RPM International Inc.
Privacy by Design Guidelines

1. Introduction

RPM's *Global Data Protection Policy* (RPMGlobalDataPrivacy.rpminc.com) requires RPM and each of its subsidiaries (each with or without RPM or each individually, as applicable, a "Company") to adopt an approach of "**Privacy by Design.**" Privacy by Design means that any new system, tool or functionality which will use Personal Data (as defined in the Global Data Protection Policy) should be built in a way which:

- takes into account the privacy rights of individuals; and
- allows the Company to comply with the Data Protection Principles, as set out in RPM's *Global Data Protection Policy* (RPMGlobalDataPrivacy.rpminc.com).

Privacy by Design means ensuring that, from the outset, considerations of privacy are built into every new system; for example in terms of what data is collected, for how long it is kept, how it is stored, security measures applicable to it and who can access it. Without Privacy by Design, the Company is at risk of not being able to comply with its obligations under data protection laws.

2. Compliance with these Guidelines

These Guidelines apply to all new or changes to existing systems, tools or functionalities (whether internally or from a third party) which involve the processing of Personal Data (each a "Change")).

When designing, developing or commissioning a Change consider each of the requirements of Privacy by Design which are set out in Section 3 below. Not all of the requirements will be applicable to every Change.

Where any Change is identified as likely to result in a **high risk** to the rights and freedoms of individuals, the Company will also need to conduct a *Data Protection Impact Assessment* (**DPIA**) before the project can continue. RPM's *DPIA Guidelines* (RPMImpactAssessmentGuide.rpminc.com) provide guidance on when any processing activity may be considered high risk and how to conduct a DPIA.

The DPIA may identify more specific Privacy by Design requirements which the project will need to address in order to mitigate against identified risks. For more information, consult the *DPIA Guidelines* (RPMImpactAssessmentGuide.rpminc.com).

3. Privacy by Design Analysis

Document the following (see Annex 1 Privacy by Design checklist):

Purpose(s)

a) Identify the purpose(s) of the Change, i.e. what is the Change for? What is it designed to do? This is the most important requirement, as it will help you to satisfy all the other requirements on the list. You should have a very clear idea about the specific purpose(s) of any new Change.

Data Collection and Usage

b) Identify what Personal Data will be collected as a result of the Change. The Change should be designed to hold only the minimum amount of Personal Data necessary to achieve the purpose you identified in paragraph a) above. If the purpose can be achieved without knowing the individual's name, email, or physical address, for example, do not collect or use this information.

c) If the Change will result in the processing any Sensitive Personal Data, banking data, credit card data, individually assigned identification number, location data, or information about children, the privacy considerations are particularly important. Only hold this information if you absolutely need it for the purpose in paragraph a) above, and make sure it is not used for any other purpose. When you collect this kind of data you will also need to conduct a DPIA for the Change.

d) Where applicable, you should distinguish between mandatory and optional fields. If the Personal Data collected would be *helpful* for the purpose, but is not strictly necessary, you should make the provision of it optional (and make this clear to the individual). Consider whether you really need the optional data to achieve the purpose you identified in paragraph a) above.

e) Where applicable, free text fields should not be used as these increase risk of collecting data which the Company may not need or that is harder to anonymise. Wherever possible, you should instead provide tick-boxes or drop-down options.

f) If possible, records should contain a unique identifier (e.g. a customer or employee ID). This makes records easier to anonymise, share and analyse without disclosing someone's name. However, you should not use government-issued identifiers such as a passport, National Insurance or Social Security number (unless this is necessary for the purpose).

Access and Data Quality

g) Consider who within the Company needs to access the Personal Data. Only staff with a need to access the Personal Data for a legitimate purpose should be able to do so. If not everyone needs access to the same Personal Data and/or to the entirety of the Personal Data set, design the Change so that access privileges can be segmented and/or tiered.

h) Design the Change so that the Personal Data can be edited or deleted as appropriate.

i) Of those staff with a need to access the Personal Data, consider who needs to be able to edit and/or delete it, and/or download it to their own machine. If this is a smaller group of people than those who only need *access*, restrict the "edit/delete" permissions accordingly. Decide from the outset who will have the right to grant and remove access rights.

j) If possible, the Change should allow self-service (with appropriate authentication) so that individuals can unsubscribe to a mailing or view, amend, update and delete the Personal Data they have provided, for example, by changing an address. If it is not appropriate to offer a self-service mechanism, it should be easy to generate a report that captures all information about a known individual.

k) The Change should keep a log of when a record was created and/or last updated. For example, the appropriate staff should be able to identify that a record was created five years ago, but that a new mobile number was added two years ago.

Retention and Deletion

l) Consider whether you need to store the Personal Data *at all*, or if it can be immediately deleted once the process is complete. For example, on a website does the information need to be kept after the customer has finished browsing?

m) Personal Data should only be kept for as long as is necessary for the purpose you identified above. Some Personal Data in the Change may be needed for longer than others, so you might need to set different periods for different categories of Personal Data. You should refer to the *Personal Data Retention Guidelines* provided by your company's or RPM's legal department for more guidance on Personal Data retention.

n) If possible, the Change should be configured to automatically delete Personal Data at the end of the retention period. However, make sure the auto-deletion can be suspended if necessary, for example if Personal Data has to be retained for longer periods due to litigation.

o) If, after a certain period, you only need the Personal Data in anonymous form, all the identifiers should be removed. This includes the name, email address, date of birth, and any identifiers which are used across systems.

p) If the Change relates to customer accounts, consider implementing a suspension or closure policy after a period of inactivity.

Security and Suppliers

q) Assess the security protections for the Personal Data, and whether they are appropriate in view of the nature of the Personal Data. Wherever possible and appropriate, use encryption techniques to protect the Personal Data, in transit and/or at rest.

r) If you are using a third party provider, conduct due diligence to confirm that they are a reliable supplier. Is there a contract in place? Do they have any security accreditations?

s) If you are using a SaaS provider, check whether the functionality of the service allows you to meet the other requirements in this checklist. For example, does it allow you to delete the Personal Data? What happens on termination?

Questions regarding these Guidelines can be directed to Dataprotection@rpminc.com or to your company's or RPM's legal department.

ANNEX 1: Privacy by Design Checklist

This checklist is designed to help ensure that due regard is given to Privacy by Design considerations as part of a Change.

No.	Privacy by Design Consideration	Has this been considered and, if applicable, addressed as part of the Change design?
a)	The purpose of the Change	☐
b)	The Personal Data which is needed	☐
c)	Any Sensitive Personal Data, data about children, or location data	☐
d)	Mandatory or optional Personal Data	☐
e)	Free text fields	☐
f)	Unique identifiers	☐
g)	Access rights for RPM Employees	☐
h)	Editing/deletion of the Personal Data	☐
i)	Editing/deletion rights for RPM Employees	☐
j)	Self-service mechanisms	☐
k)	Creation and edit log files	☐
l)	Store or immediate deletion	☐
m)	Retention Periods	☐
n)	Automatic deletion	☐
o)	Anonymisation	☐
p)	Automatic suspension for non-activity	☐
q)	Security protections	☐
r)	Third party providers	☐
s)	SaaS providers	☐
t)	Data Protection Impact Assessment	☐