Data Protection Impact Assessment Policy

1. Definitions

DPC	The nominated data protection champion for your team and/or department].
DPO	Data Protection Officer.
Personal Data	Information relating to an identified or identifiable individual.
Process or Processing	Any operation or set of operations which is performed on Personal Data, including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, combining, restricting, erasing and destroying.
Special Category Data	Information about an identifiable individual relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify a person, health data or data relating to sex life or sexual orientation.
Supervisory Authority	The data protection regulatory authority in the UK or a European Union Member State

2. Introduction

This Data Protection Impact Assessment Policy (**Policy**) explains MOPACs (referred to in this Policy as **we**, **us** or **our**) policy for carrying out Data Protection Impact Assessments (**DPIAs**) and Privacy Reviews. This Policy applies to all our employees, and contractors (referred to collectively in this Policy as **employees** or **you**).

The Policy explains what a DPIA and a Privacy Review is, when a DPIA or a Privacy Review should be undertaken and the resources available to help you complete a DPIA or Privacy Review. This Policy will help us ensure that DPIAs and Privacy Reviews are carried out as efficiently and effectively as possible in compliance with our legal obligations.

If you have any questions about this Policy, please raise them with your DPO.

3. What is a DPIA?

A DPIA is a documented assessment of the impact that a processing activity will have on individuals when we Process their Personal Data.

The purpose of a DPIA is to enable MOPAC to:

- identify the privacy risks that arise in connection with a proposed activity;
- carry out a check to ensure that the data processing is necessary and proportionate; and
- find and implement appropriate solutions to mitigate the risks identified.

A Privacy Review is a shorter form risk assessment that enables us to have oversight of all data processing activities and to ensure that all of our regulatory requirements are met when we process Personal Data. The DPIA Checklist will help you identify whether you need to complete a DPIA or a Privacy Review.

4. When is a DPIA required?

The General Data Protection Regulation (**GDPR**) requires MOPAC to carry out a DPIA for all new projects that involve Personal Data where the nature of the Processing poses a high risk to individuals. DPIAs must be completed **prior** to any Processing being carried out.

The GDPR specifies that the following types of Processing activities are considered high risk (but note that this is not an exhaustive list):

- profiling of individuals and making automated decisions which have a legal effect or another significant effect on the individual;
- processing Special Category Data on a large scale;
- processing criminal conviction data on a large scale; and
- systematically monitoring publicly accessible areas on a large scale.

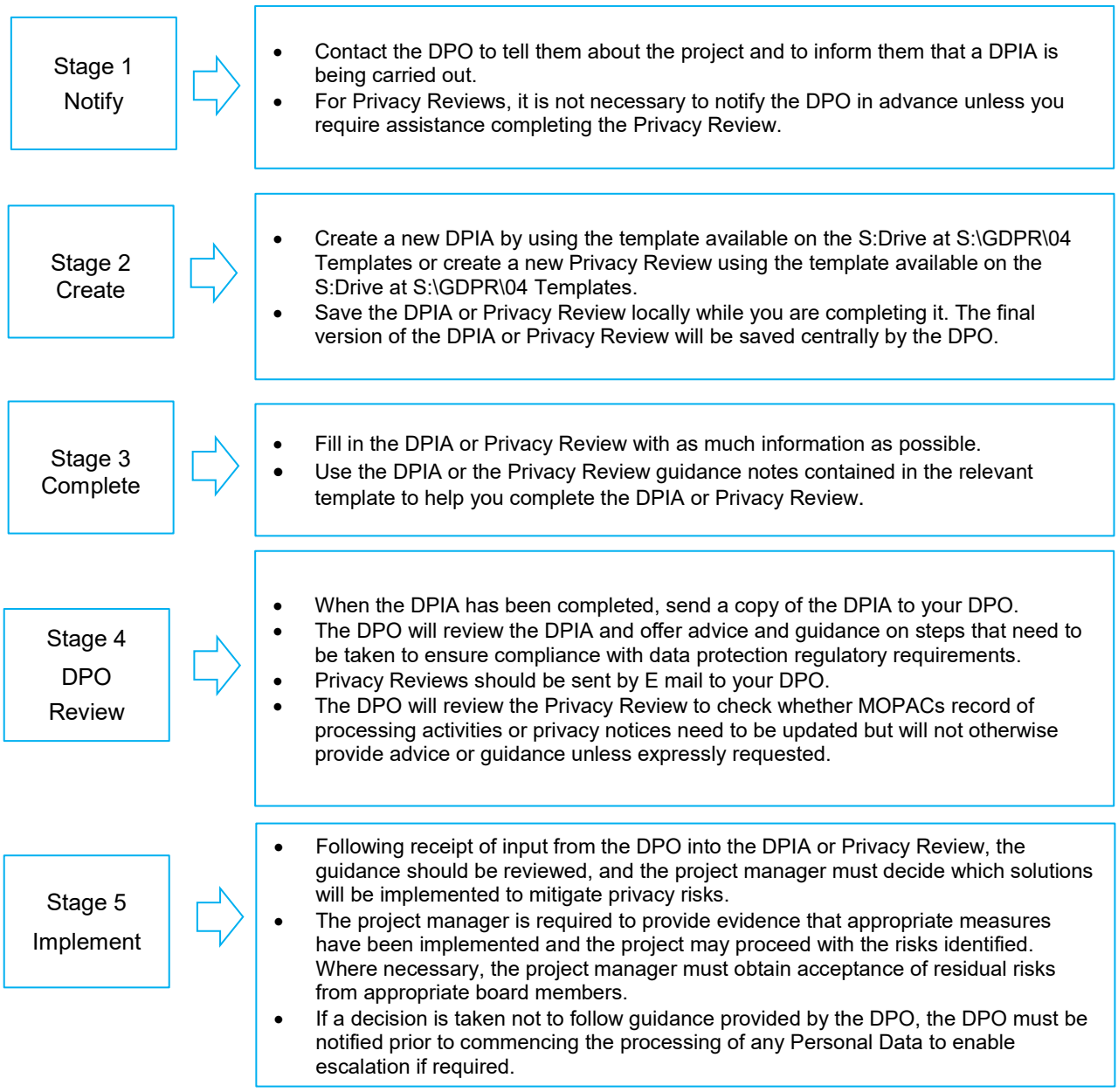
In addition, Supervisory Authorities in each European Union country are required to publish lists of data processing activities that are considered high risk and for which a DPIA must be carried out. For any new activity or project that involves Personal Data, you must check whether a DPIA is required before collecting any Personal Data or using Personal Data for a new purpose.

5. How do I know if a DPIA is required?

For all new projects involving Personal Data or where Personal Data is going to be used for a new purpose you must complete the DPIA Checklist to determine whether a DPIA is required. The DPIA Checklist is available on the S:Drive at S:\GDPR\04 Templates. If a DPIA is not required because the project is not high risk but the project does involve the Processing of Personal Data you must complete a Privacy Review instead of a DPIA.

6. How do I complete a DPIA or Privacy Review?

Once you have completed the DPIA Checklist to determine whether a DPIA or a Privacy Review is required, you need to take the following steps:



7. Who is responsible for completing the DPIA or Privacy Review?

The project manager and relevant process owners are jointly responsible for ensuring that the DPIA or Privacy Review is completed with input from relevant teams as required.

If a third-party is involved in the project (for example commissioned services), it may be appropriate to seek the third-party's input into the DPIA or Privacy Review. For example, if a service is being delivered by a third-party, the provider is likely to be best placed to provide information about the use and storage of data and its capability to delete or extract data etc.

8. Consultation requirements

If a DPIA identifies high risks that cannot be mitigated, MOPAC must consult with the relevant Supervisory Authority before proceeding with the data processing activity. The DPO is responsible for identifying where such consultation is required and will liaise with the relevant Supervisory Authority for guidance. If a project requires consultation with a Supervisory Authority, the project must not proceed until the consultation has been completed.

When DPIAs are carried out MOPAC also has a duty to consider whether it is appropriate to consult with affected individuals. The DPIA will prompt you to consider whether consultation is appropriate and the form that such consultation should take (if applicable). If you do not consider that it is necessary to consult with affected individuals, the reasons for this must be documented in the DPIA.

9. What happens if we do not complete a DPIA?

If we fail to carry out a DPIA when high risk processing is involved, this is a breach of the GDPR.

DPIAs and Privacy Reviews help us to identify and manage risks appropriately. They also help us ensure that our records of Processing are kept up to date and that our privacy notices adequately explain to individuals how we use and share their Personal Data. If we do not carry out and document DPIAs and Privacy Reviews we risk failing to comply with regulatory requirements. This could have serious implications for our customers or employees whose Personal Data we are Processing and could result in regulatory enforcement action, claims for compensation and reputational damage for MOPAC.

10. Policy updates

We will review this Policy and the associated documents periodically and will make any updates deemed necessary. You will be required to comply with any updates made from the date the updated policy is made available to employees.

Document version history

The following table details a record of the changes made to this document:

Version	Date	Author	Description of change
0.1	26/02/2020	James Bottomley	First draft
0.2			Second draft

Associated documents

- DPIA Checklist
- Privacy Review Template
- DPIA Template