THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

Policy – Data Protection Impact Assessments

This policy sets out why, how and when Data Protection Impact Assessments (DPIA) should be used at the School.

Why a DPIA should be completed

1. Article 35 of the General Data Protection Regulation states that a DPIA should be conducted '(w)here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'. The DPIA should be carried out before the processing. One DPIA can cover multiple types of the same processing.

2. Article 35(3) states that a DPIA is particularly needed for the following:

    a. 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

    b. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

    c. a systematic monitoring of a publicly accessible area on a large scale'.

3. Article 35(7) says that the DPIA should contain at least the following:

    a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

    b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The Article 29 Working Party (now the European Data Protection Board) released guidance setting out more examples of what was high risk processing. Their list includes:

a. 'Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements'

b. 'Automated-decision making with legal or similar significant effect', that is, processing that could be discriminatory.

c. 'Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area"'

d. 'Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences'

e. 'Data processed on a large scale', that is, a large amount of data subjects and/or covering a large territory and/or a large range of data and/or a large timeframe for processing.

f. 'Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject'

g. 'Data concerning vulnerable data subjects' like the mentally ill, children and the elderly and where there is a definite power imbalance like employees.

h. 'Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.'

i. 'When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.'

5. Although the DPIA is supposed to be carried out prior to processing, it can and should be carried out on any current high risk processing.

When should a DPIA be conducted

6. DPIAs should be conducted at the School for:

    a. New systems

    b. Old systems with high risk processing

    c. New forms of processing using current systems e.g. use of Microsoft Forms to collect high risk data

    d. High risk research involving human subjects

    e. High risk research involving special categories data

    f. High risk research involving the merging of large data sets

    g. Any other high risk processing.

7. CCTV and other surveillance is covered by the Surveillance Commissioner, who has developed a DPIA specifically for surveillance with the Information Commissioner. This should be used for the introduction of any new surveillance systems and processes.

Appendix A: How DPIAs should be conducted

8. The School has a DPIA form that should be used to conduct a DPIA. Originally based on the ICO template, it has been reformatted to make the language less legalistic

9. It contains two parts:

    a. The first part is screening questions to determine if a DPIA is needed. If all questions are answered no, this can be noted and the DPIA does not to be taken any further.

    b. The second part covers the requirements to consider the risks and how to mitigate them set out in 3) above.

10. The DPIA should be filled out by the staff member leading on the processing. This could be the system owner, the project leader or manager, the principal investigator, etc.

11. At any point in the process, the staff member filling out the DPIA should contact the Data Protection Officer (DPO) and/or the Cybersecurity team for advice and guidance. There are different risks based on the data protection principles including security and data subject rights. Both need to be considered.

12. The screening questions (Section 1 of the DPIA form) cover the triggers set out in 4. above.

13. Section 2 includes the following. Each session has questions and prompts to promote thinking and a worked example to show how to fill the form in.

    a. Step One – why the DPIA needs to be done, based on the screening questions.

    b. Step Two – what will happen to the personal data? This should be a description of how the personal data will be used in the system, to achieve the project aims, for the research project, etc.

    c. Step Three – consultation. Staff filling out the DPIA should consult with the individuals concerned, third party suppliers and other stakeholders as soon as possible and give a summary of that consultation here.

    d. Step Four – What are the issues and risks. This step is intended to get the staff member thinking about the issues and risks relating to the processing they intend to carry out. There are three potential areas: risks to individuals, risk to compliance and risks to the LSE. The staff member should consider which of these areas or if all of them are involved in the risk.

    e. Step Five – What are your solutions. How are the risks identified in Step Four to be mitigated. This goes through: the risk; the solution to that risk; whether that eliminates or reduces the risk or whether we just accept it; and whether the final impact of the solution is justified, compliant and

proportionate. For example, LSE email addresses are not going to need encrypted transfer when we make them available on the website, while occupational health records will need a very secure transfer method.

f. Step Six – Approval. The solution needs to be signed off by the DPO, Cybersecurity and/or the Senior Information Risk Owner (SIRO).

g. Step Seven – Doing the Actions. Covers how the solutions are going to be fed back into the project plan/research/etc.

14. Once approved by the appropriate officer(s), the staff member will ensure that the solutions are carried out. The DPO will keep a log of the DPIAs and a copy in OneDrive.

Review schedule

Review interval	Next review due by	Next review start
3 years	31/07/23	01/07/23

Version history

Version	Date	Approved by	Notes
1	22/06/2020	IGMB	

Links

Reference	Link
Data Protection Policy	https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/datProPol.pdf
DPIA form	https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/DPImpTem.docx

Contacts

Position	Name	Email	Notes
Rachael Maguire	Information and Records Manager	glpd.info.rights@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**Yes/ No**
Will training needs arise from this policy	**Yes/ No**
If Yes, please give details DPIA training and briefings.	