

1.0 Purpose

PWR Holdings Limited and its wholly owned subsidiaries:

- P.W.R Performance Products Pty Ltd trading as “PWR Advanced Cooling Technology” (Australian Business Number 96 081 798 996)
- PWR IP Pty Ltd (Australian Business Number 75 604 823 047)
- PWR Europe Limited (UK Company Number 06314126)
- C&R Racing, Inc trading as “PWR North America” (Indianapolis Business ID 2015031700833)

(collectively “**PWR Group**”) value and respect the privacy of the people we engage during our business undertakings and the PWR Group is committed to protecting individual’s privacy and complying with:

- the *Privacy Act 1988 (Cth)* (**Australian Privacy Act**) and other applicable privacy laws and regulations in Australia;
- the UK *Data Protection Act of 2018* which implements the European Union General Data Protection Regulation (**EU GDPR**) and other applicable privacy laws and regulations in the United Kingdom and as relevant in the European Union;
- the U.S. Privacy Act of 1974 (**US Privacy Act**) and other applicable privacy laws and regulations in the United States of America

(collectively “**Privacy Obligations**”).

2.0 Scope

This Privacy Policy/Notice incorporates various Privacy Obligations and applies to all PWR Group directors, executives, employees (current and prescriptive), contractors, suppliers/vendors, customers/clients, volunteers and members of the public interacting with any member of the PWR Group.

3.0 Privacy Policy/Notice Statement

The purpose of this Privacy Policy or Customer Privacy Notice (**Policy**) is to describe how we collect, hold, use and disclose your general ‘personal information’ (defined as *Personal Information* in the Privacy Act; *Personal Data* in the EU GDPR and described by general principles protecting information about individuals as per US Privacy Act), and how we maintain the quality and security of that information in accordance with various **Privacy Obligations**.

- In Australia, PWR Group complies with the Australian Privacy Principles (**APPs**) contained in the Privacy Act. APPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information. A copy of the APPs may be obtained from the website of The Office of the Australian Information Commissioner at www.oaic.gov.au.
- As the PWR Group has a presence in the United Kingdom and offers goods/services in the EU (which may include monitoring the behaviour of individuals in the EU) and is considered a ‘controller’ it has also adopted the requirements of the EU GDPR. The EU GDPR contains data protection requirements that harmonise data protection laws across the EU by introducing clear, uniform data protection requirements. A copy of the EU GDPR may be obtained from the website www.gdpr-info.eu.
- In United States of America, PWR Group adopts principles of the US Privacy Act which establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 1 of 9

information about individuals. The US Privacy Act can be obtained from the US Department of Justice website at www.justice.gov/opcl/privacy-act-1974.

The PWR Group is required to collect information from individuals as part of its business operations; and this information is subject to various Privacy Obligations. Details about how the PWR Group manages its various obligations under the Privacy Obligations are set out in this Privacy Policy/Notice and associated inquiries can be directed towards the PWR Privacy Officer as set out below. Employees and contractors of the PWR Group must comply with the PWR Code of Conduct and company policies, procedures and practices.

4.0 Privacy Policy/Notice

4.1 Policy

What Is Personal Information/Personal Data?

“Personal Information” according to the Australian Privacy Act means any information or opinion about an identified individual, or an individual who is reasonably identifiable. This term is also used generally when referencing the obligations in the US Privacy Act; and applies to the term “Identifiers” used by Californian legislation.

“Personal Data” according to the EU GDPR means any information relating to an individual or identifiable natural person.

In general terms, these definitions include information or an opinion that personally identifies you either directly (e.g. your name) or indirectly (e.g. by identifiable features), collectively we refer to this type of information as **“Personal Information/Data”**.

What Personal Information/Data Do We Collect?

The Personal Information/Data we collect about you depends on the nature of your dealings with us or what you choose to share with us; and may include:

- **Identification Data** – for example, individual name, gender, job title and roles, photograph, date of birth, country of residence and copies of identification documentation including driver’s licence, birth certificate, passport or other government identification information.
- **Contact Information** – for example, mailing/shipping or street address, email address, telephone numbers, social media profiles, next of kin and emergency contact details.
- **Workplace Records** – for example, security records, entry and exit times, log on and off times, workplace incident reports and information (for example where you have been involved, witnessed or managed employees impacted), including, audio, still/live/recorded images and data from surveillance systems such as facial recognition devices, CCTV, location tracking data and data from computers and other devices.
- **Website and Applications** (including mobile apps) – for example, access details in the form of login information, IP addresses, ID, records of use, geo-location, server usage logs, browser types, operating systems, time zone, access times and other web statistics.
- **Product/Services Customers and Vendors** – for example, Identification Data, Contact Information, Website and Applications, Legal Records, purchase records, payment details, account information, credit history, transaction history, delivery details, performance reports, order inquiries and correspondence.
- **Shareholder Records** – for example, name, address, number of shares held, tax file number and bank account details.
- **Recruitment Related Information**– for example Identification Data and Contact Information described above, licences and qualifications, employment history, education history, right to work information, security clearance details, salary/wages details (including related information such as group certificates, PAYG summaries, income statements, bank account details, tax file numbers, credit information), leave details, medical records, health records, drug/alcohol and other medical testing, performance information, disciplinary information, training records, interview notes, reference checks, psychometric test results, background

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 2 of 9

PC-52-29 Privacy Policy/Notice Policy

checks including criminal records, work visa, immigration information and other identification to verify identity and right to work; and where specifically required racial or ethnic origin, biometric information and health information.

- Legal Records – for example, Identification Data, Contact Information, Workplace Records, Website and Applications, Product/Services Customers and Vendors, Recruitment Related Information, Other Information and where specifically required racial or ethnic origin, biometric information and health information.
- Other Information – for example call records, marketing preferences, sponsorship, location data, meeting records, feedback, complaints, claims and correspondences in all forms including email, letter, facsimile, text message and other media communication platforms such as What’s App and Messenger.

What Is Sensitive Information?

In Australia, some types of Personal Information are considered more sensitive than others. “**Sensitive Personal Information**” means information or opinions about such things as an individual’s racial or ethnic origin, political opinions, political association, religious or philosophical beliefs, membership of a trade union or other professional body, sexual preferences, criminal record, health information or biometric information (examples of Sensitive Personal Information change depending on your jurisdiction).

What are ‘Special Categories’ of Personal Data?

In the EU GDPR, additional protections apply to ‘special categories’ of Personal Data, which includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

What Sensitive Personal Information/Special Categories of Personal Data Do We Collect?

In certain circumstances, PWR Group may need to collect Sensitive Personal Information/Special Categories of Personal Data about you.

If we collect this sort of information, we will do so only with your optional consent (freely given, specific, informed and via unambiguous indication of your wishes through a clear affirmative action, signifying agreement to the processing), if it is necessary to prevent a serious and imminent threat to life or health, or as otherwise required or authorised by law, and we take appropriate measures to protect the security of this information.

As set out below consent can be withdrawn at any times via contacting the PWR Privacy Officer.

How Do We Collect Your Information?

We will collect your Personal Information/Data directly from you when individual members of the PWR Group interact with you in person, for example, on the phone, via SMS, through exchange of paper or electronic written communication or when you complete forms or questions (available in hard copy email, via our website(s)), online portals, our apps, when you attend our events, subscribe to our mailing lists or apply for a position with us as an employee, contractor or volunteer or to do business with us as a supplier or customer.

We may collect information about you directly via automated data collection tools when we engage with you online.

We will collect your information as permitted by local law and subject to your contact preferences.

We may also collect your Personal Information/Data from third parties or through publicly available sources and registers, for example from recruitment agencies, your nominated referees, police/credit/fraud checks, via your authorised representatives or our customers and business partners. Where reasonable, we will take practical steps to ensure that you are made aware of the information provided to us by third parties. Where we obtain Personal Information/Data from a third party we will treat that information and protect it in accordance with this Policy in the same way as Personal Information/Data we collect directly from you.

Typically, we store Personal Information/Data in hard copy and electronic form. Our electronic databases are generally hosted in dedicated data centres in Australia (Brisbane), United Kingdom (Rugby) and the USA (Indianapolis). As described below, we may use third-parties to store and process personal information.

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 3 of 9

Why Do We Collect Your Personal Information/Data? How Do We Use Your Personal Information/Data?

We will not use or disclose your Personal Information/Data other than for a purpose for which we have collected it, unless you have consented to it, or it is required or permitted by law.

We collect your Personal Information/Data so that we can:

- Assist you with your transactions, respond to your questions and inquiries of us through customer support;
- Improve the quality of the products/services we offer as well as our business processes;
- Provide a more personalised experience and service offering;
- Tell you about and improve our products and services through marketing and advertising;
- Support our business administration and related functions, including security and sharing of information within the PWR Group;
- Manage access, safety and security risks;
- Accept/consider job applications, and send you job opportunities that may be of interest to you;
- Administration of our website, portal and associated applications, including social media sites;
- Manage employee/customer/contractor/volunteer engagement as well as shareholder relationships;
- Assist with any inquiry you may have of us;
- Research purposes;
- Investigate or take action regarding any violations or suspected violations of law or our terms;
- Meet our legal obligations; and/or
- For other reasons where you might reasonably expect us to use your Personal Information/Data.

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

We may send you direct marketing communications and information about our products, services, opportunities, or events that we consider may be of interest to you if you have requested or consented to receive such communications. These communications may be sent in various forms, including mail, SMS, fax and email, in accordance with applicable marketing laws (such as the *Australian Spam Act 2003 (Cth)*; United Kingdom (UK) *EC Directive 2003*; United States (US) *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* known as the *USA CAN-SPAM Act*). You consent to us sending you those direct marketing communications by any of those methods. If you indicate a preference for a method of communication, we will endeavour to use that method whenever practical to do so. You may opt-out of receiving marketing communications from us at any time by following the instructions to “unsubscribe” set out in the relevant communication / contacting us using the details set out in the “How to Contact Us” section below of this Policy.

If you choose to follow our companies on social media, or log into our associated accounts using social media credentials, then your use of social media could result in collection or sharing of information about you. The details we receive may depend on your social network account privacy settings, which you can manage in your own profile settings.

We are compliant with the global *Payment Card Industry Data Security Standard* which is an information security standard for organisations that handle credit card data. This means that when you shop with us, both in-store and online, your credit card details will be handled using secure processes anywhere in the world. You should still exercise caution when shopping online, and never enter any credit card details when contacting us via email or through our website “Contact Us” form as in these instances those details will not be protected by encryption.

As indicated above, sometimes we may also need to collect and process Sensitive Personal Information/Special Categories of Personal Data about you; however, we will only do this where you have explicitly provided your consent; or where we are otherwise permitted by applicable law and regulations to do so.

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 4 of 9

We collect your Personal Information/Data because in some circumstances, if we do not collect your Personal Information/Data it may affect our ability to conduct our business.

Which Third Parties May We Disclosure your Personal Information/Data To?

We may disclose your Personal Information/Data to third parties in accordance with this Policy and in circumstances where you would reasonably expect us to disclose your information, including for example, with our business partners, contractors, subcontractors and service providers, our insurers, our health care providers, organisations we need to share information for safeguarding reasons, our customers for specific business purposes, our professional or legal advisers, regulatory and government agencies, credit reporting bodies, external auditors and inspectors, warranty and guarantee providers, debt collectors, third parties to whom we choose to sell, transfer or merge part of our business or assets, other PWR Group entities or any other third-party authorised by you. Where necessary, we may share your Personal Information/Data with emergency service providers.

We may also use, disclose, de-identified information for statistical and business improvement purposes, such as reporting on gender, diversity, supply chain arrangements, sustainability achievements.

We note that protection of your Personal Information/Data may be subject to contractual arrangements that override the general positions set out in this Policy.

Will We Sell Your Personal Information/Data?

No, we will not sell your Personal Information/Data.

Will Your Personal Information/Data Be Transferred or Disclosed Overseas?

As a global business, it may be necessary to transfer or disclose your Personal Information/Data overseas in the course of our usual business operations. Some of the third-party service providers we disclose or transfer your Personal Information/Data to in accordance with this Policy may be based in or have servers located outside of Australia, the United Kingdom, the United States of America, the European Union.

Where we disclose or transfer your Personal Information to third parties overseas, we will take reasonable steps to ensure that data security and appropriate privacy practices are maintained in accordance with applicable Privacy Obligations.

Where we disclose or transfer your Personal Data to third parties outside the EU we will ensure it is to countries that have provided an ‘adequate’ level of data protection; where ‘standard data protection clauses’ or ‘binding corporate rules’ apply; and where approved codes of conduct or certification is in place.

How Do We Protect Your Personal Information/Data?

PWR Group will take reasonable steps to ensure that the Personal Information/Data that we hold about you is kept confidential and secure, and is protected from misuse and loss from unauthorised access, modification or disclosure, including for example by:

- Taking measures to restrict access to Personal Information/Data to only those personnel who need that information for business purposes;
- Protecting physical security of our premises and databases/records which include Personal Information/Data; and
- Ensuring we have technological measures in place (for example, anti-virus software, fire walls, secure sockets layers or SSL) as well as utilising cookies and website analytics.
 - *Cookies* - are a small file of letters and numbers the website puts on your device if you allow it. These cookies recognise when your device has visited our website(s) before, so we can distinguish you from other users of the website. This improves your experience and the PWR Group website(s). We do not use cookies to identify you, just to improve your experience on our website(s). If you do not wish to use the cookies, you can amend the settings on your internet browser so it will not automatically download cookies. However, if you remove or block cookies on your computer, please be aware that your browsing experience and our website’s functionality may be affected.

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 5 of 9

- *Website analytics* – are used to help us better understand visitor traffic, so we can improve our services. Although this data is mostly anonymous, it is possible that under certain circumstances, we may connect it to you or identify you from this analysis.

Do We Use Hperlinks to Third-Party Sites?

PWR Group website(s) may contain hyperlinks to websites operated by third parties. If you access a third-party website through our website(s), Personal Information/Data may be collected by that third-party website. While we make appropriate inquiries of the practices of third-party sites; we do not make any representations or warranties in relation to the privacy practices of any third-party provider or website and we are not responsible for the privacy policies or the content of any third-party provider or website. Third-party providers / websites are responsible for informing you about their own privacy practices and we encourage you to read their privacy policies.

How Long Will We Retain Personal Information/Data?

We will not keep your Personal Information/Data for longer than we need to. In most cases, this means that we will only retain your Personal Information/Data for the duration of your relationship with us unless we are required to retain your Personal Information/Data to comply with applicable laws, for example record-keeping obligations. We will retain your Personal Information/Data in accordance with PWR Control of Documented Information Procedure (details of which can be provided by the PWR Group Privacy Officer). However, most of the Personal Information/Data is or will be stored in files which will be kept by us for a minimum of 7 years post our engagement with you; with the exclusion of candidates who are unsuccessful in obtaining employment, in which case we will retain your records for 2 years.

When your Personal Information/Data 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/Data.

We have implemented and will maintain appropriate technical and organisational measures to protect your information against accidental loss, destruction or alteration, unauthorised disclosure or unlawful destruction.

How Do We Manage Children’s Privacy?

Unless it is necessary to do so (for example as part of our school-based work experience programs) we do not knowingly collect, use or disclose personal information of children (as defined locally). Any Personal Information/Data we collect related to a child will be collected with the consent of a responsible adult or guardian where possible and will be managed appropriately, including with extra protections and removal at the earliest opportunity. If you believe we have inadvertently or incorrectly collected Personal Information/Data about a child, please contact us so we can manage that information appropriately and or delete the information.

How To Access and Correct your Personal Information/Data?

PWR Group will endeavour to keep your Personal Information/Data accurate, complete and up to date.

If you wish to make a request to access and / or correct the Personal Information/Data we hold about you, you should make a request by contacting us via the methods set out below and we will respond without delay in a reasonable period, and in any event of no longer than 30 days.

PWR Group will not charge any fee for your request to access your Personal Information/Data but may charge an administrative fee for providing a copy of your Personal Information/Data.

In order to protect your Personal Information/Data we may require you to verify any agents and provide suitable identification before releasing the requested information.

If you find that the Personal Information/Data 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.

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 6 of 9

How to Contact Us with Questions About Your Personal Information/Data?

If you have a question or concern in relation to our handling of your Personal Information/Data or this Policy, you can contact us for assistance as follows:

Attention: PWR Group Privacy Officer

- privacy@pwr.com.au or +61 (7) 5547 1600 in Australia
- privacy@pwreurop.com +44 1327 362940 in United Kingdom
- privacy@pwrna.com +317 293 4100 in United States of America

Address: PWR Group, PO Box 6425 Yatala Qld Australia 4208

How to Lodge Complaints and Inquiries?

For complaints about how PWR Group handles, processes or manages your Personal Information/Data, please contact PWR Group Privacy Officer as set out above.

Please allow up to thirty (30) days for PWR Group to respond to your complaint, noting that we will endeavour to respond without delay. Note we may require proof of your identity and full details of your request before we can process your complaint or inquiry.

It will not always be possible to resolve a complaint to everyone's satisfaction. If you are not satisfied with PWR Group's response to a complaint, you have the right to contact:

- the Office of Australian Information Commissioner (www.oaic.gov.au/);
- the Information Commissioner's Office in the United Kingdom (www.ico.org.uk/make-a-complaint); or
- the U.S. Department of Justice in the United States of America (www.justice.gov)

for guidance on alternative courses of action which may be available to you.

4.2 United Kingdom/European Union Specific Details

The following additional provisions apply to individuals interacting with PWR Group in the UK.

For the purposes of all applicable UK and EU legislation, references to 'Personal Information' are to be read as "Personal Data"; and that the PWR Group is the 'controller' in relation to your Personal Information/Data and will therefore only use processors that provide sufficient guarantees, which include implementing appropriate technical and organisational measures that ensure compliance with the EU GDPR and protect your rights as the data subject.

PWR Group will only process Personal Information/Data where we have a legal or 'lawful basis' for collecting and using your personal information. Our lawful basis for the collection and use of your data, including (a) to provide services/goods; (b) for operation of customer accounts and guarantees; (c) to prevent, detect, investigate or prosecute crimes; (d) for service updates or marketing purposes; (e) for research or archiving purposes; (f) for legal requirements; (g) for recruitment purposes; (h) for dealing with queries, complaints or claims:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Contract - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation - we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Which lawful basis we rely upon may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the UK IOC's website (www.ico.org.uk):

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 7 of 9

PC-52-29 Privacy Policy/Notice **Policy**

- Your right of access – you have the right to ask us for copies of your personal information. You can request other information such as details of where we get personal information from and who we share personal information with. There are some exemptions which mean you may not receive all the information you ask for.
- Your right to rectification – You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete.
- Your right to erasure ('right to be forgotten') – You have the right to ask us to delete your personal information.
- Your right to restriction of processing – You have the right to ask us to limit how we can use your personal information.
- Your right to object to processing – You have the right to object to the processions of your personal data.
- Your right to data portability – You have the right to ask that we transfer the personal information you gave us to another organisation, or to you.
- Your right to withdraw consent – When we use consent as our lawful basis, you have the right to withdraw your consent at any time.

Where necessary, we may transfer personal information outside of the UK, including to our related PWR Group entities in Australia and the United States of America. When doing so, we will comply with the UK GDPR, making sure appropriate safeguards are in place. For further information or to obtain a copy of the appropriate safeguards for any transfer please contact us using the contact information provided above.

4.3 California, USA Specific Details

The following additional provisions apply to California residents and supplements the information contained in this Privacy Policy/Notice addressing the requirements of the *California Consumer Privacy Act* of 2018 and the associated *California Consumer Privacy Act Regulations* (referred to as “**CCPA**”) that are not covered generally by the remainder of this Privacy Policy/Notice.

At any time, you have the right to:

- Request Information about Collection, Disclosure or Sale of Personal Information “Right to Know”
- Request Deletion of Personal Information “Request to Delete”
- Non-Discrimination

As we do not sell your Personal Information, we do not provide a right to opt-out of the sale of Personal Information.

If you are a California resident and would like to exercise your rights, you may contact the PWR Group Privacy Officer as set out above. Only you or a person authorized to act on your behalf may make a consumer request related to your personal information. The request must:

- Provide sufficient information to allow us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient details to allow us to properly understand, evaluate, and respond.

Requests may be denied in whole or in part due to various factors; for example, if a request was not verifiable, was not made by a consumer, was made multiple times, or called for information exempt from disclosure.

4.4 Policy Updates

This Policy was last updated on 24 October 2024.

PWR Group may amend this Policy from time to time. Any changes to our Privacy Policy/Notice will be updated on our website and will automatically apply to all Personal Information/Data we hold about you. You may obtain a copy of the current Privacy Policy/Notice from our website or by contacting us via the details above.

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 8 of 9

5.0 Monitoring and Review

5.1 Monitoring

The PWR Group Privacy Officer is accountable for ensuring that Personal Information/Data is managed in accordance with this Privacy Policy/Notice; and for reviewing this Privacy Policy/Notice for compliance with updated legislative requirements.

The PWR Group security managers, security officers, IT managers are responsible for supporting the PWR Group Privacy Officer to ensure maintenance of these requirements.

General Managers of each of PWR Group’s business operations will ensure their direct reports understand their responsibilities and are trained with respect to the obligations set out in this Privacy Policy/Notice.

5.2 Review

The PWR Group Privacy Officer will review this Privacy Policy/Notice at least bi-annually.

6.0 Implementation

PWR Group, under direction of the PWR Group Privacy Officer, will manage Personal Information/Data in accordance with this Privacy Policy/Notice.

7.0 Definitions

Defined words have been used throughout this document as indicated.

8.0 References

PWR Group Policies and Procedures

Code of Conduct Policy (PC-52-07)

Control of Documented Information Procedure (WI-75-02)

Australia

Australian Spam Act 2003 (Cth)

Privacy Act 1988 (Cth), including Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 referenced as the “Australian Privacy Principles” or “AAPs” and Privacy Regulation 2013 (Cth)

Europe

Regulation (EU) 2016/679 (General Data Protection Regulation)

United Kingdom

Data Protection Act 2018 (UK)

Privacy and Electronic Communications Regulations 2003 (UK)

United States of America

Privacy Act of 1974 (USA)

California Consumer Privacy Act of 2018 and the associated California Consumer Privacy Act Regulations (USA)

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (USA) known as the ‘USA CAN-SPAM Act’

Reviewed by: General Counsel	Owner: PWR Group Privacy Officer	Revision: 01 Effective: 24/10/2024	
Approved By: Martin McIver	Printed copies are uncontrolled	Doc.No: PC-52-29	Page 9 of 9