Employee Guidelines for Data Protection Impact Assessments

1. Introduction

RPM and each of our subsidiaries (whether together or individually, each a "Company") is committed to protecting the Personal Data (as defined in the Global Data Protection Policy) of our employees, customers and business contacts, and in line with this we have adopted the data protection principles set out in our *Global Data Protection Policy* (RPMGlobalDataPrivacy.rpminc.com).

WHY a DPIA? In order to comply with the principle of "Accountability" under our Global Data Protection Policy, the Company is required to conduct a "Data Protection Impact Assessment" (also known as a "DPIA") where there are likely to be high risks associated with any new processing of Personal Data.

These Guidelines set out triggers for when you will need to discuss a new project with your Data Protection Champion (DPC). Also in the event of any uncertainties, please seek the advice of your Data Protection Champion. It will then be for the Data Protection Champion to decide whether a full DPIA is necessary.

2. What is a Data Protection Impact Assessment, or "DPIA"?

A DPIA is an assessment of the impact on individuals of the processing of their Personal Data. Conducting a DPIA enables the Company to decide whether it is justified in conducting a particular data processing activity, and to determine how to do it in the most 'privacy friendly' manner.

The DPIA works by requiring the Company to identify the benefits of a proposed project, the possible privacy and data protection risks, and any safeguards which can be put in place to mitigate those risks. Whoever is conducting the DPIA can then decide whether the project can go ahead, or whether any further mitigation steps are needed.

You should be able to identify when a DPIA is required and you may have the responsibility to assist with a DPIA if asked to do so by your Data Protection Champion. In particular, the Data Protection Champion will need to know all relevant details of the project, including the business case and proposed technology.

3. Is the processing of Personal Data potentially high risk?

A DPIA is necessary where any processing of Personal Data **is likely** to result in a '**high risk**' to the rights and freedoms of individuals. Therefore, at the outset of any new project or processing activity involving Personal Data, you must consider whether the project has the potential to involve 'high risk' processing.

Any new processing which has the potential to be high risk should be referred to your Data Protection Champion. The Data Protection Champion will then decide whether to conduct a full DPIA.

The Company deems the processing activities referred to below as potentially high risk. All such activities (and similar/equivalent activities) should be referred to your Data Protection

Champion. Please note that these are examples of "risk triggers" and are not intended to provide an exhaustive list. You are expected to use your judgment in considering whether any new processing has the potential to be high risk. As a general rule, any substantial new use of Personal Data has the potential to be high risk. In the event of uncertainties, Employees should consult with the Data Protection Champion.

If you consider that the new processing might be high risk, you should complete Step (1) of the form in the Appendix to these guidelines and submit it to your Data Protection Champion.

Processing Activity	**Examples**
Sharing a significant amount of Personal Data with a third party, including service providers	– Appointing a supplier of a new HR system, who will intentionally or de facto have access to Employment Data
Collection of a new type of Personal Data	– Collecting photographs in connection with the roll-out of a new internal instant messaging service
Collection of a new type of Sensitive Personal Data (or Highly Confidential Sensitive Data), or using Sensitive Personal Data (or Highly Confidential Sensitive Data) for a new purpose "**Sensitive Personal Data**" is Personal Data relating to: - racial or ethnic origin - political opinions - religious or philosophical beliefs - trade union membership - biometrics - genetic information - mental/physical health - sex life or sexual orientation "**Highly Confidential Sensitive Data**" is Personal Data relating to: - bank accounts - credit card accounts - personal identifications numbers such as Social Security Numbers	– Collecting Employee health data in connection with a new corporate healthcare insurance offering – Collecting fingerprints for a new building security system
Using Personal Data for a new purpose	– Using data collected from attendees at a RPM event for analytics purposes, or sharing the data with third parties
Using Personal Data to make a decision about someone on an automated basis (even if there is a human review)	– Using an automated programme to assess CVs in recruitment – Scoring system for customer's liquidity

New collection or use of location data	– Adding location tracking to an app used on Employee devices
Sharing Sensitive Personal Data (or Highly Confidential Sensitive Data) with a third party	– Appointing a third party service provider who will have access to Employee occupational health data or financial data
Conducting monitoring of individuals	– Adopting a new CCTV system – Monitoring Employee use of an IT system (e.g. keylogger software, email monitoring, drug testing)
Combining datasets previously maintained separately	– Combining business contact data collected from customers in different countries for the first time
Transferring Personal Data overseas, other than as part of an existing processing arrangement already in place	– Appointing a US service provider (e.g. a cloud provider or offshore call centre), server location needs to be considered??
Data processed on a large scale	– Appointing a new supplier who will have access to all RPM Employment Data worldwide Where is the threshold, does this also applies for global data of operating group or company?
Innovative use of Personal Data or applying technological or organisational solutions	– Combining the use of fingerprint and facial recognition for improved physical access control
Processing preventing individuals from exercising a right or using a service or a contract	– A project which ranks Employees in order of performance but which does not allow the Employees to access that information – Workplace related complaints that are kept confidential from the individual about whom the complaint has been made

Again, if you are still not sure, you should speak to your Data Protection Champion. They may need to conduct their own assessment, or they may be able to tell you immediately whether the proposal has the potential to be high risk.

The following are examples of processing which is unlikely to be high risk, and in the absence of special circumstances would not require a DPIA:

– ‘Business as usual’ processing which the Company has been engaged in for several years, such as recording visitors to Company premises, provided there is no material change in the processing.

- A cosmetic design change to an internal IT system that changes the order in which data is collected, but not the type of data collected; for example, changing look and feel of an existing online employee portal.
- Ad hoc processing of a small amount of Personal Data in response to a specific request by an individual (e.g. in the context of a customer query).
- Disclosure or other processing of employees' business contact details.

Questions regarding these Guidelines can be directed to your company's Chief Compliance Officer.

Last updated May 2018

Appendix: DPIA Template
DATA PROTECTION IMPACT ASSESSMENT

Please review the RPM Guidelines for Data Protection Impact Assessments and in particular section 5 (Conducting the DPIA), before you complete this form.

PROJECT NAME:

PROJECT MANAGER:

PROJECT DESCRIPTION AND GOALS:

RESPONSIBLE COMPLIANCE LIAISON:

DATE DPIA COMPLETED:

STEP (1): A DESCRIPTION OF THE PROCESSING	
Nature of the Personal Data	
Identity and approximate quantity of Data Subjects	
Nature of the processing	
Purpose and business objectives of the processing	
Identity and location of the parties	
How is it stored (on which system(s))?	

How long is it planned to be stored?	
Other information	
STEP (2): WHY IS THERE A NEED FOR A DPIA?	
STEP (3): WHAT IS THE LEGAL BASIS FOR THE PROCESSING?	
STEP (4): WHAT ARE THE RISKS?	
Key Privacy Risks and impact on Data Subject	
Likelihood and severity of any resulting harm	
Commercial or Legal risks to RPM	

STEP (5): SAFEGUARDS		
Risk	**Proposed Safeguard / actions**	**Do the proposed safeguards / actions eliminate or reduce the risk or is the risk accepted?**

STEP (6): ACTIONS	
Who is responsible for implementing proposed safeguards / actions?	**Deadline for implementing safeguards / actions**
STEP (7): IS IT NECESSARY AND PROPORTIONATE?	

[CONSULTATION WITH LEGAL AND/OR THE DATA PROTECTION AUTHORITY]			
[DELETE IF NOT APPLICABLE]			
APPROVAL OF DPIA			
Role	**Print Name**	**Signature**	**Date**
Project Manager			
Data Protection Champion			

Please provide a copy of the completed DPIA to the Chief Compliance Officer.