Data Protection Impact Assessment Template:
Tinopolis Group

1. What is a DPIA?

A Data Protection Impact Assessment (**DPIA**) is a means of helping organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

A DPIA should not be a one-off exercise. It should be updated throughout the lifecycle of the project to ensure that data protection and privacy are considered.

2. When does a DPIA need to be carried out?

Whenever we intend to collect new types of personal data, carry out new processing activities or use existing personal data for new purposes, we should consider carrying out a DPIA. Ideally, the DPIA should be carried out prior to the processing and as early as is practicable in the design of the project.

Carrying out a DPIA is not mandatory on every occasion. The General Data Protection Regulation (**GDPR**) requires organisations to carry out a DPIA in certain circumstances, including where the processing is likely to result in a high risk to the rights and freedoms of individuals. "High risk" is not defined but this template is designed to help employees to identify when a particular project is likely to result in a high risk to individuals' rights and freedoms.

For more information about DPIAs, please contact the Data Protection Manager (Sara Bond).

3. Why carry out a DPIA?

The purpose of a DPIA is to identify privacy risks and allow us to mitigate or eliminate those risks at the outset of a project.

When a DPIA indicates that processing would result in a high risk to data subjects, the employee must notify the Data Protection Manager who in consultation with the Group Finance Director (Jennifer Roberts) shall consult with the ICO. Failure to comply with the DPIA requirements will constitute a breach of the GDPR and could lead to regulatory action against the Group, including fines.

Where a Group company is acting as a Data Controller, it is responsible for ensuring that the DPIA is carried out where required.

4. How to use this template

Step 1 of the template is designed for you to identify whether a DPIA is required. The screening questions should assist you in determining whether or not a DPIA is required. If you have any questions, please contact the Data Protection Manager.

Once you have determined that a DPIA is necessary, the DPIA process follows a logical sequence:

- Step 2 requires you to identify the data flows and any potential consultees.
- Steps 3 and 4 require you to identify privacy risks and potential solutions.
- Steps 5 and 6 require you to record actions and who is accountable for them.

Finally, the DPIA should be kept under review for the duration of the project and, if anything changes, should be updated accordingly.

Step 1: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the Group company, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project - for example, a project proposal. Also, summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Overview of the project:

Benefits of the project:

Reason why a DPIA is required:

[Processing is high risk because [•].]

Consider the DPIA screening questions:

1. Will the project involve the collection of new information about individuals?
2. Will the project compel individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
8. Will the project require you to contact individuals in ways which they may find intrusive?

Step 2: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Provide a description of the processing.

Set out the nature, scope, context and purposes of the processing.

Set out the personal data, recipients of the personal data and period for which the personal data will be stored.

Identify the assets (hardware, software, networks, people, paper, paper transmission channels,

mobile devices, cookies, clouds, data warehouses, etc.) on which personal data rely.

Assess the necessity and proportionality of the processing in relation to the purpose of the processing.

Questions to consider:

- How is the personal data collected? Who is collecting it?
- Who will receive / have access to the data?
- How will the data be shared / transmitted?
- What security will be in place to protect the data at transmission?
- Why is the data being collected?
- How will the data be used?
- How long will it be kept?
- What governance arrangements are in place to ensure it is kept securely?

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Consider the following consultees:

- Internal consultation
- Consultation within the industry
- Do you need to consult with government and/or the regulator on these proposals?
- Are there any consumer bodies that could be consulted?

How will you consult?

What feedback have you received?

Explain how views will be sought and, if they will not be, set out the justification for not seeking input from data subjects (for example, compromises confidentiality of business plans; disproportionate; impractical)

Step 3: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks.

Consider the origin, nature, particularity and severity of risks and consider each risk (such as illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects.

Privacy issue	Risk to individuals	Compliance risk	Organisation/corporate risk

Step 4: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result** (e.g. risk eliminated / reduced / accepted)	**Evaluation** (is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)

Step 5: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	**Approved solution**	**Approved by**

Step 6: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action	**Date for completion**	**Responsibility**

Contact point for future privacy concerns