THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

IGC/19/17

Operational

Data Protection Impact Assessment

Overview

Data Protection Impact Assessments (DPIA) are the new name for Privacy Impact Assessments under the General Data Protection Regulation. They are intended to assess if new processing of personal data will have risks to the individuals concerned and how those risks will be mitigated.

Remember that personal data is any data that identifies or is identifiable regarding an individual. So include names, email addresses, IP addresses etc.

You should use the screening questions in Section 1 to decide if you need to fill out the template. Section 2 contains the DPIA template itself.

Contact Rachael Maguire, the Data Protection Officer for advice on filling out the template, particularly if you have never done this before.

Section 1: Screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

1. **Does this involve the collection of new information about individuals?**
   Re-use of data collected for one purpose e.g. providing a service but now being used for research is covered by question 4.

2. **Will individuals be required to provide information about themselves?**
   This could occur if an organisation has commissioned a research project relating to staff or if we are introducing a new staff or student system.

3. **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**
   This could cover situations where an organisation is providing you with information for a research project that they haven't supplied to a third party before or when the School has a new partner they will be sharing information with.

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?**
   If you are re-using data for research, then this question won't apply.

5. **Are you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**
   This would cover things like fingerprint or facial recognition technologies.

6. **Will the processing result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**
   For example, could the processing affect examinations? If you are conducting research for an organisation that could affect their clients or staff, this may apply.

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 private.**
   Or any of the special categories personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life.

8. **Will the processing require you to contact individuals in ways that they may find intrusive?**
   This may vary from individual to individual e.g. some people are happy for their health records to be used for research, others only want them used for their health care.

9. **Has a research funder or data provider asked for the results of a Privacy Impact Assessment?**
   If you have not done a privacy impact assessment prior to this request, but are required to by a research funder or data provider, you will need to fill out this form.

Section 1: Data Protection Impact Assessment

Please note: all italicised text can be deleted as you fill in the form.

The DPIA contains the following steps:

1. Why do you need a DPIA
2. What will happen to the personal data
3. Consultation with the individuals whose data you are using and others
4. What are the issues with the processing and the risks to the individuals
5. What are your solutions
6. Risk, Solution and Approval

Step one: Why do you need a DPIA

The personal data includes ethnic origin, trade union membership, physical/mental health condition of the waste workers covered in the research project, which are classified as Confidential. The personal data will only be used as control variables in statistical analysis and no personal data will be disclosed, idnetified or shared. The research project is expected to result in journal articles, policy reports and a book.

Step two: What will happen to the personal data?

The data will be collected via the Qualtrics survey software avaialble through LSE by trained field enumerators. The data will be stored with the RLAB at CEP. Only project staff will be able to use the personal data for statistical analysis which will only bereported as aggregate statistics in any publication.

↓

Data will be stored encrypted on RLAB drives. A Data Management Plan has been approved by the Research Ethics Committee of the LSE.

↓

Pseudonymised dataset will be available for future research, after removing the personal data questions.

Step three: Consultation with the individuals whose data you are using and others

The RLAB has helped prepare the Data Management Plan. Informed consent will be taken from participants.

Step four: What are the issues with the processing and the risks to the individuals

None, only anonymised data will be available and the personal data questions will not be shared.

Annex 2 can be used to help you identify the DP related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Data will be obtained anonymised. Personal data on ethnic origin, trade union membership and physical/mental health will only be held by RLAB and used just in statistical analysis as aggregates (and not published for individuals).	*The only variables of a sensitive nature are trade union membership or physical/mental health condition of the individuals, but these will not be shared on an individual basis. Therefore, no risk to individuals is expected.*	*None*	*None*

Step five: What are your solutions?

What actions will you take to mitigate these risks and issues? Will these actions eliminate the risk, reduce it or can you live with it? Will the proposed actions provide a solution that is DP compliant, justifies your processing and is proportionate to what you want to do with the data?

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
The only variables of a sensitive nature are trade union membership or physical/ mental health condition of the individuals, but these will not be shared on an individual basis. Therefore, no risk to individuals is expected.	*Data will be obtained anonymised. Personal data on ethnic origin, trade union membership and physical/ mental health will only be held by RLAB and used just in statistical analysis as aggregates (and not published for individuals).*	*Eliminated.*	*Final impact is justified, compliant and proportionate.*

Step six: Risk, Solution and Approval

Add the risks and solutions here and either the DPO or the AD of Cybersecurity and Risk will sign them off.

Risk	Approved solution	Approved by
The only variables of a sensitive nature are trade union membership or physical/mental health condition of the individuals, but these will not be shared on an individual basis. Therefore, no risk to individuals is expected.	*Data will be obtained anonymised. Personal data on ethnic origin, trade union membership and physical/mental health will only be held by RLAB and used just in statistical analysis as aggregates (and not published for individuals).*	*Rachael Maguire, DPO*

Step seven: Doing the actions

Who will actually take the actions listed in the solutions? When will they be done by?

Action to be taken	Date for completion of actions	Responsibility for action
Nic Warner, RLAB	*2 years, Sep 1 2023 to Aug 31, 2025*	*Swati Dhingra* *Nic Warner*

Contact point for future privacy concerns
Swati Dhingra and Nic Warner

Annex 1: Primary contacts for advice and guidance

Rachael Maguire
Information and Records Manager
Secretary's Division
r.e.maguire@lse.ac.uk
ext: 4622

Jethro Perkins
AD Cyber Security and Risk
DTS
j.a.perkins@lse.ac.uk
ext: 6641

Annex 2: Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

Have you identified the purpose of the project? Yes

How will you tell individuals about the use of their personal data? Informed verbal or written consent (Some individuals may be unable to read and write so verbal consent might be needed)

Do you need to amend your privacy notices? No

Have you established which conditions for processing apply? Yes

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? Informed verbal or written consent will be taken and the survey will be terminated if it is denied.

If your organisation is subject to the Human Rights Act, you also need to

consider: Will your actions interfere with the right to privacy under Article 8? No

Have you identified the social need and aims of the project? Yes

Are your actions a proportionate response to the social need? Yes

Principle 2

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

Does your project plan cover all of the purposes for processing personal data? Yes

Have you identified potential new purposes as the scope of the project expands? No

Principle 3

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

Is the quality of the information good enough for the purposes it is used? Yes

Which personal data could you not use, without compromising the needs of the project? If trade union embership, ethnic origin and physical/mental condition is not important in work performance, teir use will be dropped. We expect union membership is non-existent for these workers.

Principle 4

Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

If you are procuring new software does it allow you to amend data when necessary? NA

How are you ensuring that personal data obtained from individuals or other organisations is accurate? Trained field enumerators are collecting the data, but these are self-reported answers and not being verified from elsewhere .

Principle 5

Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

What retention periods are suitable for the personal data you will be processing? Two years

Are you procuring software that will allow you to delete information in line with your retention periods? Yes

Principle 6

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Do any new systems provide protection against the security risks you have identified? No

What training and instructions are necessary to ensure that staff know how to operate a new system securely? N/A

Chapter 3 Data subject rights

Will the systems you are putting in place allow you to respond to subject access requests more easily? Yes

Can the new system cope with demands for data rectification, deletion and portability? Yes

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose? N/A

Principle 7

Chapter 5 transfers outside EEA

Will the project require you to transfer data outside of the EEA? No, the data collection will happen in India and be porcessed in the UK.

If you will be making transfers, how will you ensure that the data is adequately protected? N/A

Review schedule

Review interval	Next review due by	Next review start
2 years	20/09/2021	01/9/2022

Version history

Version	Date	Approved by	Notes
3	25/6/2018	Rachael Maguire	Minimal changes to reflect change in legislation
4	20/9/2019	IGMB	Major changes to template

Contacts

Position	Name	Email	Notes
Data Protection Officer	Rachael Maguire	r.e.maguire@lse.ac.uk	Author

Communications and Training

Will this document be publicised through Internal Communications?	**YES**
Will training needs arise from this policy	**YES**
If Yes, please give details To BIU so they are able to integrate this into their processes. Also into Data Protection and Research training.	