Last updated November 2, 2022

DATA SUBJECT REQUEST POLICY

A request or an inquiry from a person that involves the collection, use, handling or storage of information that directly or indirectly identifies them or links information to them ("Personal Data") is called a Data Subject Request ("DSR"). Personal Data includes non-private data like the individual's name and email address, as well as more sensitive information like health records, government identification and financial data. The individual making the request is called the Data Subject. A DSR may include a request to modify, access, restrict the use of, delete; or an instruction not to sell or share Personal Data. DSRs may come from current or former employees, customers, consumers or other individuals.

Purpose

The purpose of this Policy is to create a compliant and consistent response to DSRs.

Scope

All employees of RPM companies are required to follow this Policy when receiving or responding to a DSR. The following are not considered DSRs for purposes of this Policy: subpoenas, discovery requests or routine or general updates to existing contact information including revisions to someone's name or address updates, and updates to someone's benefits or financial information.

Policy

In the event you receive a DSR you must promptly forward the Data Subject's name, address, email and details of the request to your group's designated DSR contact (listed below) and copy the RPM Legal and Compliance department at dataprotection@rpminc.com. Also include your contact information and the date the request was received. The group DSR Contact will maintain an inventory ("DSR Log") of all DSRs received by companies within the respective group. Your DSR contact will assist you with the process described in this Policy.

DSR Contact by Group		
Group	**Contact Name**	**Email Address**
RPM HQ	Jessica Medvec	jmedvec@rpminc.com
Consumer Group	Lisa Brown	Lisa.Brown@rustoleum.com
Performance Coatings Group	Liz Merritt	lmerritt@rpmpcg.com
Construction Products Group	Justin Ray	jray@tremcoinc.com
Specialty Products Group	Sara Johnson	sjohnson@rpmspg.com

Prior to processing any DSR, the identity and place of residency (country and state) of the Data Subject must be verified, unless the identity and residency of the Data Subject is already known to you and verifiable, e.g., if you are in HR and the request comes from an employee you know and can verify. You will coordinate with your applicable group DSR Contact to complete the identity verification process. The attached template verification response (Attachment A) shall be used in verifying the Data Subject's identity.

If the data subject does not respond to the identity verification within thirty (30) days of the request, the DSR will be invalidated, and a formal notice must be sent to the data subject informing them the matter is being closed. You will coordinate with your applicable group

DSR Contact to coordinate the distribution of the formal notice of closure. The attached template (Attachment B) shall be used as a response for failure to verify identity. If the individual provides verification after the original request is closed, the DSR will be considered verified and reopened. All DSRs must be responded to in the same format they are received, unless otherwise requested.

Response Timelines
The legal timelines for responding will vary depending on the residency of the Data Subject and the type of request. In most instances this will require sending the initial identity verification response within ten (10) days of receiving the request. All responses received which verify the identity of the data subject must be submitted to the RPM Legal and Compliance department at dataprotection@rpminc.com for review within two (2) business days of receipt of receiving the verification.

Complying with a DSR
No DSR is to be completed without coordination with your group's DSR Contact and the RPM Legal and Compliance Department. After you forward the verification of identity, the RPM Legal and Compliance department will review the information provided and prepare a response plan based on an analysis of the request, the identity verification, and the applicable law. As part of this process, you and/or your group's DSR Contact may be asked to assist the Legal and Compliance department in facilitating the identification or removal of Personal Data and to ensure responses are provided to the Data Subject in a timely manner.

Group DSR Log
The DSR Contact for each group will maintain a log of all DSRs received by each entity within their group and the log shall be made available at the request of internal audit or the legal department. The group DSR log must be submitted to RPM Legal and Compliance, at dataprotection@rpminc.com, on an annual basis, no later than January 5th of each calendar year, beginning January 2024.

Data Retention
All correspondence with the Data Subject must be kept in a secure location by the company that received the request for a period of two (2) years after the matter is closed. Any questions related to the retention of a DSR record may be directed to the RPM Legal and Compliance department at dataprotection@rpminc.com.

Report Suspected Violations
A suspected violation of this policy can be reported to your immediate supervisor, Human Resources, the Company's Hotline or the Legal & Compliance department. For more information, refer to RPM's Hotline and Non-Retaliation Policy. Any employee who violates this Policy, including the failure to report a Policy violation, directs or who knowingly permits a subordinate to violate a Policy, or who engages in retaliatory actions may be subject to disciplinary action up to and including termination.