Research: Data Protection Impact Assessment (DPIA)

Authored	**Research Office (K Hasan)**
Date	**Nov-2018**
Approved by	**Information Compliance**
Version	**1.0**

Table of Contents

1. Requirement

1.1 The Data Protection Impact Assessment (DPIA) is a requirement that is set out in both the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.[1]

1.2 The Research Office has prepared the guide set out here as it relates to Research and it forms part of the overall Research Ethics process. It is formulated in line with SOAS' corporate approach as set out in the Data Protection Impact Assessment Guide.

2. The Nature of the DPIA

What is a DPIA?

2.1 A Data Protection Impact Assessment (DPIA) is a process, mandatory in some instances, to help with the identification and minimisation of data protection risks associated with a given project. Risk is defined as: "*…a scenario describing an event and its consequences, estimated in terms of severity and likelihood.*"[2]

2.2 Where a determination is made that processing[3] is likely to result in a high-risk to individuals a DPIA *must* be undertaken. [4]

2.3 There are several aspects to the DPIA that must be covered. In particular, these relate to a description of the nature, scope, context and purpose(s) behind the processing. It must provide an assessment of the necessity, proportionality and compliance measures. Moreover, a risk assessment will be undertaken as part of that assessment. Invariably, that would identify and assess risks that may occur to individuals as well as outlining what measures are being proposed that seek to mitigate those risks.

2.4 In order to provide a sufficient assessment pertaining to the level of risk, consideration must also be given to both the likelihood and severity of any impact on individuals. Matters judged as falling within the realm of high risk, could arise from a high probability of some harm or alternatively, a lower possibility of serious harm.

---

[1] See: GDPR Article 35. DPA (2018) Schedule 6, Part 1 (27) (The applied GDPR and the applied Chapter 2), omits paragraphs 4/6 and 10 of GDPR Article 35. This is significant because paragraph 10 of Article 35 had that where processing was pursuant to Article 6 (1) (e) *[processing is necessary for the performance of a task carried out in the public interest*], the DPIA was deemed to have already been carried out by virtue of the general impact assessment made in the context of adopting that as being the lawful basis of processing.

[2] See: Section III, p. 6 of the WP29 published Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

[3] Processing: In relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as: collection, recording, organisation, structuring or storage, etc. See: GDPR Article 4 (2) and DPA (2018) Part 1 section 3 (Preliminary) (4).

[4] See: GDPR Article 35 (1). The salient features being: a) Processing involving the use of new technologies (e.g. such as AI); b) Given the nature, scope, context and purposes of processing – likelihood of high risk to the rights and freedoms of natural persons; and c) Impact assessments are to be undertaken *prior* to any processing operations being undertaken.

Responsibility and Ownership

2.5 As the Controller, SOAS retains overall responsibility for each DPIA.[5] In practice the individual who is leading on a project as it relates to research, is the Principal Investigator (PI) that has ownership. As part of the process in formulating the DPIA (including sign-off, assurance etc) other stakeholders[6] will also be involved, namely:

i. Information Compliance Manager
ii. Research Governance Officer
iii. (any other relevant stakeholders, e.g. IT, head of legal and governance)

2.6 With regards to the formulation of the DPIA, the PI shall seek the advice of the Information Compliance Manager and any of the other relevant parties as outlined in (2.5) above.[7]

2.7 A research project must not be commenced until the DPIA has been completed and it has received the appropriate authorisation and sign-off.

3. Screening Evaluation

3.1 Certain types of data processing activities by law require a DPIA to be undertaken. A preliminary screening assessment has therefore been formulated in order to help a researcher identify whether a mandatory DPIA is required for their particular project.

3.2 The screening evaluation is set out in Appendix 1 to this document. A copy of this, must be retained by the PI.

4. Content and scope

4.1 As outlined in (2.3), The DPIA must include and address the following:

i. A description of the nature, scope, context and purposes of the data processing
ii. Detail an assessment of the necessity, proportionality and compliance measures
iii. As far as is practicable, outline, identify and assess risks to individuals
iv. Identify the appropriate and proportional measures that will seek to mitigate those risks.

[5] GDPR Recital 84 reads: In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation.

[6] In some instances, it may be practicable to consult research participants. The ICO expects engagement of data subjects, though this may be difficult to achieve in certain research projects. There may be occasion where third-party data processors would be required (particularly if stipulated in relation to contract) to assist.

[7] GDPR Article 35 (2)

4.2 Although not mandatory, if the following areas appear as part of a research project it is *recommended* as best practice that a formal DPIA will be undertaken. These are:

i. Systematic processing of sensitive data or data of a highly personal nature.
ii. Processing of data concerning vulnerable data subjects.[8]
iii. The use of innovative technologies like AI.
iv. A large-scale project involved with processing personal data on a large scale.
v. A significant change to the nature, scope, context or purposes of data processing within the research context.

4.3 Prior to completion, the PI should seek the advice of the Information Compliance Manager and Research Governance Officer for any of the five-areas outlined in (4.2).

5. Process

5.1 There are nine elements or steps to the DPIA as a process.[9] These are details as follows:

i. Identifying whether a DPIA is required
ii. Describing the processing activities
iii. Consideration of consultation with any relevant parties or stakeholders
iv. Undertaking the assessment of necessity and proportionality
v. Identifying and assessing any risks arising
vi. Identifying and documenting the appropriate mitigation to reduce those risks
vii. Obtaining the requisite authorisation/sign-off and retaining documentation
viii. Integrating the DPIA into the overall project plan
ix. Setting necessary and appropriate dates for review.

5.2 The initial step for the PI will be to complete the Screening Evaluation (as per Appendix 1).

5.3 Where the Screening Assessment reveals that a DPIA is required, the PI must complete the DPIA template as set out in Appendix 2.

5.4 Upon completion, the PI is to retain a copy of the DPIA and submit a copy to:
i. Information Compliance Manager
ii. Research Governance Officer.

6. Unmitigated High-Risks

6.1 Where a determination has been made that high risks, which have been identified in the assessment cannot be mitigated, it *must* be escalated and referred to the Information Commissioners Office (ICO).

[8] Examples of vulnerable persons include children, individuals with mental/cognitive impairment, refugees etc.
[9] Taken from the ICO guidance.

6.2 Following such a referral, work on a given project *cannot* begin unless and until authorisation has been provided by the ICO.

6.3 The process for referral to the ICO will commence upon completion of the assessment and where it is determined that the risks cannot be mitigated. Although ownership rests with the PI, that referral to the ICO will be undertaken by the Information Compliance Manager and not the PI.

6.4 Where a DPIA has been referred to the ICO, the turnaround time for completion is approximately 8 weeks. For complex cases, the ICO reserves the right to extend this timeframe by a further 6 weeks. Following submission to the ICO, the Information Compliance Manager will notify the PI accordingly when a response is received.

Appendix 1: Screening Evaluation

Name:
Department / Centre:
Project Title:

Status:	*Staff*	*Doctoral Researcher*	*Postgraduate*	*Undergraduate*
	☐	☐	☐	☐

Externally funded?	**Yes**	**No**
	☐	☐

Please consider carefully whether each of the questions below applies to your research project.

Large scale[10] processing of special category data / data relating to criminal convictions and offences.[11]	**Yes** ☐	**No** ☐
Systematic monitoring of a publicly accessible place on a large scale.	**Yes** ☐	**No** ☐
Use of innovative new technologies (such as Artificial Intelligence) in the data processing	**Yes** ☐	**No** ☐
Processing of biometric or genetic data.	**Yes** ☐	**No** ☐
The processing of personal data which could result in a risk of physical harm in the event of a security breach.	**Yes** ☐	**No** ☐

- If you have answered **yes** to any of the areas identified above, then it will be mandatory to conduct a Data Protection Impact Assessment (DPIA).[12]

- Where you have answered **no** to any of the areas identified above, although a DPIA is not mandatory, you must retain the record of having conducted the screening assessment.

[10] As per the published guidance (WP248) p. 10, the factors to be considered when determining as to what extent constitutes 'large-scale' are: a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b) the volume of data and/or the range of different data items being processed; c) the duration, or permanence, of the data processing activity, and d). the geographical extent of the processing activity.
[11] GDPR Articles 9 and 10.
[12] See: GDPR Article 35 (3). In line with Article 35 (4), the ICO has outlined a list of processing operations that would precipitate a DPIA.

Appendix 2: Data Protection Impact Assessment (DPIA) Template

1. This template must be used to detail the DPIA covering the various issues, process and outcome. It broadly follows template provided by the Information Commissioners Office (ICO) and the published guidance accompanying the regulations.
2. The template will need to be completed once the screening evaluation (see appendix 1) and any 'yes' answer is recorded.
3. Additionally, if any significant changes are being made to an existing research project and therefore come within the scope of requiring a DPIA (post-screening) then this assessment template will also have to be completed and integrated into the overall research project plan.

1. DPIA Requirement
▪ *Detail a brief synopsis of the research project* ▪ *Outline the reason why the DPIA has been required (refer to initial screening evaluation) and what part it plays in the overall research project* ▪ *Other documentation can be referenced, including the detailed research proposal, Ethics Assessment etc.*
2. Nature, extent and context of Processing
▪ *Outline the methods for collection, use, storage of data* ▪ *Detail the nature and source of data (where appropriate)* ▪ *If data is being shared, detail with who (e.g. another institution)* ▪ *Detail the following: is the data relating to Special Category Data? Is the data relating to criminal convictions and offences? Does it involve any data relating to vulnerable persons?* ▪ *Outline the number of data subjects and scope of data collection* ▪ *Outline any concerns relating to the security underpinning that data collection/storage* ▪ *Mention whether there is use of new or innovative technologies relating to the above*

3. Consultation

- *The section can be utilised to detail any discussion(s) / advice received or sought from various stakeholders: e.g. IT security, Head of Department, third-parties etc.*

4. Assessing Necessity & Proportionality

- *Detail the lawful basis for processing: as set out in Ethics Assessment*
- *Other areas to consider may include: the relationship of this data processing to the overall aims/methodology of the research project*
- *What steps are being undertaken to ensure data quality, minimization*
- *How do you plan to safeguard international transfers (if applicable)*
- *Any significant or other serious issues relating to obtaining consent from research participants*

5. Assessing Necessity & Proportionality

Describe source of risk and nature of potential impact		**Likelihood of harm**	**Severity of harm**	**Overall risk**
[*Individual risks can be numbered for ease of reference and given an appropriate assessment as per the additional columns*]	[*In tandem, risks that could potentially affect the School's compliance/ organisational risk position should be detailed (e.g. obligations, reputation, funding obligations etc*)]	*Remote, possible or probable*	*Minimal, significant or severe*	*Low, medium or high*

6. Mitigation

Identify additional appropriate and proportional measures in order to reduce or eliminate risks identified as being medium or high risk in section 5 above.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	*Low medium high*	*Yes/no*

7. Authorisation

Item	**Name/date**	**Notes**
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
ICM provided:		*Information Compliance Manager to advise on compliance: step 6 measures and whether processing can proceed*

Summary of advice: [*E.g. by the Information Compliance Manager and other relevant parties where required: e.g. Research Governance Officer*]		
Advice accepted or overruled by:		If overruled, detail the reason(s) and rationale.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		