

# Data Protection Impact Assessment (DPIA) Procedure

Version number: 1.0

Publish date: 16-05-2018

Document control	
Prepared by	Mike Moore, Managing Director
Authorised by	Upper Management
Physical Copy location(s)	Operations Folder
Source Copy Location(s)	Dropbox - GDPR123\Documents\Final Documents
Published Copy Location(s)	www.Dephoto.biz\GDPR
Other Referenced Documents	
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Data Protection Impact Assessment (DPIA) Procedure			
Description	Helps to identify and reduce the privacy risks of a data processing undertaking.			
Created by	Mike Moore			
Date Created	16-05-2018			
Maintained by	Upper Management			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	Mike Moore	First creation	16-05-2018	Published

## Contents

Purpose .....	3
Prerequisites .....	3
Conditions .....	3
Outcomes.....	3
Processes .....	4
Mapping data flows sub-process .....	4
Identifying a risk sub-process .....	4
Consulting the Data Protection Officer.....	4
Reporting DPIA results if there are risks to data protection .....	4
Reporting risk assessment results if there are no risks to data protection .....	4
Management and Review.....	4

## Purpose

A Data Protection Impact Assessment (DPIA) is a process which helps DE Photo (Franchising) Ltd (referred to as the company here after) to identify and reduce the privacy risks of a data processing undertaking.

DPIA should be used throughout the development and implementation of a project, using existing project management processes. This allows DE Photo (Franchising) Ltd to analyse how a particular project or system will affect the privacy of the individuals involved.

Managing privacy effectively and in line with current guidance and best practice is an important means of enabling the effective use of information for all concerned and that information is managed safely in a secure manner and used for its intended purposes.

All new projects, procedures and policies that involve using or sharing personal information will require a completed Data Protection Impact Assessment at the initial stages and prior to any decision being made regarding processing or controlling of personal data.

## Prerequisites

For this procedure to be followed the following conditions need to be met:

- All parties need to be aware of their roles and responsibilities.
- Any systems/services/devices referenced need to be available to the relevant parties.
- All parties have had the relevant training and the training is current and up to date.
- Documented controls and measures are in place to allow swift reporting of incidents.

## Conditions

If the conditions below are met a DPIA should be performed:

- If a data process or set of processes presents a high risk to the rights and freedoms of the data subject.
- If a data process or set of processes makes use of new technologies.
- If a data process or set of processes makes use of large amounts of personal information.
- If a data process or set of processes involves sensitive information.

## Outcomes

DPIA report is completed

DPIA and outcome of the DPIA is logged and stored

## Processes

### Mapping data flows sub-process

1. Create a diagram to identify all of the systems that will be used to process data, and how the data will be transferred between them.
2. Mark on this chart what classifications of information will be processed and transferred.

### Identifying a risk sub-process

1. Using the diagram created in the Mapping Data Flows sub-process consider how the unauthorised parties could view the information.
2. Using the diagram created in the Mapping Data Flows sub-process consider how data integrity could be compromised.
3. Using the diagram created in the Mapping Data Flows sub-process consider how data could be rendered unavailable.
4. Use the identified risks to carry out a risk assessment (use the Risk Assessment Procedure to carry this out)

### Consulting the Data Protection Officer

1. Present the diagram and risk assessment to the Data Protection Officer for feedback.
2. Incorporate the Data Protection Officer's feedback into the risk assessment and data flow diagram.

### Reporting DPIA results if there are risks to data protection

1. The risk assessment and data flow diagram is saved to Dropbox: \GDPR123\Documents\File Locations\Data protection impact assessments to be actioned
2. The project owner and information security dept. is informed of the results via an encrypted email.

### Reporting risk assessment results if there are no risks to data protection

1. The risk assessment is saved to the location Dropbox: \GDPR123\Documents\File Locations\Data protection impact assessments
2. The project owner is informed of the results via an encrypted email.

## Management and Review

This policy should be reviewed as scheduled once annually unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16-05-2018

Next Review Date: 16-05-2019