

RPM – Privacy Policy

1. Protecting your privacy

RPM is committed to protecting the privacy and Personal Information of its customers, suppliers and other stakeholders, ensuring only the information needed or appropriate for business purposes is collected and done through lawful and fair means. RPM respects your preferences regarding the collection and use of your Personal Information, and the following policy sets out how RPM collects, processes, transfers, stores, uses and discloses Personal Information provided to RPM.

RPM, as a company operating in Australia, is bound by the Privacy Act 1988 (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**), and is an APP Entity under the provisions of that Act. Further, as a provider of products and services with operations and affiliate companies worldwide, RPM may also be subject to the laws and regulations of other countries. To the extent required, this policy shall be read subject to and in accordance with the mandatory provisions of those additional laws to which RPM may be obligated to comply.

This privacy policy applies to the information collected by RPM (including all affiliate companies of RPM), in its dealings with you, including but not limited to through the RPM Website and/or RPM Store and/or in person.

2. What Personal Information does RPM collect, use, process, transfer and store?

When you contact RPM, visit our website or request, receive or use RPM software products or services (**RPM Software or Services**) from us, RPM may collect, hold, process and use certain data, which may include Personal Information from you, which assists us in managing our relationship with you.

This Personal Information may be collected from you and subsequently held, processed and then used (subject to this policy) by RPM, as a direct or indirect result of RPM's dealings with you, including but not limited to during the provision of RPM Software or Services to you or following referrals of third parties.

The Personal Information we may collect, hold and use (subject to this policy) may include:

- Your name, company, title or position, personal and employers' contact details (such as email address, phone number, emergency contact(s), postal address and street address);
- Identification and verification information (e.g., photographs, driver's license, passport, other proofs of identity);
- Information security data (e.g., communications created, stored or transmitted by a person using RPM's information technology or communications equipment);
- Information to fulfil items such as, but not limited to, communications, contracts, purchase orders, payments, and receivables;
- Other information required to comply with applicable laws, including valid search warrants, subpoenas, or court orders;
- Software credentials, including your username and password, machine identification details and similar information used for authentication and account access and for software maintenance and support;
- When using RPM Software or Services, location services usage data, including when using RPM mobile RPM Software or Services, the GPS location of the device when that Software is being used;
- Demographic information and location data, such as your country, preferred language, post code (or ZIP), age, gender, preferences, interests and favourites;
- If you choose to make a purchase of RPM Software or Services in the RPM Store or directly from RPM, we may process additional information, such as your credit card number, expiry date and billing details and address and will also collect information in respect of the RPM Software or Services you purchase from us and additional information to assist with ongoing support and customer success including (by way of example) purchase history, and customer satisfaction information;
- Information relating to your visit to the RPM Website and/or RPM Store, including for example, we may use web analytics tools to retrieve information from your browser, including the site you came from, the search engine(s) and the keywords you used to find the RPM Website and/or RPM Store, the pages you view within the RPM Website and/or RPM Store, your browser add-ons, and your browser's width and

height. Additionally, we may collect and hold certain standard information that your browser sends to every website you visit, such as your IP address, browser type and language, access times and referring website addresses. When you use our website, we may also collect and hold information from your browser, such as language choice, to improve your customer experience, for example, by making the RPM Website and/or RPM Store accessible to you in your preferred language where possible;

- Software analytics information as further detailed in Section 3 (Software Analytics) of this policy below;
- Additionally, for individuals who visit or attend an RPM facility or location, photographs or video may be captured (e.g., closed-circuit television cameras or CCTV).
- Employees and contractor suppliers will have further data collected:
 - Background information (e.g., birth date, marital status, dependent information, ethnicity and/or nationality);
 - Social Security Number or other national/taxpayer identification numbers;
 - Residency information (e.g., work permit status);
 - Financial account information;
 - Reference information (e.g., letters of recommendation or reference, or reports provided by former employers or colleagues);
 - Background check information (e.g., credit and criminal background checks, drug and alcohol testing);
 - Health information (e.g., prescription records, benefit claims, and the explanation of benefits sent in connection with claims);
 - Biometric information (e.g., thumbprints);
 - Trade union affiliation;
 - Automotive information (e.g., driving history, vehicle registration, driver's license number);
 - Professional qualifications information (e.g., work experience, education); and
 - Employment-related information (e.g., work history, new hire forms, skills, education and training, performance appraisals, goals, attendance, work absences, vacation entitlement and requests, compensation history, workplace injury and illness reporting, disciplinary issues, and grievances).

The above information is collectively known in this policy as your **Personal Information**.

3. Software Analytics

Users of RPM Software and/or recipients of RPM Services may be requested at the time of installation of that Software (or an upgrade or new release of that Software) or receipt of those Services, whether they wish to assist RPM to improve its Software and Services by sending us anonymous usage data about how you are using the Software or Services (**RPM Software Analytics**).

By installing and using RPM Software and by choosing not to 'opt out' from RPM Software Analytics either at the time of installation or subsequently at any point by not 'opting out', you are agreeing to and are granting RPM the right and permission to collect, maintain, process and use analytics data related to your use of our Software.

For the purposes of the RPM Software Analytics program, RPM may rely on third-party analytics services to collect and process this data, and such data is stored and processed on servers located in Europe and the USA.

You can opt in or out of the RPM Software Analytics program at any time from the Software "about box" or by emailing privacypolicy@rpmglobal.com.

4. RPM's guidelines for collecting Personal Information

Prior to collecting Personal Information from an individual or an external third party, the Data Owner must fulfil the following requirements:

- Purpose – determine the legitimate business purpose for processing the information.
- Minimisation – determine the type(s) of Personal Information relevant for the stated purpose and only collect that Personal Information.
- Notice – create a clear, appropriate notice and implement a procedure to deliver this notice to the individuals whose information is collected.

- Security – implement appropriate security for the information, including both organisational controls (e.g., access granting/revoking processes) and technical controls (e.g., encryption).
- Accuracy – implement processes to keep the Personal Information relevant and up-to-date and to rectify or erase inaccurate or incomplete Personal Information as appropriate.
- Rights Fulfilment – implement processes to support the fulfilment of data subject rights requests.
- Records Retention – determining appropriate retention times for the Personal Information in accordance with RPM's Record Retention Policy and developing processes to implement the retention times.
- In-Country Requirements – coordinate with the RPM Privacy Lead and Legal to understand and fulfil any in-country requirements (e.g., registering with, or obtaining approval from, competent data protection authorities) as well as any restrictions on processing the Personal Information for the stated purpose.
- Data Protection Officers – coordinate with any applicable Data Protection Officers to the extent that the processing involves a facility, location, or other part of the business with a Data Protection Officer.
- Third Parties – determine if any third parties will need to have access to the Personal Information and, if so, confirm that the requirements of Section 6 (RPM's Guidelines for Transferring Personal Information) below are met.
- Inventory and Assessments – follow the applicable RPM processes for completing records of processing activity and any assessments, including any data privacy/protection impact assessments.
- Refresh – develop and follow a process to re-evaluate (and re-execute) the above as necessary before making changes to the processing of the Personal Information.

5. RPM's guidelines for processing already collected Personal Information for a different purpose

In some cases, there may be a legitimate business purpose to process Personal Information (that has already been collected by RPM) for a purpose that is different from the original purpose described in a notice. Prior to processing Personal Information for a different purpose, the original Data Owner must determine whether the new purpose is compatible with the original purpose and the notices provided to the individual.

The Data Owner for the new processing of Personal Information is responsible for his or her process, and the processing of the Personal Information must be consistent with the above information and the steps described under Section 4 (RPM's Guidelines for Collecting Personal Information) above, including fulfilling the following requirements:

- Purpose – determine the legitimate purpose for the new processing of the information and ensure consistency with the original purpose and the notice provided (see Notice below).
- Minimisation – determine the type(s) of Personal Information that is relevant for the new purpose and only receive or create the Personal Information relevant for the new purpose.
- Notice – determine the type(s) of Personal Information that is relevant for the new purpose and only receive or create the Personal Information relevant for the new purpose.
- Security – Implement appropriate security for the information, including any new access, systems, or technology necessary or used for the new processing.
- Accuracy – validate, update, and implement as appropriate, the processes that keep the Personal Information relevant and up-to-date and to rectify or erase inaccurate or incomplete Personal Information as appropriate for the new purpose.
- Rights Fulfilment – validate, update (if appropriate), and apply and enforce the retention period for the Personal Information in accordance with RPM's Record Retention Policy and develop processes to implement the retention times.
- Records Retention – determine appropriate retention times for the Personal Information and develop processes to implement the retention times in accordance with RPM's Record Retention Policy.
- In-Country Requirements – coordinate with the RPM Privacy Lead and Legal to understand and fulfil any in-country requirements (e.g., registering or updating a registration with, or obtaining approval from, competent regulators) as well as any restrictions applicable to the new processing activities.
- Data Protection Officers – coordinate with any applicable Data Protection Officers to the extent that the new processing involves a facility, location, or other part of the business with a Data Protection Officer.
- Third Parties – determine if any third parties will need to have access to the Personal Information as a result of the new processing, and if so, confirm that the requirements of Section 6 (RPM's Guidelines for Transferring Personal Information) below are met.

- Inventory and Assessments – follow the applicable RPM process to complete or update records of processing activity (inventory) and any assessments, including data privacy/protection impact assessments.
- Refresh – develop and follow a process to re-evaluate (and re-execute) the above as necessary before making changes to the processing of the Personal Information.

6. RPM's guidelines for transferring Personal Information

At times, RPM may transfer Personal Information to non-RPM third parties retained to process it on RPM's behalf. RPM will seek assurance that any transfers of Personal Information to those third parties will provide the same level of privacy protection as stated above. Additionally, RPM may be required to disclose certain Personal Information to third parties, including, for example: (1) as a matter of law (e.g., to a government agency with authority over RPM or applicable affiliates); (2) to protect RPM's legal rights; or (3) in an emergency where the health or security of an individual is endangered.

However, prior to providing a third-party access to Personal Information, whether internal (e.g., to another RPM legal entity) or external (e.g., a service provider processing the information on RPM's behalf, a government agency requiring the information or another third party), the Data Owner must fulfil the following requirements:

- Purpose – determine the legitimate business purpose for disclosing the information to or with the third-party, including whether granting such access is voluntary (e.g., a vendor) or mandatory (e.g., a court order or otherwise required by law).
- Minimisation – determine the Personal Information relevant for the third-party to access and limit the disclosure to only that Personal Information.
- Notice – verify that the notice provided to the individual(s) covers the disclosures to the third-party or provide an updated notice if necessary.
- Security – implement appropriate security for the disclosure of the information and the recipient's storage and processing of the information, including both organisational controls (e.g., access granting/revoking processes) and technical controls (e.g., encryption).
- Accuracy – validate, update, and implement as appropriate, processes to keep the Personal Information relevant and up-to-date and to rectify or erase inaccurate or incomplete Personal Information, even when in the hands of a third-party.
- Rights Fulfilment – update processes to incorporate the third party, to the extent applicable (e.g., copies held by the third party), to support fulfilling data subject rights requests.
- Records Retention – implement processes with the third party to determine appropriate retention times for the Personal Information and develop processes to implement the retention times in accordance with RPM's Record Retention Policy.
- In-Country Requirements – coordinate with the RPM Privacy Lead and Legal to understand and fulfil any in-country requirements (e.g., registering with, or obtaining approval from, competent data protection authorities) as well as any restrictions on processing the Personal Information for the stated purpose, including any requirements that result from access or transferring Personal Information to a third-party or a different country if applicable.
- Data Protection Officers – coordinate with any applicable Data Protection Officers about the transfer of Personal Information to the extent that the processing involves a facility, location, or other part of the business with a Data Protection Officer.
- Third Parties – for voluntary disclosures to third parties that will process the Personal Information on behalf of RPM, implement a process to govern the relationship with the third-party and appropriately manage data privacy risks around the processing of such information to ensure compliance with RPM's Data Privacy and applicable laws, including:
 - Undertaking to have appropriate protections in place to protect the Personal Information that reflects the nature of the relationship (e.g., a contract between RPM and the third-party with appropriate contractual terms); and
 - Assessing the security and controls of the third party around its processing of the Personal Information.
- Inventory and Assessments – follow the applicable RPM processes for updating records of processing activity (inventory) and any assessments, including any data privacy/protection impact assessments, to reflect the disclosure to the third party.

- Refresh— develop and follow a process to re-evaluate (and re-execute) the above as necessary before making changes to the processing of the Personal Information, including changes in the recipient (e.g., change in vendor) or its processing (when processing on behalf of RPM).

7. How does RPM access, store, use, transfer, and disclose Personal Information, and what is it used for?

Your information is provided to RPM throughout your dealings with RPM as an employee, recipient or potential recipient of RPM software and/or Services or by engaging with RPM as a supplier, partner or service provider to RPM.

Both Personal Information and non-personal information may be collected by RPM through your direct interactions with us, such as entering into contracts with RPM or filling out forms, sales enquiries and other transactions, publicly available data from third parties, such as data from marketing opt-in lists and data aggregators and from automated interactions such as RPM's Software Analytics program or from website cookies, URLs and tools.

RPM collects, uses, and discloses Personal Information as an essential part of its operations, while minimising the amount of your personal data that is shared. The Personal Information will be processed transparently and fairly. Further notice will be provided to the individuals when their Personal Information is collected, and it will describe how the Personal Information will be used and shared, unless there is a legitimate basis for not providing notice.

The information collected and held by RPM may be used and disclosed by RPM for purposes such as:

- Engaging in new transactions with you;
- Providing support or other services to you in accordance with fulfilling our contractual obligations to provide RPM software, technical services and/or training services to you;
- Continually improving the RPM licensed Software, annual maintenance and support services, consulting services and/or training services for you;
- With respect to the RPM Software Analytics program, the information collected can assist RPM with analysis about software bugs and crashes, analysis on the most used software features, provision of in-app messaging with the latest product news and automatic checks for the latest software updates, so RPM can let you know when they are available;
- Administering our relationship with you, providing RPM Software or Services, including in respect of any subscription based software and services;
- Verifying your identity and entitlement to RPM Software or Services when you contact RPM, including when RPM provides a response to any customer or supplier enquiries;
- Processing and responding to investor enquiries;
- Processing applications for employment;
- Processing and maintaining employee records (including bank, personal identification details) for current, prospective and/or past employees;
- Business development, including sending marketing releases, publications, and details of training events;
- Meeting legal or other regulatory obligations imposed on us;
- Auditing usage of our websites;
- Developing, customising, enhancing and operating the RPM Website and/or RPM Store and to carry out the transaction(s) you have requested or authorised;
- Provide customer support for any RPM Software or Services provided to you;
- Respond to questions or complaints;
- To conduct customer surveys;
- To detect and prevent fraud;
- To ensure safety and security throughout RPM offices.
- To identify or authenticate users and for access control purposes.
- To verify qualifications, experience, and suitability for a role.
- To facilitate access to RPM facilities (e.g., parking).
- To meet compliance obligations and to enable physical or remote access to RPM facilities or systems.
- To meet legal and safety regulations.
- To maintain a safe and healthy workplace.

- To determine an individual's ability to perform the inherent requirements of a role safely.
- To protect company assets, employees, customers, and the broader community. Providing you with any newsletter, product updates or technical alerts relating to any RPM Software or Services or in respect of any marketing communications and information on new RPM Software or Services;
- Solicit your opinion or feedback, provide opportunities for you to test RPM Software or Services;
- On the basis of our legitimate interest in the effective delivery of RPM's Software or Services and communications to you, as well as to our other customers and partners, in order to
 - Communicate commercial promotions and provide quotes for RPM Software or Services;
 - Research and implement product improvements and product updates;
 - Evaluate and improve the performance and quality of RPM Software or Services, and websites;
 - Provide you with a customised experience when you visit our websites;
 - Allow interoperability within our applications;
 - Secure our systems and applications;
 - Allow for the provisioning of services;
 - Enforce our legal rights; and
 - Share your data with partners for sales conversions and lead generation.
- To provide a more effective customer service, improve the RPM Website and/or RPM Store; and
- To provide you with important information about the RPM Software or Services that you are using, including critical updates and notifications.

You consent to RPM using artificial intelligence (AI) systems and algorithms, including to process your information. RPM will retain human oversight over all tools used, and will ensure the AI systems utilised do not use your information in any way that results in your information being disclosed to any third party or in a way that is a breach of any confidential or private information.

Occasionally, we may use Personal Information to provide you with information about other RPM Software or Services, together with events and promotions that we believe may be of benefit to you. If you prefer not to receive these updates, please email us at privacypolicy@rpmglobal.com and put "unsubscribe" in the subject line, together with the name of the publication you wish to unsubscribe from. Our marketing communications will also include an "unsubscribe" link.

We may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law, ASX listing rule requirements or respond to lawful requests or legal process; (b) protect the rights or property of RPM or our customers; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of RPM staff, customers or the public. We may also disclose Personal Information as otherwise permitted by law and as part of a corporate transaction such as a merger or sale of assets.

RPM is a global company, and as such, we may be required to process data in many countries. To conduct our business, and in accordance with this statement, you acknowledge that irrespective of your location and the origin of the Personal Data, RPM may store, transfer or process your Personal Data in Australia or any other country/region in which RPM or its subsidiaries, or authorised service providers maintain facilities. Outside of Australia, these locations include Canada, Chile, Colombia, Indonesia, Kazakhstan, Mexico, Singapore, South Africa, and the USA.

For the purpose of the RPM Software Analytics program, RPM may rely on third-party analytics services to collect and process this data and such data is stored and processed on servers located in Europe and the USA. All transfers will occur in compliance with the data transfer requirements of applicable laws and regulations. Further, RPM will comply with all international laws on sanction compliance when storing, transferring, using or processing your Personal Data in any location.

Where Personal Data originating from the EU is transferred to RPM entities or to third-party vendors engaged by RPM to process such Personal Data on our behalf who are located in countries that are not recognised by the EU as offering an adequate level of Personal Data protection, such transfers are covered by alternative appropriate contractual and security safeguards.

In the process of continuing to develop our business, we may also occasionally acquire subsidiaries or other business entities. As a result of such transactions, and for maintaining a continued relationship with you, we may transfer your Personal Data to an acquired and related affiliate. If we are involved in a reorganisation, merger, acquisition or sale of our assets, your Personal Data may be transferred as part of that transaction. We will notify you of any such deal and outline your choices in that event.

Except as otherwise described in this statement or with your permission, Personal Data you provide to RPM will **not** be shared outside of RPM.

RPM stores your Personal Information in different ways, including in paper and in electronic form. RPM takes the security of your Personal Information very seriously and uses a variety of security procedures in our RPM Website and RPM Store to help protect Personal Information from unauthorised access, use, or disclosure.

We may use cookies on the RPM Website and/or RPM Store.

When Personal Information is no longer useful, or, in any event, after the legal authority to retain it has expired, Personal Information will be destroyed in accordance with local law and pursuant to procedures established by the relevant RPM system or process.

8. How do we protect Personal Information?

RPM takes reasonable and appropriate technical, compliance, administrative and physical security and risk mitigation processes and safeguards that are designed in accordance with applicable laws to protect any Personal Information stored by RPM from any loss, misuse, unauthorised access, disclosure, alteration or destruction.

Protection mechanisms include (i) physical safeguards, including locked filing cabinets and secure document destruction and (ii) technical safeguards, including user authentication, network and data monitoring and other appropriate security measures across the RPM group of companies.

Further, RPM divides roles for protecting your privacy through the use of the RPM Privacy Lead, Data Owners, Data Users, Data Protection Officers, and Global Data Privacy Managers:

- **RPM Privacy Lead** – RPM must identify one or more persons within the business responsible for compliance with external data privacy laws and regulations and internal program requirements. Typically, this role is filled by a member of RPM Legal. The RPM Privacy Lead is responsible for executing Data Privacy initiatives, defining and tracking risks to Personal Information, and measuring and tracking success, all within RPM. Additionally, the RPM Privacy Lead will serve as a liaison, collaborating with the other affiliate Privacy Leads and the Global Data Privacy Manager.
- **Data Owners** – all Personal Information collected or held by RPM must have a data owner. The data owner is responsible for ensuring that Personal Information is collected and processed in accordance with applicable laws and RPM policies and procedures, including providing appropriate notice and obtaining any necessary consents. If Personal Information is used for a new purpose (i.e., different from the purpose determined by the Data Owner), then the individual processing the information for that new purpose becomes a Data Owner for that new purpose and must ensure that this procedure is followed for that new purpose. A Data Owner at RPM is generally defined as the individual(s) within RPM who face(s) the greatest negative impact from disclosure or loss of the information. For Personal Information, this means the Data Owner is the individual at RPM who is primarily responsible internally for the application or data-processing operation concerning the Personal Information. For example, if a business unit within RPM sponsors the creation of a website that collects Personal Information about potential customers, then the Data Owner for that information is the website owner (i.e., the business sponsor of the website, the individual identified by the business unit or the RPM CEO).
- **Data Users** - All individuals who have access to or engage in any form of processing of Personal Information are required to comply with the requirements of this Privacy Policy and only process Personal Information in accordance with the instructions of the Data Owner. For example, an employee who has access to an RPM's phone and email directory should only use the Personal Information in the directory in furtherance of legitimate RPM business and must not use it as a lead list for a personal business.
- **Data Protection Officer** – any individuals appointed by the applicable RPM company as a Data Protection Officer, either as required by law or at the discretion of RPM's CEO. Any individual appointed as a Data Protection Officer shall inform the RPM Privacy Lead of his or her appointment.
- **Global Data Privacy Manager** – The Global Data Privacy Manager provides subject-matter expertise and guidance in data privacy and, in conjunction with Legal, communicates changes in laws and requirements and changes in enterprise requirements, and creates and cascades training, communications, and tools to facilitate compliance and the appropriate management of risk.

RPM takes reasonable measures to prevent breaches of Personal Information. If these occur, we have a process in place to take swift action within our responsibilities and in accordance with any mandatory breach-notification requirements at law.

Reasonable and appropriate measures will be implemented to keep personal data confidential and to protect Personal Information against loss, manipulation, falsification, unauthorised access, disclosure, alteration and destruction by any party inside or outside RPM, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Taking into account technical considerations and costs, these measures shall ensure a level of security appropriate to the risk posed by the processing and the nature of the information being protected.

Everyone must keep Personal Information confidential and must not make Personal Information public except in very limited circumstances that are consistent with applicable law and only after appropriate notice to the individual whose information is being disclosed. Access to Personal Information should only be granted on a need-to-know basis that is consistent with the purposes for which the information is being processed.

9. Access to and correction of Personal Information

You have a right to request access to Personal Information held by RPM and to request its correction.

You may request to review, correct, update, suppress, or otherwise modify any of your Personal Information that you have previously provided to us through RPM's business partners, or object to the use or processing of such Personal Information by us. RPM procedures grant you access to your Personal Information and enable the exercise of other rights that may be available to you under applicable local law. In some cases, as mandated by local law, your right to access your Personal Information may be limited. Examples for why your access may be limited include:

- The request relates to legal advice and proceedings;
- A legal privilege may be claimed regarding the subject matter of the information;
- The Personal Information also includes the Personal Information of a third party who has not consented to disclosure and whose privacy would be affected by any such disclosure;
- The request is insufficiently detailed or has already been responded to;
- The request is frivolous or vexatious; or
- (Employees only) The information could disclose a confidential reference.

RPM will consider local laws when reviewing requests to access or alter Personal Information held by RPM.

If you require any changes, please contact us using the details in the contact information Section 12 (Reporting) of this policy below.

In your request, please make clear what Personal Information you would like to have changed, whether you would like to have your Personal Information that you have provided to us suppressed from our database or otherwise let us know what limitations you would like to put on our use of your Personal Information that you have provided to us.

While most questions and access-related issues can be handled quickly, complex requests may require more research and time. In such cases, issues will be addressed, or you will be contacted regarding the nature of the problem and the appropriate next steps.

RPM will retain your Personal Information for as long as your account with RPM is active; as needed to provide you with RPM Software or Services; as needed for the purposes outlined in this policy or at the time of collection; as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements; or to the extent permitted by law.

10. Agreement to the terms of this Privacy Policy, right to changes and withdrawal of consent

By contacting RPM, using the RPM Website, RPM Store, RPM Software Analytics and/or providing information to us, you consent, accept and agree to the collection and use of your Personal Information for the purposes described in this policy. In circumstances where it is not practical or possible for you to access this policy on RPM's website, RPM will, upon request made to the details in the contact information Section 12 (Reporting) of this policy below, provide you with a copy of this Privacy Policy.

Subject to applicable laws, you may have the right to request the following in respect of Personal Information stored or processed by RPM, including:

- to ask us to provide you with information regarding the Personal Information we process concerning you;
- to rectify, update, delete or erase any Personal Information concerning you;
- to withdraw any consent, you may have previously granted for RPM to use, access or process your Personal Information; and
- to lodge a privacy complaint with a supervisory authority, for example, the Australian Privacy Commissioner, if you are unhappy with the way that RPM has handled any Personal Information or the provisions of this policy;

As a company focused on serving the needs of businesses, RPM's websites, RPM Software or Services are not directed to, nor do we knowingly collect data from, children and minors. If you believe that we have mistakenly or unintentionally collected Personal Information of a child or minor, please contact RPM using the details set out in Section 12 (Reporting) of this policy below.

We ask that you not send us or share any sensitive Personal Information (e.g., government-issued or financial account numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, genetic, or biometric data, criminal background, or trade union membership).

Whilst RPM acknowledges your right to deal anonymously or by pseudonym and to elect not to permit RPM to collect or store Personal Information, except in relation to general enquiries or complaints made to RPM on an anonymous basis, it is impractical for RPM to deal with you with respect to RPM Software or Services unless you identify yourself and provide the required Personal Information.

11. GDPR

As an Australian business that offers goods and services to individuals in the European Union, RPM complies with the applicable requirements of EU General Data Protection Regulation (**GDPR**).

If you believe that your Personal Data was unduly collected or is unduly processed by RPM, please refer to Section 12 (Reporting) of this policy below.

12. Reporting

Anyone suspecting that the security of Personal Information (or systems that contain Personal Information) has been compromised, there has been an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Information, or that Personal Information has been or is otherwise being misused must immediately contact the below email.

If the Company Secretary is unavailable, the incident must be reported to the RPM CEO. Additionally, if the incident involves information security and is ongoing, it must be reported immediately to the RPM CEO and Company Secretary.

Requests relating to RPM's Privacy policy, including but not limited to complaints, details of alleged breaches of this policy or the APPs, requests for access to Personal Information or correction, complaints or concerns or for further information about how we process and treat Personal Information or comments or suggested improvements on RPM's Privacy policy, can be sent by email to: privacypolicy@rpmglobal.com or by writing to:

Company Secretary
RPMGlobal Holdings Pty Ltd
Level 14, 310 Ann Street
Brisbane, Queensland, Australia 4000
Ph: +61 7 3100 7200

13. Definitions and General

In this policy:

- Data Owner has the meaning detailed in Section 8 of this policy.
- Data User has the meaning detailed in Section 8 of this policy.
- Data Protection Officer has the meaning detailed in Section 8 of this policy.
- Global Data Privacy Manager has the meaning detailed in Section 8 of this policy.
- Personal Information has the meaning detailed in section 2 of this policy;
- RPM Privacy Lead has the meaning detailed in Section 8 of this policy.

Individuals who have permanent or regular access to Personal Information, who are involved in the collection of Personal Information or who participate in the development of tools to process Personal Information must participate in appropriate training regarding the requirements of processing Personal Information.

RPM reviews its policies regularly and occasionally may need to change or update them.

This Privacy Policy was last reviewed and updated on **1 September 2026**.