RPM International Inc.

April 29, 2022

RPM INTERNATIONAL INC.
AND ITS SUBSIDIARIES AND OPERATING COMPANIES
Employee Biometric Data Protection Policy

Applicable to the United States and Canada

RPM International Inc. ("RPM") and its subsidiaries (collectively with RPM, the "Company") are committed to complying with all applicable Data Protection Laws. This Employee Biometric Data Protection Policy sets forth how, and the purposes for which, the Company collects, discloses, and uses Biometric Data, and the responsibilities and obligations of the Company and its authorized representatives with regard to such Biometric Data. Definitions for any defined terms are set forth in Section 9 below.

1. Scope and Disclaimer

1.1. This Biometric Data Protection Policy applies to current and former (full or part-time) employees of the Company. The Company may amend this Employee Biometric Data Protection Policy from time to time and will provide notice of such amendments, as appropriate or required by law. Biometric Data is considered Personal Information in the event of conflict between this Employee Biometric Data Protection Policy and the Employee Data Privacy Policy, the provisions set forth in this Employee Biometric Data Protection Policy shall supersede and control with respect to such conflict.

1.2. This Employee Biometric Data Protection Policy does not form, in full or in part, any contract of employment or other agreement to provide services, and nothing herein shall be construed to terminate, supersede, or modify the status of the employment between the Company and any other individual, pursuant to which the Company may terminate the employment at any time, with or without cause, and with or without notice.

2. Biometric Data: Purpose of Collection, Company Policy, and Procedures

2.1. The Company may collect and use Biometric Data from a Covered Individual for the following purposes: (i) performing wellness and health screening functions; (ii) implementing or enforcing timekeeping, access controls, security measures, or other Company policies; (iii) maintaining Company records, (iv) providing litigation or other legal, regulatory, or compliance related support, or (v) completing a financial transaction requested or authorized by the Covered Individual, or his/her legally authorized representative. For the avoidance of doubt, the Company has, in certain employment settings, implemented a time management system where employees and similar personnel may scan their finger each time they "clock-in" or "clock-out" from work, and this time management system works by converting a scan of an individual's finger to a numerical template using a proprietary mathematical algorithm, and this data is used for purposes of verifying employee identity and ensuring that all hours worked are accurately recorded.

2.2. The Company will not, at any time, sell, lease, trade, or otherwise profit from its collection and use of Biometric Data, or collect or retain Biometric Data for commercial purposes.

2.3. All Covered Individuals who furnish Biometric Data directly to any of the Company's equipment or devices (e.g., fingerprints, facial recognition) shall only do so in accordance with the guidelines, instructions, or rules applicable to the equipment or device.

2.4. All Company representatives who collect, use, or access Biometric Data from a Covered

Individual shall comply, at all times, with applicable Data Protection Laws and Company policies and procedures, including this Employee Biometric Data Protection Policy.

2.5. All Company representatives who collect, use, or access Biometric Data from a Covered Individual shall (i) maintain such Biometric Data under the strictest of confidence and in accordance with the restrictions set forth herein, (ii) protect the Biometric Data from any unlawful or unauthorized access, use, or disclosure, and (iii) limit access and use to Biometric Data to the minimum extent necessary and required to perform their authorized business or legal function. Without restricting or limiting any other provision set forth in this Employee Biometric Data Protection Policy, all Company representatives who collect, use, or access Biometric Data are hereby prohibited from the following: (iv) publicly displaying or posting Biometric Data, (v) requiring a Covered Individual to transmit Biometric Data over the internet without a secure connection or encryption, or (vi) selling or using the Biometric Data for any purpose unrelated to the Company's business operations.

2.6. Any Company representative who becomes aware of, or reasonably suspects, a breach of any aspect of this Employee Biometric Data Protection Policy, must immediately notify his/her supervisor or contact dataprotection@rpminc.com.

3. Sharing and Disclosure of Biometric Data

3.1. The Company may share Biometric Data related to a Covered Individual to any Company representative who has a need-to-know or who otherwise requires access to such Biometric Data in order to directly or indirectly satisfy or support a legitimate business interest of the Company that is set forth in Section 2.1 of this Employee Biometric Data Protection Policy.

3.2. The Company may share, disclose or otherwise disseminate Biometric Data related to a Covered Individual to any third-party service provider (e.g., software service providers) in order to assist in achieving the purpose for which such Biometric Data was collected. The Company will seek to undertake measures to ensure that any third-party to whom it discloses or otherwise disseminates Biometric Data is subject to contractual obligations pertaining to confidentiality and security.

3.3. The Company may share, disclose or otherwise disseminate Biometric Data related to a Covered Individual when required by federal or state law, or municipal ordinance, or pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

3.4. The Company is headquartered in the United States and has offices and locations in several countries and jurisdictions. The Company may, in its sole discretion, transfer, process, and retain Biometric Data related to a Covered Individual outside the jurisdiction in which it is collected, and in such circumstances, the relevant Biometric Data may be available to government authorities under lawful orders and laws applicable in such foreign jurisdictions. Depending on the jurisdiction in which a Covered Individual resides or where the Company conducts its business activities, additional cross-border notice requirements may be applicable, and Section 6 sets forth those additional requirements.

3.5. The Company may share, disclose or otherwise disseminate Personal Information (including Biometric Data) to a third party in connection with a sale or transfer of the Company's business or assets, an amalgamation, re-organization or financing of parts of the Company's business. However, in the event the transaction is completed, the Personal Information (including Biometric Data) will remain protected by applicable Data Protection Law. In the event the transaction is not completed, the Company will seek to require the other party not to use or disclose Personal Information (including Biometric Data) in any manner whatsoever and to completely delete such information.

3.6. Notwithstanding any other provision set forth herein, the Company may share, disclose or disseminate the Biometric Data related to a Covered Individual in accordance with the consent so furnished by the applicable Covered Individual, or his/her legally authorized representative, provided such disclosure or consent does not violate any Data Protection Law.

4. Security Measures

4.1. The Company will implement and maintain commercially reasonable security measures and use reasonable care to store, transmit, and safeguard any Biometric Data in its custody, control, or possession, and such measures and care shall be equivalent to or exceed the manner in which the Company stores, transmits, and protects its other confidential and sensitive information.

4.2. All Company representatives must, at all times, comply with the Company's information technology and data security policies and procedures. Unless otherwise granted approval in writing from the Company's senior management, or unless otherwise as part of their professional responsibilities, Company representatives are prohibited from seeking to degrade, evade, or circumvent the Company's data security measures.

5. Data Retention and Disposal

5.1. In the event the Company collects a Biometric Data from a Covered Individual, the Company shall retain such Biometric Data for no longer than one year following collection or as long as necessary to fulfill its purpose.

5.2. Notwithstanding Section 5.1, the Company may retain Biometric Data beyond the retention timeframe set forth in Section 5.1 in order to comply with an applicable law or regulation, or a valid warrant, subpoena, or order issued by a court of competent jurisdiction, or for the Company to establish, exercise, or defend against, legal claims (e.g., litigation holds), provided the Company retains such Biometric Data for the minimum time necessary in order to satisfy the same.

5.3. The Company will implement and maintain commercially reasonable protocols for permanently destroying, or disposing of, Biometric Data in a manner that will not compromise its confidentiality or integrity. Any Company representative responsible for destroying, or disposing of, Biometric Data (i) shall only destroy, or dispose of, such Biometric Data in a manner that complies with applicable Data Protection Law and renders such Biometric Data unreadable so as to remove any potential for its reuse or re-identification, and (ii) may procure a third party to assist with undertaking the same, provided the Company has executed a written agreement with the third party that sets forth the third party's obligations, responsibilities, and liabilities with respect to confidentiality and security.

6. Rights and Responsibilities

6.1. Depending on the jurisdiction in which a Covered Individual resides, or where the Company conducts business, the Covered Individual may be afforded additional notice of processing, or data privacy rights or privileges under applicable Data Protection Laws pertaining to Biometric Data. These rights are not absolute, and the Company may, when applicable and appropriate, refuse to undertake an action in response to a request made pursuant to any such Data Protection Law.

6.2 Covered Individuals in some jurisdictions may have a right to be informed of the collection of their Biometric Data and provide their consent prior to such collection. Covered Individuals residing

in Canada are informed that Personal Information collected from them may be available to government authorities under lawful orders and laws applicable in foreign jurisdictions. For more information regarding Canada's provincial and territorial privacy laws as well as who is responsible for their enforcement, please see the following: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/.

6.3. To the extent a Covered Individual provides the Company with Biometric Data, the Covered Individual must ensure, on a continuing basis, the accuracy, reliability, and relevancy of such Biometric Data, and only provide to the Company such Biometric Data in accordance and compliance with all applicable Data Protection Laws, including when applicable, in accordance with all data processing notice and consent requirements. Without limiting the foregoing, all Covered Individuals must, promptly and without delay, notify the Company (preferably in writing to dataprotection@rpminc.com) of any amendments that need to be made to their Biometric Data, or the Biometric Data concerning a third party that they provided the Company, to ensure its accuracy, reliability, and relevancy.

6.4. If a Covered Individual does not provide the Company with the Biometric Data identified herein, then the Company may not be able to satisfy its own contractual or legal obligations, and in such circumstances (and to the extent permitted by local law), the continued employment of the Covered Individual with the Company, or the professional relationship between the Covered Individual and the Company, may not be permissible or sustainable and all Covered Individuals acknowledge and agree that the Company shall not be held liable for any consequence directly resulting from these circumstances.

7. Enforcement

7.1. Failure to comply with this Employee Biometric Data Protection Policy may, in the Company's sole discretion, result in disciplinary action, including termination of employment.

7.2. The Company's decision to not enforce any aspect of this Employee Biometric Data Protection Policy, at any given time, shall not be construed, and is not the intent of the Company for such act or omission to be construed, as the withdrawal of any of the Company's legal or contractual rights or privileges, or the enforceability of this Employee Biometric Data Protection Policy.

8. Contact Information

8.1. Any questions, concerns, or comments related to this Employee Biometric Data Protection Policy should be directed to your supervisor, an HR representative, or to dataprotection@rpminc.com.

9. Definitions

For purposes of this Employee Biometric Data Protection Policy, the following definitions shall apply:

9.1. "Biometric Data" refers to a Biometric Identifier and/or Biometric Information.

9.2. "Biometric Identifier" means data generated by automatic measurements of an individual's biological characteristics (e.g., a retina or iris scan, fingerprint, voiceprint, record or scan of hand or face geometry) or any other unique biological patterns or characteristics that are used to identify a specific individual. Unless otherwise provided by an applicable Data Protection Law, the term

"Biometric Identifiers" does not include writing samples; written signatures; photographs; human biological samples used for valid scientific testing or screening; demographic data; physical descriptions (e.g., height, weight, hair color, or eye color).

9.3. "Biometric Information" means any information provided to the Company, regardless of how it is captured, converted, stored, or shared, based on any Biometric Identifier that is used, or that can be used, to identify an individual.

9.4. "Covered Individual" means any person who provides the Company with Biometric Data or about whom the Company collects Biometric Data, and who may include a Company employee or temporary worker, or any other person who visits a Company office, worksite, or other location that is collects Biometric Data from such visitors.

9.5. "Data Protection Law" refers to 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 Biometric Data.

9.6. "Personal Information" refers to any information, or a combination of pieces of information, that can reasonably identify an individual, and that is subject to, or otherwise afforded protection under, an applicable Data Protection Law and includes Biometric Information.