

RPM International Inc. Employee Data Privacy Notice

For use in Countries Other Than the U.S. and Canada

1. Introduction

RPM International Inc. ("RPM") and its affiliated companies (separately and collectively the "Company", "we" or "us") are committed to complying with all applicable Data Protection Laws (as defined below). This Employee Data Privacy Notice (the "Notice") describes how the Company collects, discloses, or otherwise uses Employment Data (as defined below), sets forth the data privacy responsibilities and obligations of the Company's employees, and discloses the data privacy rights afforded to individuals under certain Data Protection Laws (as defined below). This Notice may be substituted or supplemented by applicable local law. Any individual rights and/or obligations herein apply only in those countries and to those individuals where they are legally required or permissible, respectively.

In this Notice, we refer to Personal Information processed in the employment and Human Resource context as "Employment Data" and applies to current and former members of our workforce, including employees, workers, agency workers, contractors and self-employed consultants, as permitted by applicable law. When processing Employment Data, the Company is considered a "Data Controller," which means that we determine the purposes and means of processing the Employment Data.

2. Overview: Our 10 Data Protection Principles

The Company observes these 10 Data Protection Principles in relation to Employment Data:

- a) **Fairness and Transparency:** We will provide individuals with information about how we process their Employment Data.
- b) **Lawful Processing:** We will take steps to ensure we always have a good, lawful reason to process Employment Data.
- c) **Purpose Limitation:** We will only collect Employment Data for a specific business need. If we want to use the Employment Data for a new purpose, we will make sure the two are compatible or that we have another lawful basis.
- d) **Data Minimisation:** We will endeavor to only process as much Employment Data as we need.
- e) **Accuracy:** With your help, we will keep Employment Data accurate, complete, and up-to-date.

- f) **Retention:** We will only keep Employment Data for as long as we need it and in accordance with applicable law.
- g) **Security:** We will implement technical and organizational security measures to protect Employment Data from getting lost or against other unauthorized processing, and we will require our service providers protect our Employment Data.
- h) **Individual Rights:** We will, when required by law, allow individuals the right to access, correct or have erased their Employment Data, to receive their data in a structured, commonly used and machine-readable format, to restrict or object to it being used for certain purposes, or to withdraw their consent to its processing, as required by applicable law.
- i) **Employment Data Transfers:** We will ensure adequacy decisions or safeguards are in place before transferring Employment Data to third countries.
- j) **Accountability:** We will take reasonable measures to ensure that our processing of Employment Data complies with applicable Data Protection Laws and this Employee Privacy Notice.

3. What Employment Data does the Company collect?

The Company collects various types of Employment Data, both in paper and electronic form, about you in connection with your work at the Company, including “sensitive” or “Special Category” Employment Data (e.g., race, gender, health data, trade-union membership). This may include the following categories of Employment Data:

- a) **Contact details**, such as your address, telephone number and email address, etc., and contact details of others that you provide, such as who to contact in the event of an emergency, details of your dependents, life insurance beneficiaries, etc.
- b) **Financial and benefits-related information** relating to your compensation, benefits and pension arrangements (if applicable), such as details of your salary and any deductions, bank account, tax codes, social security number (or the local equivalent), corporate credit card usage, employment benefits, travel expenses, etc.
- c) **Recruitment information**, such as your curriculum vitae/resume, notes of interviews, application forms, decisions to offer employment, background information and third party references (if recorded), pre-employment drug tests (if applicable), criminal records check file (if applicable), and psychometric test results (if applicable), etc.
- d) **Employment Administration and Career information**, such as employment and career history, photograph, absence and attendance records (including hours worked), health and safety records, gender, age, sickness records, accident reports, performance information (including any appraisals, performance reviews, or other internal communication regarding

performance), employment drug testing (if applicable), compliance related behavior (e.g., grievance or disciplinary records, compliance training course assignments, violations of Company policies and procedures, hotline submissions, internal complaints or claims, investigations, results and remediation steps and actions), skills and experience records, records of projects you have worked on, termination details, etc. This also includes information obtained in the administration of Company assets including Company e-mail, Company IT accounts, IT collaboration tools, and helpdesk information.

- e) **Location Information** (where such information is legally permitted to be collected), such as when recorded by electronic card access systems and location data related to the use of our information resources.
- f) **Technical and Asset Usage Information:** such as information about your use of Company data, computers, devices, networks, systems, software, telephones, and other information and communications technology that is owned, licensed, or maintained by the Company (where such information is legally permitted to be collected). For more information about your use of Company assets please see our [Acceptable Use Policy](https://policies.rpminc.com/legal-compliance-policies/acceptable-use-policy/), which is accessible at <https://policies.rpminc.com/legal-compliance-policies/acceptable-use-policy/>.
- g) **Information that may reveal sensitive characteristics** including race or ethnic origin, gender, religious or philosophical beliefs, or information that concerns health, for example to identify or keep under review the existence or absence of diversity and inclusion (where permitted and in accordance with applicable law).
- h) **The Company may collect biometric data** for employment, health and safety, security, and administrative purposes. For more information with respect to the Company's collection, use, and processing of biometric data, please see our [Employee Biometric Data Policy](https://policies.rpminc.com/legal-compliance-policies/covid-19-policies/employee-biometric-data-protection-policy/), which can be accessed at <https://policies.rpminc.com/legal-compliance-policies/covid-19-policies/employee-biometric-data-protection-policy/>.
- i) **Other information** which you voluntarily provide in the course of employment that it is necessary to hold or use for our business purposes. For example, where you register an interest in a particular sport or activity we run for our staff.

4. What are the Sources of Employment Data?

The Company collects this Employment Data directly from you, and in some instances, from third parties.

- a) **Employment Data Directly from You:** The Company generally collects Employment Data directly from you (electronically, in writing, or verbal). The Company may, for example, ask you for Employment Data when you begin your employment with the Company. You may also provide new, or updated or corrected Employment Data to the Company from time-to-time.

- b) **Employment Data from Third Parties:** The Company may receive Employment Data from your colleagues or supervisors, for example, in the context of performance evaluations. The Company may also receive Employment Data from third parties who provide services to the Company, such as companies that provide benefits, payroll or other services. If, for example, you were hired through a third-party staffing or recruiting firm, we will receive Employment Data on your professional experiences. Employment Data from third parties may include Special Category Data, such as recruitment agencies, job boards, behavioural, training providers, professional assessors, occupational health professionals, and background check providers. Where we receive such information from these third parties, we will only use it in accordance with this Notice. In some cases, the third party will be acting as a controller of your Employment Data and in such cases we may advise you to read their privacy notice and/or data protection policy.

5. **What will the Company do with your Employment Data and what is our Legal Basis for Processing?**

The main purposes for which we use Employment Data is set forth below. The Company will only process your Employment Data where we have a legal basis for doing so. The Company's processing of Employment Data is generally required because it is necessary for us to do so in connection with your employment contract (e.g. so we can pay your salary) or because it is in our legitimate interests to do so (e.g. to protect the security and integrity of our systems and premises). In addition, certain processing may be necessary to comply with our legal or regulatory requirements, or, where applicable, based on your consent (which you have the right to withdraw). More specifically, we process Employment Data as follows:

- (a) **Compliance with Legal Obligations**, this may include confirmation of eligibility to work in a specific country as required by immigration laws, such as processing passport and visa documentation; payroll records, social security, child maintenance, marital status, student loans and national insurance information, to comply with social security and Taxation Authorities (tax) requirements; information in relation to legal claims made by you or against you, in order to comply with court processes and court orders including court ordered deductions from pay; accident investigations; information relating to the occurrence, investigation or prevention of fraud and any other criminal offences or information required in the Civil Courts; pension benefits to comply with pension legislation; and - certain checks in specific countries (e.g. DVLA/DVSA in the UK and RSA checks in Ireland) to validate driving license information including the number of points on your license in the event you drive our vehicles or hire cars.
- (b) **Workforce Planning and Recruitment**, business forecasting, employee assignment planning, budgeting, job advertising, interviewing, selecting and hiring staff. The Company uses various legal grounds as a basis for this data processing, such as: (i) the performance of the employment contract, (ii) legitimate Interests (as set out above), and (iii) compliance with works council agreement, where applicable.

- (c) **General Human Resources Management and Administration**, employee career development, performance management, compensation and benefits management and benchmarking, administering payroll and benefit arrangements (including long-term incentive awards and bonus administration), obtaining management and employee satisfaction feedback, managing absences (e.g. sickness, parental leave and other family related and flexible working policies), health and safety, travel and expense management, general headcount reporting, disaster recovery, emergency response planning and Code of Conduct compliance. The Company uses various legal grounds as a basis for data processing, such as: (i) the performance of the employment contract, (ii) legitimate Interests (as set out above), and (iii) compliance with works council agreement, where applicable.
- (d) **Performance of RPM's Business Operations**, carrying out the Company's day-to-day business activities, allowing us to work together and collaborate, providing services to our customers and ensuring business continuity. The Company uses various legal grounds as a basis for data processing, such as: (i) the performance of the employment contract, (ii) legitimate Interests (as set out above), and (iii) compliance with works council agreement, where applicable.
- (e) **Security Management and Internal Investigations**, ensuring the security of the Company's premises, assets, information, and employees. The Company uses various legal grounds as a basis for data processing, such as: (i) the performance of the employment contract, (ii) legitimate Interests (as set out above), and (iii) compliance with works council agreement, where applicable, and (iv) your consent (i.e., some EU member state law may require your consent in order to access the content of your communications, and if the Company asks you to provide your consent to a specific processing activity; you may refuse to give and withdraw your consent at any time).
- (f) **Marketing, Advertising and Public Relations**, displaying employees' business contact details and names or photographs on our website, or on other professional social media websites and in other means of communication such as press releases, newsletters or marketing materials. The Company uses various legal grounds as a basis for data processing, such as: (i) legitimate Interests (as set out above), and (ii) compliance with works council agreement, where applicable.
- (g) **Complying with Health and Safety Obligations**, including taking the following actions: helping to maintain the health and safety of the Company's employees and others in the workforce; implementing and maintaining emergency and/or exposure management programs concerning hazardous substances; assessing the working capacity of an individual; reintegrating individuals into the workforce (including checking and monitoring fit-for-work status); providing support and care for individuals entitled to benefits in connection with illness or (partial or full) work incapacity; detecting and responding to an incident; managing the employee health file; providing employees with social benefits that depend on the state of an individual's health (e.g., parental leave, sick leave); maintaining proper documentation of accidents and first-aid health care in case of incidents; and responding to pandemics,

epidemics, and other health emergencies (including temperature and health screening). The Company uses various legal grounds as a basis for data processing, such as: (i) compliance with legal obligations, (ii) protection of vital interest, (iii) occupational health, and (iv) compliance with works council agreement, where applicable.

- (h) **Carrying out Diversity and Equal Opportunity Monitoring and Reporting**, thereby enabling the Company to support employees in expressing their individual diversity, ensuring that our workforce is positioned to meet the diverse needs of our consumers, ensuring that talent systems and practices support the development and advancement of all employees, and generating aggregated level reports and analytics for the Company so that we have a better understanding of our diversity in support of inclusive cultures. The Company uses various legal grounds as a basis for data processing, such as: (i) compliance with legal obligations, (ii) legitimate interests (for certain non-sensitive data), and (iii) compliance with works council agreement, where applicable.
- (i) **Other Legal and Regulatory Compliance**, ensuring compliance with health and safety requirements and other legal or fiscal obligations, in connection with litigation or an internal investigation or audit and to ensure compliance with our policies regarding anti-money laundering, bribery, fraud and corruption. To pursue our (or a third party's) legitimate interests as a business. This may include processing: training records, appraisals, 360 review reports and 1:1 meeting notes about you in order to assist/assess your career development and training needs and/or to ensure that you are properly managed and supervised; information relating to the performance of your employment duties, such as disciplinary records, as this is relevant to your ability to carry out your job and for us to assess and identify areas in which we may need to help you improve; information relating to the performance of your duties may also be used to conduct an investigation if circumstances warrant it and to take appropriate action either for conduct or capability reasons in accordance with our Grievance and Disciplinary Policies/Procedures; information relating to any grievance process involving you, in order that an investigation may be conducted and appropriate action taken (if any) in accordance with our Grievance and Disciplinary Policies/Procedures; management reports (including statistical and audit information) to ensure workplace efficiencies are maximised; health, safety and environmental information, including records to ensure that we are complying with relevant policies and procedures; work related contact details on our intranet and/or internal systems to facilitate efficient communication within the business; voicemails, emails, correspondence and other work-related communications created, stored or transmitted by you using our computer or communications equipment for the purposes of the efficient management of the business in accordance with the applicable law, our IT Security Policies and our Acceptable Use Policy; non-medical absence records and details including holiday records, appointments, jury service, maternity, paternity, adoption and parental leave in order to monitor attendance levels and to comply with our policies; CCTV across the whole of our estate for the protection of our property, security reasons, health and safety reasons and to ensure business efficiencies; network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access in

accordance with applicable law, our IT Security Policies and our Acceptable Use Policy; data relating to tracking devices/technologies and activities in respect of our vehicles you drive, in order to maximise efficiencies within the business; photographs of you are retained in your employment records and may be included on security and access cards and in internal directories; photographs and videos of you are used in newsletters, bid documents and training and marketing materials to enable us to efficiently manage and develop our business; use of voice and video recordings captured by mystery shoppers for the purposes of quality assurance, identifying individual training needs and providing training to staff to improve the overall quality of the services provided. The Company uses various legal grounds as a basis for data processing, such as: (i) compliance with legal obligations, and (ii) legitimate interests (in particular in cases involving compliance with foreign laws and regulations).

- (j) **Criminal Convictions**, In certain circumstances we may process information about criminal convictions. We will only collect this information if it is appropriate given the nature of your role and where the law allows us to do so. We may collect this information as part of the recruitment process, as part of the checks that we are required to undertake if you drive for us or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal offences and convictions in the following ways: checking for driving convictions to ensure that you may lawfully drive Company or hire vehicles and where appropriate as part of a disciplinary procedure or to recover losses of fees and salary paid where gained by way of pecuniary advantage.
- (k) **Automated Processing**, when legally permissible, we may use automated systems to profile your data. "Profiling" means any form of automated processing to evaluate certain personal aspects relating to you, in particular to analyse or predict aspects concerning performance at work, development, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements. However, You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you. Automated decision-making takes place when an electronic system uses information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances: Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights and freedoms and legitimate interests; Where authorised by law and where appropriate measures are in place to safeguard your rights and freedoms and legitimate interests; and with your explicit consent and where appropriate measures are in place to safeguard your rights and freedoms and legitimate interests. Subject to applicable law, you will have the right to obtain human intervention, to express your point of view, and to contest the decision.
- (l)

6. Who is your Employment Data shared with?

- (a) **Within the Company and Among our Affiliates**, the Company restricts access to Employment Data to people within the Company (which is defined to include RPM and all

its affiliated companies) who have a “need to know” that information. For example, your manager will have access to certain Employment Data for career development purposes and performance management.

- (b) **With Outside Service Providers,** We also share Employment Data with service providers who act on the Company’s behalf, such as our IT support providers (e.g., companies who provide software and computing services, data management and storage services, web-hosting, and email services); technology companies who provide hardware and equipment (e.g., manufacturers and distributors of computers); support services such as companies that provide business support services (e.g., mailing vendors, printing services, office cleaning, and companies that install, service and monitor alarm systems), companies that provide financial administration (e.g., payroll providers who assist in calculating salary and wages, bill payment and employee benefit services), companies that provide waste and disposal services (e.g., shredding provider). The service providers are generally bound by law or contract to protect the confidentiality and security of Employment Data, and to only use Employment Data to provide requested services to the Company and in accordance with applicable law.
- c) **With Other Third-Parties,** The Company may also share data with other companies, vendors and business partners to perform functions for us, whereby these companies are themselves responsible to determine the purposes and/or means of the processing and for the lawfulness of the processing. Examples include financial institutions such as banks involved in processing compensation payments or providing the Company financing; financial institutions such as non-life (property and casualty) and life insurance companies involved in the provision of employee benefits; financial services such as assets managers, pension administrators, and actuaries who assist the Company in providing employee benefits; support services such as business support companies and business training and employment agencies who provide business or management training courses and employment services (e.g., third party recruiting agencies who identify candidates for employment and/or who provide contingent and leased employees); telecommunications companies who provide fixed line and mobile telecommunications services; technology companies that provide technology and hardware such as telecommunications equipment; travel and leisure companies such as travel agency(ies), hotels, airlines, car rental agencies and other companies involved in providing corporate travel services; health care equipment and services companies such as health providers who provide medical services to the Company; and other parties (such as legal and regulatory authorities, accountants, auditors, lawyers and other outside professional advisors) if needed to support auditing, compliance, legal, financial or corporate governance functions and/or in accordance with the law.
- d) We may share Employment Data with third parties in the event of an actual or potential merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company’s practice or assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Employment Data held by the Company is among the assets transferred.

- e) We may share your Employment Data with third parties when required to comply with the law, or when such disclosure is in our legitimate interest, provided such disclosures based on legitimate interests are not prohibited by law.
- f) We may share your Special Category Employment Data with third parties for other reasons. For example, to comply with our legal obligations we may share your data with the following: Taxation Authorities for tax purposes; Immigration Authorities for immigration purposes; student loan agencies to ensure that appropriate reductions are made from your salary; DVLA/DVSA checks in the UK and RSA checks in Ireland to validate driving license information and the number of points on your license if you drive company vehicles.

7. How long will the Company Retain your Employment Data?

The Company will retain your records in accordance with industry standards and its internal policies, and as long as needed to satisfy its responsibilities or its own legal or regulatory obligations, or to protect its legal interests and business needs, as permitted by applicable law. The Company will destroy all Personal Information and any devices and assets that retain or transmit Personal Information in accordance with applicable law, industry standards and its internal policies, and the Company may contract with a third-party vendor to perform these data disposal and asset destruction functions on the Company's behalf.

8. Where does the Company Store your Employment Data?

RPM is headquartered in the United States, and you should be aware that your Employment Data may be transferred to, and stored in, the United States or another location outside your country of residence, which may have less strict, or no data protection laws, when compared to those of your country of residence. It may also be processed by staff of the Company (defined to include RPM and all RPM affiliated companies) or one of their respective suppliers operating outside of your country of residence.

In the event we transfer your Employment Data outside its originating country, we will take legally required steps to ensure that adequate safeguards are in place to protect your Employment Data and to make sure it is treated securely and in accordance with this Notice. For example, if your reside in the EEA or the UK and we transfer your Employment Data outside the EEA and the UK to other Company operating entities we will do so in accordance with the Company's Intra-Group Data Transfer Agreement, and transfers to third parties located in other third countries outside the EEA and the UK will take place using an acceptable data transfer mechanism, such as the EU Standard Contractual Clauses, Binding Corporate Rules, approved Codes of Conduct and certifications or, in exceptional circumstances, on the basis of permissible statutory derogations.

9. Exercising your Data Privacy Rights.

Under the conditions set by applicable Data Protection Laws, you may have the following rights regarding your Employment Data:

9.1 Access. The right to obtain from us confirmation if Employment Data is being processed, a copy of that Employment Data, the purpose of processing, the categories of data, the legal basis of the processing, information on recipients of the data and the countries in which they are located, the safeguards put in place for the transfer of data to third countries, storage period of data or criteria to determine it, further information on your rights, our processing activities, sources of information and the significant and envisaged consequences of processing.

9.2 Rectification. The right to request the rectification of inaccurate Employment Data and to have incomplete data completed.

9.3 Objection. The right to object to the processing of your Employment Data for compelling and legitimate reasons relating to your particular situation, except in cases where legal provisions expressly provide for that processing.

9.4 Portability. The right to receive your Employment Data that you have provided to us, in a structured, commonly used and machine-readable format and you have the right to transmit it to other data controllers without hindrance. This right may only exist if the processing is based on your consent or a contract and the processing is carried out by automated means.

9.5 Restriction. The right to restrict processing of your Employment Data if (i) you contest the accuracy of it (at least for the period we need to verify your request); (ii) the processing is unlawful and you oppose the erasure of it and request restriction instead; (iii) we no longer need it, but you tell us you need it to establish, exercise or defend a legal claim; or (iv) you object to processing based on public or legitimate interest (for the period we need to verify your request).

9.6 Erasure. The right to erase your Employment Data if (i) it is no longer necessary for the purposes for which we have collected it, (ii) you have withdrawn your consent and no other legal ground for the processing exists, (iii) you objected and no overriding legitimate grounds for the processing exist, (iv) the processing is unlawful, or (v) erasure is required to comply with a legal obligation.

9.7 Right to Lodge a Complaint. The right to lodge a complaint with a supervisory authority, in particular in the UK or the EU Member State of your residence, place of employment, or the location where the issue that is the subject of the complaint occurred.

- a) For data protection authorities in the EEA, please see here: https://edpb.europa.eu/about-edpb/about-edpb/members_en.
- b) For the data protection authority in Switzerland, please contact the Federal Data Protection and Information Commissioner (<https://www.edoeb.admin.ch/edoeb/en/home.html>).
- c) For the data protection authority in the UK, please contact the Information Commissioner's Office (<https://www.ico.org.uk>).

9.8 Right to Refuse or Withdraw Consent. Please note that in case we ask for your consent to processing, you may have the right to refuse to give consent and to withdraw your consent at any time without any adverse negative consequences. The lawfulness of any processing of your Employment Data that occurred prior to the withdrawal of your consent will not be affected.

Any request to exercise one of these rights will be assessed by the Company on a case-by-case basis. There may be circumstances in which we are not legally required to comply with your request because of the laws in your jurisdiction or because of relevant legal exemptions provided for in applicable data protection legislation. You should contact RPM's Chief Compliance Officer, General Counsel or you may email dataprotection@rpm-inc.com if you would like to exercise your rights.

10. Your Obligation to Safeguard Personal Information.

In the event you have access to Employment Data or other Personal Information by way of your employment or otherwise in connection with the Company you shall collect and use such data in accordance with all applicable Data Protection Laws and Company policies.

If you have access to an individual's Special Category Data, social security number, driver's license number, or other government identifiers, financial information, or other Personal Information you shall (i) protect its confidentiality, integrity, and availability, (ii) protect it from any unlawful or unauthorized access, use, or disclosure, including compliance with the Password Policy, which can be accessed at <https://policies.rpm-inc.com/data-privacy-policies/password-policy/>, and (iii) limit its access and use to the minimum extent necessary and required to perform an authorized business or legal function.

All new or revised data processing activities involving Personal Information must comply with the DPIA Policy, which can be found at <https://policies.rpm-inc.com/data-privacy-policies/dpia/dpia-policy/>.

If you become aware of, or reasonably suspect, a breach of Employment Data or any Personal Information, you must immediately notify your supervisor and submit a reportable event at https://rpm-inc.ethicspointvp.com/custom/rpm-inc/forms/mgr/form_data.asp?land=en in accordance with our Reportable Events Policy, which is accessible at <https://policies.rpm-inc.com/reportable-events-and-hotline-policies/reportable-events/reportable-events-policy/>.

It is your responsibility to ensure that any Personal Information that we hold about you is accurate and up to date by keeping us informed of any relevant changes. You can update your details by contacting HR.

11. Contact us

Please contact dataprotection@rpm-inc.com if you would like to find out more about any matters relating to this Notice.

If you have concerns about the way in which we have handled your Employment Data you may have the right to complain to the applicable Data Protection Authority for the Company processing your information. However, if you do have concerns, we encourage you to raise them with us in the first instance.

This Notice may be amended from time to time to reflect any changes in the ways in which we process your Employment Data. We will make updates available to you, and we reserve the right to notify you in other ways from time to time about the processing of Employment Data.

Definitions

For purposes of this Notice, the following definitions shall apply:

“Data Protection Law” refers to any EEA, EU or UK data protection laws, statutes, and regulations applicable to the Company in the context of the Company’s collection, processing, retention, dissemination, disclosure, transfer, disposal, or use of Personal Information.

“Personal Information” means any information relating to an identified or identifiable natural person, or as otherwise defined under applicable Data Protection Law.