RPM INTERNATIONAL INC.
Global Data Protection Policy

1. Introduction

As directed by RPM International Inc.'s ("RPM") Code of Conduct referred to as the "Values & Expectations of 168," all of RPM's and its subsidiaries' (collectively with RPM, the "Company" or, each an "RPM Company") officers, directors and employees (collectively, "Employee(s)") must safeguard the privacy and security of everyone. Consequently, each RPM Company has the responsibility to look after the information that it collects about individuals, including information about individuals connected to its customers, suppliers, Employees and people browsing its websites. We must ensure we live up to the trust people have in us to protect their information.

Data protection laws give individuals the right to understand, and in some cases control, how their personal information is used. They also place obligations on each Company to handle people's information fairly and to respect their rights.

We take these obligations under data protection laws seriously. A breach of our data protection responsibilities could result in a violation of our values, a significant financial penalty being levied against us, negative publicity, damage to our brands or we could lose the trust of our customers.

To protect against these risks, this Global Data Protection Policy and its accompanying guidelines should be read and followed by Employees of all RPM Companies. Any such Employee who fails to comply with this Policy may be subject to disciplinary action, up to and including dismissal.

If you have any questions about this Policy, you should contact your Data Protection Champion, General Counsel, Chief Compliance Officer, Data Protection Officer (if applicable) or any one of the people listed as an RPM contact at compliancecontacts.rpminc.com or email dataprotection@rpminc.com.

2. Who and What is covered by this Policy?

This Policy applies to all RPM Companies and their Employees, including permanent and temporary employees and any third-party personnel such as agents, contractors and consultants, who have access to Personal Data processed by any RPM Company.

What is "Personal Data"? This Policy only applies to "***Personal Data***". That means information which relates to an identified or identifiable individual (i.e. a natural person). It includes by way of example: names, addresses, email addresses, job applications, photographs, employment records, purchase histories, bank details and correspondence to and from an individual. Where it can be linked to an individual, it also includes web browsing information (e.g. cookie data) and IP addresses.

What is "Sensitive Personal Data"? Certain Personal Data is designated as "***sensitive***" and requires enhanced protections under the European Union's ("EU") General Data Protection Regulation ("GDPR"). Sensitive Personal Data is Personal Data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric or genetic information; or information about a person's health, sex life or sexual orientation.

What's "processing"? This Policy also talks about "***processing***" Personal Data. Processing essentially means *doing anything with* Personal Data; this includes collecting it, storing it, accessing it, combining it with other data, sharing it with a third-party, and even deleting it.

RPM Companies process Personal Data about our customers and prospective customers, our customer's staff and customers, our own staff, job applicants, staff at our suppliers, and people who visit our premises and browse our websites. All of this Personal Data should be treated in accordance with this Policy.

3. RPM's Data Protection Principles

This Global Data Protection Policy consists of the following Data Protection Principles. RPM Company Employees should follow our Data Protection Principles when processing Personal Data.

1. Fairness and Transparency: Give people information about how RPM processes their Personal Data.

What does this mean?

We should be transparent and give people information about how we use their Personal Data. This also means not doing anything with their Personal Data that they would not expect or about which we would be embarrassed for them to know.

In particular, we should inform people if their Personal Data will be passed to a third-party. Similarly, if we receive Personal Data about an individual from a third-party, we should make sure the individual knows we have their data promptly.

2. Lawful Processing: Make sure we always have a good, lawful reason to process Personal Data.

What does this mean?

This means that we need to make sure that we are legally allowed to process Personal Data.

RPM Companies should only process Personal Data in accordance with applicable data protection law. Under the GDPR, which is applicable to Personal Data of European Economic Area (**EEA**) persons processed by your Company, the most relevant of these are the following:

(i) The individual has consented. For example, under GDPR or other applicable regulations, RPM Companies may be required to obtain consent from individuals before sending them email marketing communications.
(ii) The processing is necessary for a contract with the individual. For example, we may need to process an individual's contact and bank details (or details of a contact at a business customer) to deliver goods and services that they have ordered from the Company.
(iii) The processing is necessary to comply with a legal obligation; or
(iv) The processing is necessary for our (or a third-party's) legitimate interests, which are not overridden by any risk or harm to the individuals. For example, each Company will need to process certain Personal Data relating to its Employees to manage their performance, development and benefits etc.

To comply with GDPR, as applicable, RPM Companies should only process Sensitive Personal Data in exceptional circumstances, where it is satisfied it has a lawful basis for doing so under applicable law. For example, Sensitive Personal Data about our customer's employees may be processed where it is necessary to carry out our obligations under a services contract (e.g. where we manage building access security systems, this may involve the processing of biometric data such as fingerprint or retinal recognition in certain circumstances).

3. Purpose Limitation: Only collect Personal Data for a specific business need. If we want to reuse the Personal Data for a new purpose, we must make sure the two are compatible.

What does this mean?

We should always have a clear purpose for any Personal Data before we collect it, and this should reflect a specific business need. We may also need to conduct a Data Protection Impact Assessment for certain types of processing or when processing may be likely to result in an elevated risk to individuals' interests. To assess the level of risk, we may need to consider both the likelihood and the severity of any impact on individuals. High risks could result from either a high probability of some harm, or a lower possibility of serious harm. For further guidance on whether a Data Protection Impact Assessment is required, and how to conduct one, please refer to the Data Protection Impact Assessment Guide found at RPMImpactAssessmentGuide.rpminc.com.

If an RPM Company later wants to use the Personal Data for a new or different purpose or share it with a new third-party, we should consider whether it is compatible with the original purpose, whether it complies with applicable law and whether it would be within the reasonable expectations of the individual to whom the Personal Data relates.

Before starting any new processing or collecting any new Personal Data, you should speak to the Data Protection Champion, General Counsel or Chief Compliance Officer for your Company, to ensure data protection and privacy is considered from the outset. If there could be risks associated with any new processing, your Company may need to conduct a *Data Protection Impact Assessment* (RPMGlobalDataPrivacy.rpminc.com) to decide whether any safeguards need to be put in place to protect the individuals.

4. Data Minimisation: Only process as much Personal Data as we need, and no more.

What does this mean?

In any particular case, RPM Companies should only collect or otherwise process as much Personal Data needed for that specific purpose. This means we should not collect Personal Data that we do not need nor ask for Personal Data 'just in case' it may be useful.

Before asking for or accessing information about someone, you should ask yourself whether you *really* need that information to achieve your result.

5. Accuracy: Keep Personal Data accurate, complete and up-to-date.

What does this mean?

Wherever possible, RPM Companies should give individuals the opportunity to amend or correct their Personal Data (and offer a self-service tool where possible, for example an HR portal for staff to access and update certain Personal Data that the Company holds about them). If you independently become aware of Personal Data which is inaccurate or out-of-date, we should take reasonable steps to correct it or delete it.

All Employees should inform HR about any changes in their Personal Data processed by the Company.

6. Retention: Only keep Personal Data for as long as needed. If we don't need the Personal Data anymore, we must delete it or anonymise it.

What does this mean?

RPM Companies should only keep Personal Data for as long as needed for its specified purpose. Once the Personal Data is no longer needed, it should be deleted, or anonymised so that it cannot be used to identify individuals.

7. Security: Protect Personal Data from getting lost or stolen. Make sure our service providers protect our Personal Data as well.

What does this mean?

We must make sure we protect Personal Data with appropriate security measures to prevent any accidental or unauthorised access, damage, loss or disclosure.

Although all Personal Data requires adequate and reasonable safeguards, enhanced safeguards are necessary to protect Sensitive Personal Data and Personal Data that is related to bank accounts, credit card accounts, and personal identifications numbers such as Social Security Numbers (the latter referred to herein as "Highly Confidential Sensitive Data"). You must ensure that all documentary ("hard copy") Sensitive Personal Data and Highly Confidential Sensitive Data is properly stored in locked containers, offices or cabinets that are not accessible to unauthorized users. Electronic storage devices and files containing Sensitive Personal Data or Highly Confidential Sensitive Data should be password protected and/or encrypted to prevent unauthorized access. For instructions on how to password protect or encrypt documents and external storage devices, please refer to RPM's Password Protection/Encryption Instructions (RPMPasswordEncryptionInstructions.rpminc.com).

If you become aware of any actual or suspected loss or breach of security relating to Personal Data or do not believe the appropriate security measures are being used to protect Personal Data, you should immediately report it to your Data Protection Champion, Chief Compliance Officer or General Counsel or in accordance with the RPM Non-Retaliation and Reportable Events Policy and the RPM Data Breach Reporting Policy, as appropriate.

This Security Principle extends to our service providers who handle Personal Data on our behalf. RPM Companies should only appoint service providers who can provide appropriate protection for Personal Data they process. In order to ensure appropriate due diligence is

conducted, you should consult with your Data Protection Champion, Chief Compliance Officer or General Counsel before appointing any service provider who will have access to Personal Data, even where the provider is offering a free or inexpensive service or trial (for example this could be a provider of a new IT system).

8. Individual Rights: Allow individuals the right to access, correct or erase their Personal Data, or object to it being used for certain purposes.

What does this mean?

We may have an obligation to provide a copy of Personal Data and allow correction of inaccurate Personal Data by the person who is the subject of the Personal Data. In certain circumstances, the subject of the collection may also have a right to have their Personal Data erased, transferred to another party or not used for a particular purpose. For example, individuals have a right to "opt-out" of receiving marketing from the Company.

The Company must respect these rights and respond to requests in accordance with applicable law. However, under certain circumstances, the Company may be entitled to refuse such requests. If you receive a request from an individual relating to her Personal Data, you should refer it to the Data Protection Champion, Chief Compliance Officer or General Counsel for your group.

9. Personal Data Transfers: Put in place safeguards before sending Personal Data outside Europe.

What does this mean?

Because data protection standards may not be the same in countries outside the EEA, EU data protection laws place restrictions on when Personal Data of data subjects who are in the EEA may be transferred outside the EEA. The transfer will only be allowed if certain safeguards are put in place to protect the Personal Data, wherever it goes.

These restrictions apply whether the Company is sending EEA Personal Data to a third party (e.g. a US-based cloud provider) or another company within RPM. Importantly, the restrictions apply not only when the Personal Data will be stored in the non-EEA country, but also if the Personal Data will only be accessed remotely from that country (e.g. if a third-party IT service provider or one of our staff members based outside the EEA has remote access to Personal Data on our systems in the EEA).

You should consult with the Data Protection Champion, Chief Compliance Officer or General Counsel of your Group before sending Personal Data outside the EEA or allowing a party outside the EEA to have access to Personal Data stored within the EEA.

Similar restrictions may apply in other countries where we gather Personal Data. Should you wish to transfer Personal Data out of the country in which it was gathered, confirm the legal requirements in that country with the Data Protection Champion, Chief Compliance Officer or General Counsel of your group.

10. Accountability: RPM Companies will take steps to make sure our processing of Personal Data complies with this Policy.

What does this mean?

Each RPM Company is responsible for establishing controls required to ensure its processing of Personal Data is compliant with applicable law. RPM has implemented this Global Data Protection Policy, as well as accompanying guidelines covering: Data Protection Impact Assessments, Individual Rights, Privacy by Design, Data Breach Reporting and Personal Data Retention, among others (see the Data Protection Champion, Chief Compliance Officer or General Counsel of your Group for copies).

Each Company is also responsible for conducting and supervising the completion of training for all personnel who process or have access to Personal Data. Such training must educate the relevant personnel on their responsibilities under this Policy and the accompanying guidelines.

Any new websites, apps, user functionality platforms or other tools should be designed to enable RPM Companies to comply with this Policy and Global Data Protection Principles contained herein.

Each RPM Company has a Data Protection Champion, Chief Compliance Officer and General Counsel assigned to it, who will assist with the application of this Policy and any data protection queries. RPM has also appointed a Global Data Protection Champion who has overall responsibility for this program.

This Policy and the accompanying guidelines will be periodically reviewed and updated as necessary to ensure that they are effective and meet applicable requirements.

Last updated May 2018