DPIA Policy

Purpose

The purpose of this Policy is to define when employees must complete a DPIA (Data Protection Impact Assessment), related to the implementation of any new or updated activity that may involve data about identified or identifiable people ("Personal Data"). Examples of these activities may include changes to or the implementation of internal processes, procedures, software, SaaS, the engagement of a new service provider, development of a new website or other projects that involve collecting, storing, transferring or any use of Personal Data (each a "Processing Activity"). Processing Activities that involve Personal Data trigger data privacy considerations and therefore require evaluation of any associated risks through a DPIA.

Policy

If a new or updated Processing Activity involves or has the potential to involve Personal Data, you must request and complete a DPIA and submit it for review to the RPM Legal and Compliance department, prior to moving forward with the Processing Activity. All technology-based solutions must also be subjected to a general security review and a vulnerability assessment. All security reviews and assessments can be requested by emailing the RPM Corporate Issue Log at issuelog@rpminc.com.

Scope

This Policy applies to all employees responsible for assessing, evaluating or procuring any new or updated Processing Activity.

Procedure

New Request

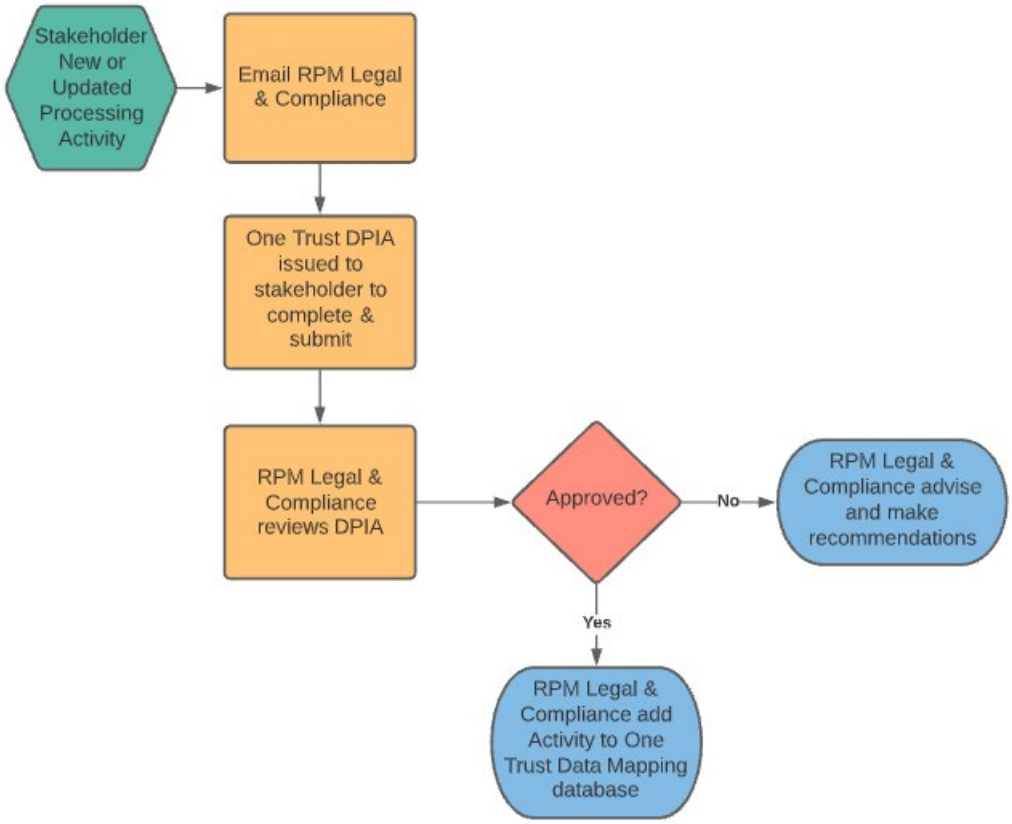
When a new or updated Processing Activity is identified as a target for implementation within the Company, promptly request a DPIA from the RPM Legal and Compliance department by emailing dataprotection@rpminc.com. You will receive a DPIA questionnaire from One Trust to fill out and submit for review by the RPM Legal and Compliance department.
If there is a material change or update to the Processing Activity thereafter, a new DPIA must be requested and submitted for review by the RPM Legal and Compliance department.

Review Process

The RPM Legal and Compliance department will assist with the completion of the DPIA as needed and provide recommendations related to mitigating any Personal Data risks identified as a result of the DPIA analysis. If the DPIA review process identifies significant issues or risks related to how the Processing Activity will use Personal Data, the RPM Legal and Compliance department will issue recommendations.

Following the completion and approval of the DPIA, the RPM Legal and Compliance department will collaborate with you to add the Processing Activity to the One Trust central data mapping inventory system.

To assist in illustrating the process, please refer to the general process workflow diagram below.



How to Report Suspected Violation

A suspected violation of this policy can be reported to your immediate supervisor, Human Resources, or the Legal & Compliance department. Employees are also welcome to contact the Company's Hotline to report their concerns to RPM. Allegations will be investigated thoroughly and objectively. 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.