Overview

IGC/19/17

Operational

Data Protection Impact Assessment

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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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 2: Data Protection Impact Assessment

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

The DPIA contains the following steps set out in the boxes below.

1. Why do you need a DPIA – fill out this step yourself
2. What will happen to the personal data fill out this step yourself
3. Consultation with the individuals whose data you are using and others – this may need filling out with the DPO/Cybersecurity
4. What are the issues with the processing and the risks to the individuals – this will need filling out with the DPO/Cybersecurity
5. What are your solutions – this will need filling out with the DPO/Cybersecurity
6. Risk, Solution and Approval – this will need filling out with the DPO/Cybersecurity.
7. Doing the actions – fill out with DPO/Cybersecurity but you will need to carry out the actions identified.

|  |
| --- |
| **Step one: Why do you need a DPIA***What are you going to use the personal data for. Is it a research product, a new system or a new service? Use the screening questions as the basis for your response here. If it is a specific project, use your project documentation for this question.* |

|  |
| --- |
| **Step two: What will happen to the personal data?***How are you going to collect the data? Where will it be stored? Who will have access? If you are using it in a publication, how?**e.g. Data will be collected from research participants via online forms**↓**Data will be stored encrypted on departmental drives**↓**Pseudonymised dataset will be provided to Department X along with report* |

|  |
| --- |
| **Step three: Consultation with the individuals whose data you are using and others***Who have you talked to about this processing? Are you able to talk to the individuals concerned and how? Have you talked to other people e.g. Discussed storage with Information Security Team.* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step four: What are the issues with the processing and the risks to the individuals***Could the processing possibly harm or inconvenience the individuals concerned. Could we be in breach of data protection or any other law e.g. confidentiality? Could the School’s ability to teach or conduct research have a negative impact?**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 |
| *E.g. 1. Using video to assess research subjects’ attitudes to race* | *If released could cause harm and distress to research subjects due to subject matter* | *Could be requested under Subject Access requests at which point we lose control of the video* | *Could lead to future research being affected if potential research subjects think the School will not keep their data secure.* |

 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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? |
| *E.g. 1. Videos could be requested under Subject Access requests at which point we lose control of the video* | *Provide access to videos on site if requested, without providing a copy* | *Eliminated – the videos would not be released outside the School.* | *Final impact is justified, compliant – research subjects can still see videos – 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  |
| *e.g. 1. Videos could be requested under Subject Access requests at which point we lose control of the video* | *Allow access onsite* | *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 |
| *e.g. 1. Access to videos onsite* | *When requested: within 40 days of request being made* | *Primary Investigator and Data Protection Officer* |

|  |
| --- |
| Contact point for future privacy concerns  |
| *List all the people with responsibility for action above.* |

 |

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?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

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?

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?

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

Are your actions a proportionate response to the social need?

**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?

Have you identified potential new purposes as the scope of the project expands?

**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?

Which personal data could you not use, without compromising the needs of the project?

**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?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

**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?

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

**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?

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

**Chapter 3 Data subject rights**

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

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

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

**Principle 7**

**Chapter 5 transfers outside EEA**

Will the project require you to transfer data outside of the EEA?

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

**Review schedule**

|  |  |  |
| --- | --- | --- |
| **Review interval** | **Next review due by** | **Next review start** |
| 2 years | 28/02/2022 | 01/02/2022 |

**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 |
| 4.1 | 28/2/2020 | Rachael Maguire | Minimal 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 detailsTo BIU so they are able to integrate this into their processes. Also into Data Protection and Research training. |