Completion of Data Protection Impact Assessments Guidance

Version Control

1. Full Document Number:	OPEGUI002
2. Version number:	2.0
3. Superseded version number:	1.1
4. Document owner job title:	Data Protection Officer
5. Department / function:	Strategic Operations
6. Next review date:	01-APR-2021
7. Add document to external LSTM website?	Yes

This document is uncontrolled if downloaded or printed. Always view the current version of the document via the Knowledge Exchange Policy Hub. Approved documents are valid for use after their approval date.

Modifications from previous version of document

Version	Date of issue	Details of modification
0.9	30/04/2019	DPO first draft
1.0	29/05/2019	Inclusion of risk template document
1.1	05/06/2019	Added info on risk scoring
2.0	09/03/2021	Inclusion of Word template, updated guidance, change to approval step

Contents

1 Scope

This guidance applies to all staff managing projects sharing data with other organisations or that could involve high risk processing.

Introduction and Context

Data Protection Impact Assessments (DPIA) are best practice for any public sector data sharing under the ICO's Data Sharing Code of Practice and are mandatory for any high-risk processing under the Data Protection Act 2018. A DPIA must therefore be done when designing or modifying a process that involves personal data that poses a high risk to data subject rights. Guidance on what constitutes high risk has been built into the screening questions in LSTM's DPIA OnTrack tool.

What is a DPIA?

A DPIA should be a positive and informative way of considering data protection risks where LSTM is controller. Completing a DPIA helps build "Privacy by Design and Default" and demonstrate accountability, which are important aspects of data protection law. It is separate from project risk assessments or other kinds of impact assessment.

The online workflow or alternative Word template should be started, advice of the DPO sought and addressed, and a finalised DPIA approved by the project's risk owner (for example the Principal Investigator) before work commences. This ensures that when processing begins it gives proportionate protection to data subjects. DPIAs should be regularly reviewed at least annually. You should update the DPIA whenever the assessed risks change. The sharing of summary findings or conclusions from your DPIA is encouraged, for example in your project's privacy notice.

How to start a DPIA

Follow the tool via OnTrack to start a DPIA, or use this Word template:

Word template
DPIAT-.docx

Answer each question based on your current understanding. The tool will walk you through all steps of the process that relate to your answers. Information on what is expected in each field is included below (the same information is also accessible via the 'I' buttons in OnTrack). The OnTrack DPIA process will result in a Microsoft Word document to which further additions, comments and edits will be made.

Further work on the DPIA could also include engagement with people regarding their preferences for how their data should be managed

The Data Protection Policy and GDPR FAQs may be useful reference points. There is also European best practice guidance about DPIAs on which the process and remainder of this document is based. University College London have a similar DPIA process with screening questions followed by a full assessment – read their guidance here.

If you require any further assistance, please contact the Data Protection Officer dataprotection@lstmed.ac.uk / (+44) 0151 702 9323

Step by step guidance from OnTrack

PROJECT DETAILS

Name of project - A project here is a defined piece of work where personal data are processed. The project name could be the title of a grant application.

Other identifiers for your project - This information is for those supporting you with this DPIA to refer to information already held by LSTM. Shorthand names can be as helpful as numbers on administrative systems. Useful codes could include: abbreviation, RBPS number, ROC number, G&E number, DMPOnline reference number. If your project is at a very early stage and does not have any associated codes please enter 'no'.

Department – the department responsible for the project.

Who has oversight of your project? - A senior member of LSTM staff who has responsibility for the proposed work. This box should contain the name of a manager (if not yourself) who is responsible for the project risks and who will approve the completed DPIA. For example, your line manager, the principal investigator, or your head of department.

DATA FLOWS

Please describe your project and its data - Describe what data your project involves. Wherever applicable please describe how these data will be collected, received, processed, and sent. Important details here are which organisations (legal entities) are involved, which organisation controls the flow of data, the countries where the data will be, and what work each organisation will be doing.

What benefits do you anticipate from this project? - The measures put in place to protect personal data need to be proportional to the risks and to the benefits that will hopefully arise. These benefits could be in terms of advancement of knowledge, service efficiency, public health, finances, etc. If you are doing a DPIA for an existing project that you are making changes to please describe the benefits that will arise from the changes.

What organisation(s) is/are receiving data?

What organisation(s) is/are sending data? - Some organisations might send and receive data. If so, please enter them in both the receiving and sending boxes.

What role does LSTM fulfil in this project? - LSTM's obligations and liabilities depend on its role in a project. Select as many options as apply to your project.

If you have an information or data flow diagram, please upload here - It can be helpful to sketch out exactly what data is being sent when, where and by whom. If you have produced such a diagram please upload it. Scanned images of handdrawn diagrams are acceptable.

ASSESSMENT SCREENING QUESTIONS

The following screening questions have been produced using the latest guidance to ascertain whether we need to complete a DPIA. Please answer accurately and to the best of your knowledge.

If you are in any doubt as to whether to select yes/no you can see examples by clicking the 'i' button. If you are still unsure please contact the Data Protection Officer.

Will your project process data about identifiable individuals to do any type of activity in?

Table 1 Types of personal data processing that may pose a high risk, with examples of how they might relate to work at LSTM. The examples listed are not exhaustive.

Processing activity	**Examples**
Evaluation or scoring	Assessing people's performance/health/interests/behaviour, e.g. risk prediction modelling, surveying student opinions, or staff activity tracking.
Automated decision-making with significant effects	Any automated algorithm that may discriminate between people or exclude certain groups e.g. machine learning in online assessments or applying artificial intelligence to triage medical complaints.
Systematic monitoring	Efforts to observe, monitor or control data subjects, e.g. linking data from different health providers, surveillance of entrants to buildings, or deploying drones over a study area.
Processing of new, special, or highly personal data	Genetic data, biometric data, mental or physical health records, criminal records, fine scale or real-time location data, or information about private activities such as household communications.
Processing on a large scale	Defined by the number of data subjects, volume of data, duration of processing activity, and geographical extent, e.g. national public health surveillance or wrangling big datasets. European guidance gives examples of large scale processing:

	• "processing of patient data in the regular course of business by a hospital • processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards) • processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities • processing of customer data in the regular course of business by an insurance company or a bank • processing of personal data for behavioural advertising by a search engine • processing of data (content, traffic, location) by telephone or internet service providers" Examples that do not constitute large-scale processing include: • processing of patient data by an individual physician • processing of personal data relating to criminal convictions and offences by an individual lawyer"
Processing of data concerning vulnerable data subjects	Any group where LSTM is in a more powerful position including as an employer or donor, e.g. towards children, patients, refugees, students or employees.
Innovative technological or organisational solutions	A new app, improved diagnostic tool, integrated computer systems, fingerprint access control, or Internet of Things trial.
Data sharing with a new organisation	A new IT system supplier, new research collaboration, or a new consultancy
Contacting individuals in a new way	SMS alerts, email marketing campaign, or new alumni survey
Processing that involves preventing data subjects from exercising a right or using a service or contract	Limiting web access that might prevent someone viewing transparency information, pre-screening people to determine whether to enter into a contract with them

Processing in a country outside Europe	Select ‘yes’ if any country outside the EEA is involved in any data processing, e.g. clinical trial data collection in Kenya, processing of human tissue samples in a lab in Malawi, or data stored in the cloud with a US-based company. This indicates that we may need to put additional considerations or protections in place in line with the guidance on international transfers.

PRIVACY RISKS

Identify the risks (what could go wrong in terms of data protection) and relate them to individual rights, legal or regulatory obligations, and corporate risks to LSTM. Examples of risks could include:

- activities that may hinder people’s ability to exercise their rights like their right to privacy or freedom of speech;
- lack of transparency resulting individuals are unaware of how their personal data is used;
- personal data used for a new purpose without a legal basis; and
- transfer of personal data to a "third country" (i.e. one outside of the EEA) in a way that breaches data protection law.

If necessary, record any risks on your project or departmental risk register. If you have identified risks relevant to the LSTM corporate risk register contact Kevin Francis.

Below are the assessment screening questions that were answered 'yes'. Each of these raises risks that you should list in the table below. Please add rows to this table for each risk you identify, and then complete the corresponding columns to your best judgment.

A template list of risks has been produced based on the screening questions. You may well have other risks of your own.

Data protection risk lookup.xlsx

Risks should be scored by their impact (1 – negligible, 2 – small, 3 – medium, 4 – high, 5 – disastrous) and likelihood (1 – remote, 2 – small, 3 – medium, 4 – high, 5 – inevitable).

Table 2 Risk assessment table header

Privacy risk	Risk to individuals	Compliance risk	Associated organisational risk	Impact	Likelihood

PRIVACY SOLUTIONS

Describe the actions you can 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).

The Result is either accepted, reduced, or minimised. Evaluation is your verdict on whether you believe the solution is ok, should be revisited, needs wider input, depends on another project, etc.

Table 3 Privacy solutions evaluation table

Risk	Solution	Result	Evaluation

INTEGRATE OUTCOMES INTO PROJECT

Here you should outline who is responsible for integrating the outcomes from the DPIA back into the project plan and updating any project management paperwork, e.g. the project manager. You should also outline who is responsible for implementing the solutions that have been approved and for securing the necessary budget to implement them. This should be signed off by the risk owner identified above.

Table 4 Proposed solutions table header

Risk	Solution	Action to be taken	Date for completion of action	Responsibility for action

ASSESSMENT ADVICE & FURTHER AMENDMENTS

It is everyone's responsibility at LSTM to uphold the data protection principles including accountability.

Advice – we have moved away from version 1.0 and 1.1 guidance where the DPO approved or rejected a DPIA. Now the DPO provides advice that project teams are responsible for considering and reflecting in their project plans.

You should revisit the DPIA to ensure actions are completed and to assess changes to your project in terms of their data protection risks.