Information Compliance

Data Protection Impact Assessments

May 2019

Document properties

Authority

Chief Information Officer

Sponsor

Chief Information Officer

Responsible Officer

Data Protection Officer

Version history

This is version 1 of this policy.

1 Introduction

Data protection law focuses on accountability and a concept called ‘data protection by design and default’. Data protection impact assessments (DPIAs) are a central part of this focus.

This document explains the advantages and requirements of DPIAs, and the process to follow for conducting DPIAs.

2 Executive summary and key points

2.1 What is a DPIA?

A DPIA is process used to identify and minimise risks to personal data associated with a new project, or a modification of an application already in use. It is an integral component of privacy by design and default.

If a DPIA is required, it must be completed as early in the project timeline as possible, and reviewed at regular intervals.

2.2 Conducting a DPIA

Initially, a pre-assessment questionnaire is used to determine if a full DPIA is required.

There are 6 steps to complete in a full DPIA, which must then be reviewed and signed off.

2.3 Risks and risk mitigation

This section presents the kinds of risks which may arise from using personal data, including identity theft, financial loss and reputational damage, and measures which can be taken to mitigate those risks.

2.4 Register and publication

The Data Protection Officer has established a register of DPIAs. The Information Commissioner’s Office recommends that public authorities make their completed DPIAs externally available.

2.5 Related policies and further guidance

A list of University policies and other documents affecting confidentiality of student information is provided in section 7.

3 What is a DPIA?

3.1 Accountability and privacy by design and default

A DPIA is a process which helps the University identify and minimise risks to personal data with respect to a particular project or plan. It is a legal requirement under principle 7 of the Data Protection Act 2018. This principle states that the Controller (in this case, the University) shall be responsible for, and able to demonstrate compliance with, the other principles.

DPIAs are also an integral component of privacy by design and default. In any case where a new application or system, which uses personal data, is being considered, a DPIA should be conducted. This is also the case where a change is being made to an application or system currently in use, where that change will introduce new uses of personal data.

A DPIA should be conducted as early in the development of a project as possible. It is always easier to build compliance in at the beginning, than it is to try to retrofit data protection compliance later in the process.

It is important to remember that, once completed, a DPIA is not a 'file and forget' document. It should be revisited and revised as necessary at each stage of the project, to ensure that any changes to the project design or function are taken into account. It also provides a useful way to check that mitigation strategies have been appropriately addressed.

3.2 Advantages of a DPIA

Conducting a DPIA helps to identify several possible risks:

- Risks to individuals' rights and freedoms with respect to the use of their personal data
- Corporate risks, such as reputational damage or fines
- Compliance risks, not only with data protection law, but other laws and statutes.

Once the possible risks are identified, programme or application design can be modified as necessary to mitigate the risks as far as possible. Any residual risks can be entered into the corporate risk register, and either further mitigated as design changes are made, or accepted by the University.

3.3 Legal requirements

Although it is recommended that a DPIA be conducted for any new or modified project, application or system which is or will be using personal data, there are instances where conducting a DPIA is a *legal requirement*.

If it is likely that the use of personal data will result in a **high risk** to the rights and freedoms of individuals, then a DPIA is required. There are three types of personal data use which always require a DPIA, and these are set out in data protection legislation:

- Systematic and extensive profiling with significant effects
- Large scale use of special category data (including personal data related to criminal convictions or offenses)
- Systematic monitoring of a publicly accessible area on a large scale.

The Information Commissioner's Office (ICO), as required, had published a list of processing operations that require a DPIA:

1. Use of innovative technology
2. Denial of service
3. Large-scale profiling
4. Biometrics
5. Genetic data
6. Data matching
7. Invisible processing
8. Tracking
9. Targeting of children or other vulnerable individuals
10. Risk of physical harm

Detailed information on each of these is available on the ICO's website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/.

3.4 Consulting the ICO

If a completed DPIA identifies a high risk, and there are no effective ways to reduce it, data protection law states that we must consult the ICO. No use of personal data in the project or application can occur until the consultation is completed.

Should consultation with the ICO be necessary, please contact the Data Protection team at data-protection@brunel.ac.uk. The Data Protection Officer (DPO), or Deputy Data Protection Officer (DDPO), will act as liaison with the ICO.

4 Conducting a DPIA

DPIAs *must* be conducted for any use of personal data which is likely to result in a *high risk* to individuals' interests, but as a matter of good practice, should be conducted as part of any project which involves a new use of personal data, whether for a new application or system, or changes to an application or system already in use.

DPIAs are an effective way of assessing the data protection risks in projects involving personal data.

Appendix 1 shows a flowchart of the DPIA process.

4.1 Responsibility

Someone with an in-depth knowledge of what personal data will be used in the project or application, how it will be used, shared, and the likely retention period, should conduct the DPIA. It is permissible to outsource the DPIA to a consultant or data processor, but the University is still responsible for the DPIA.

The Data Protection team is *not* responsible for conducting a DPIA. As the DPO has certain responsibilities for providing advice on the DPIA, authoring the DPIA itself presents a conflict of interest, and is not in keeping with the statutory responsibilities of the DPO.

4.2 Pre-assessment

The pre-assessment questionnaire is used to conduct a high-level analysis of the project or application. The answers will assist the DPO to determine if a full DPIA is required.

The pre-assessment questionnaire is available on the intranet at https://intra.brunel.ac.uk/s/GILO/Information%20Compliance/Data%20Protection/Pages/Policies-Procedures-Guidance.aspx.

Upon completion, the pre-assessment questionnaire must be sent to the DPO at data-protection@brunel.ac.uk. The DPO will notify the person completing the pre-assessment questionnaire if a full DPIA is required.

Even if a full DPIA is not required, should there be any redesign or other changes to the scope of the project, the answers to the pre-assessment questionnaire should be reviewed to determine if a full DPIA should, in fact, be conducted. Revised pre-assessment questionnaires must be sent to the DPO as above, with a short explanation of the reasons for the revision.

4.3 Full DPIA

The project sponsor may decide a full DPIA is required, the DPO may advise that one is needed, or one can be conducted because it is good practice to do so.

The template for a full DPIA can be found on IntraBrunel at the URL in the previous section.

There are six steps to a DPIA:

1. Identify the need for a DPIA

   If the project is a major one, involves a high risk to personal data, or the DPO has recommended a DPIA be conducted, then this step can be skipped. Otherwise, indicate what the project is intended to achieve, and what uses of personal data are involved.

2. Describe the processing

   This step asks for detailed information regarding the personal data which is intended to be used.

3. Consultation process

   It is often useful to have a consultation with a representative group of stakeholders, especially those whose personal data may be used. If no consultation is anticipated, the reasons for not doing so should be noted in this section.

   If consultation is to take place, no further work on the DPIA or the project should take place until that is complete, and the responses have been analysed. It may be necessary to tweak the project design based on the responses, and this will have an effect on the rest of the DPIA.

4. Assess necessity and proportionality

   This step addresses the legal basis for using personal data, privacy notices, retention schedules, and individuals' rights.

5. Identify and assess risks

   This step, and the one following it, is one of the most important of the DPIA. The source and potential impact on the use of individuals' personal data must be carefully considered; this may be physical, emotional or material harm.

   Possible security risks must also be assessed, to include the sources of risk and the potential for each type of breach.

   Please refer to section 5 for further information on risks.

6. Identify measures to reduce risk

   For each risk identified in step 5, you should try to identify any options which could reduce or eliminate the risk, the effect of each option on the risk, what the residual risk would be. The cost and benefit of each option can be taken into account to decide if the mitigation would be appropriate.

   Whether the proposed mitigation measure is approved will be determined when the DPIA is signed in step 7.

7. Sign off and record outcomes

   For this part, a number of individuals should sign off the DPIA.

   The project sponsor should review the DPIA at this point.

   a) Mitigation measures and residual risks must be approved by the Chief Information Security Officer (CISO). Note that, if the decision is to accept a residual risk which is a high risk, the ICO must be consulted. *No further work should take place on the project until that consultation is complete.*

   The CISO should go through step 6 and indicate whether each proposed risk mitigation measure is approved.

   b) The DPO will review the DPIA, and provide a summary of her/his advice on the risk mitigation measures.

   c) The project sponsor, in consultation with the CISO, should indicate if the DPO's advice is accepted or rejected. If the DPO's advice is *not* accepted, the reasons for overruling it must be explained.

   d) The individual who reviewed the consultation responses (most likely the project sponsor) must sign, and if the decision is not to take the consultation responses into account, the reasons for doing so must be recorded.

   e) The project sponsor or project manager must sign that they will keep the DPIA under review during the life of the project.

   The outcomes of the DPIA must be integrated into the project plan, and the DPIA should be reviewed, and if necessary, modified at appropriate intervals.

5 Risks and risk mitigation

5.1 Possible risks

The following provides a non-exhaustive lists of the kinds of risks which may arise from using personal data in a project:

- Inability to exercise rights (not limited to privacy rights)
- Inability to access services or opportunities
- Loss of control over use of personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Re-identification of pseudonymised data
- Any other significant economic or social disadvantage.

5.2 Possible risk mitigation measures

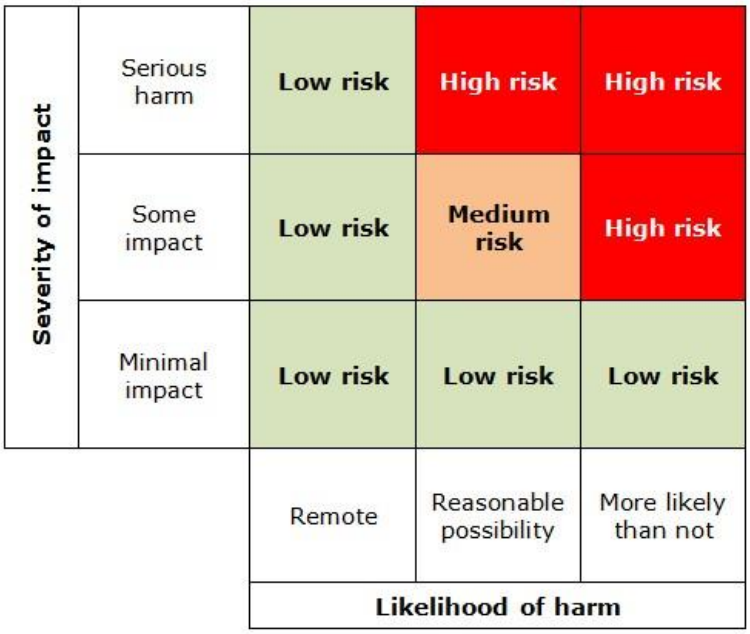
Some possible ways of reducing risks in relation to the use of personal data are:

- Not collecting certain types of data
- Reducing the scope of the processing
- Reducing retention periods
- Putting in additional technological security measures
- Training staff to ensure risks are anticipated and managed
- Anonymising or pseudonymising data where possible
- Producing internal guidance or processes to avoid risks
- Using a different technology
- Putting clear data-sharing agreements in place
- Making changes to privacy notices
- Offering individuals the opportunity to opt out where appropriate
- Implementing new systems to help individuals exercise their rights.

This list is not exhaustive.

5.3 Risk assessment matrix

The matrix shown below is useful for assessing risks based on severity of harm and likelihood of occurrence:



6 Register and publication

The DPO has established a register for recording pre-assessments and DPIAs, and will report the outcome for each to the relevant Committee or Sub-Committee.

It is considered good practice for public authorities to make their DPIAs externally available. If necessary, the documents can be redacted, or a summary can be published.

7 Related policies and further guidance

Further information can also be found in the following University documents:

- Data Protection Policy: https://www.brunel.ac.uk/about/documents/pdf/DP-policy.pdf
- Records Management Policy: https://www.brunel.ac.uk/about/documents/pdf/records-management-policy.pdf
- University Retention and Disposal Policy: https://intra.brunel.ac.uk/s/GILO/records/Pages/Retention-Policy.aspx
- University Retention Schedules: https://intra.brunel.ac.uk/s/GILO/records/Retention%20Schedule%20Docs/Brunel%20University%20Retention%20Schedules%20-%20Master%20List.pdf

- Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- Cyber & Information Security ISMS Policies and Procedures: https://intra.brunel.ac.uk/s/cc/security/cyber-security/Cyber%20Documents/Forms/AllItems.aspx

For further guidance:

email: data-protection@brunel.ac.uk

web page: http://www.brunel.ac.uk/about/administration/information-access/data-protection

Appendix 1 – DPIA process flowchart