purposes;
- (c) accurate and up to date;
- (d) kept for no longer than is necessary for the purposes for which it was collected; and
- (e) secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

We will comply with all obligations imposed on data importers under the GDPR and the *Data Protection Act 2018* (UK) with respect to the personal data of EU and UK residents, including the Standard Contractual Clauses, to the extent that they may apply to us and our relationships with third parties.

EU and UK residents have the right to access personal data we hold about them and to request that personal data be corrected, updated, deleted or transferred to another organisation. EU and UK residents are also able to request that the processing of their personal data be restricted or objected to their personal data being processed. To make any of these requests, please contact our Privacy Officer.



15 Changes to our Privacy Policy

Over time, aspects of our business may shift as we respond to changing market conditions and legislative obligations. This may necessitate our policies to be reviewed and revised. We reserve the right to change this Privacy Policy and notify you by posting an updated version of the policy on our Online Platforms. In light of this, we strongly recommend that you review our Privacy Policy each time you visit or use our Online Platforms or provide us with any of your Personal Information.

16 Contacting us

If you have any inquiries or complaints about how we handle your Personal Information, or if you have any questions about this Privacy Policy, we welcome you to get in touch with us by contacting our Privacy Officer at:

Attention: Privacy Officer

Email: privacyaustralia@quantaservices.com

We will endeavour to assess and respond to your query within 30 days. More information about your rights and our obligations in respect to privacy and information on making a privacy complaint are available from the Office of the Australian Information Commissioner at:

Website: www.oaic.gov.au

Post: GPO Box 5218
Sydney NSW 2001

Email: enquiries@oaic.gov.au

Rick Boreham
President
Quanta Services Australia

12 December 2023