University of Essex

Data Protection Impact Assessment Policy

Authors:	Information Governance Manager
Publication date:	November 2022
Amended:	-
Review date:	December 2025

Table of Contents

Data Protection Impact Assessment Policy

Introduction

1. A Data Protection Impact Assessment (DPIA) is a tool that enables the University to identify and minimise the data protection and privacy risks of processing (using personal data). As well as ensuring compliance with the associated requirements of the Data Protection Act 2018, an effective DPIA can also bring financial and reputational benefits, helping the University to manage personal data appropriately, identify solutions to questions raised about such data management, as well as demonstrating accountability and building trust within and among data subjects.

2. DPIAs consider data protection compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The risk focus within a DPIA should be on the potential for harm to individuals or to society at large, whether this would be physical, material or non-material. The question of the likelihood of any harm should be clearly addressed. The risk assessment should indicate whether any mitigations may reduce the level of risk, and/or whether the risk is acceptable. There may be some instances where the risk and associated likelihood of harm are accepted when balanced with the necessity of the data processing.

3. DPIAs are a legal requirement under Data Protection law for any processing that is likely to be high risk. Failure to carry out a DPIA when required, carrying out a DPIA in an incorrect way, or failing to consult the ICO where required, may result in financial penalties.

Responsibilities

4. The University's designated Data Protection Officer:

   - informs and advises all members of staff of the need to complete a DPIA
   - supports staff in completing a DPIA, providing expert advice and guidance on matters such as legal bases and consent processes, and
   - monitors the performance of DPIAs, to ensure identified actions are completed and risks are mitigated

5. All staff:

- must seek the advice and support of the Data Protection Officer before beginning any new processing or undertaking a project which requires a DPIA

When to conduct a DPIA

6. The University will conduct a DPIA whenever a DPIA is legally required. This is where the processing is likely to result in a high risk to individuals, and the project/processing:

- uses systematic and extensive profiling or automated decision-making to make significant decisions about people
- processes special-category data or criminal-offence data on a large scale1
- systematically monitors a publicly accessible place on a large scale
- uses innovative technology in combination with any of the criteria in the European guidelines2
- uses profiling, automated decision-making or special category data to help make decisions on an individual's access to a service, opportunity or benefit
- involves carrying out profiling on a large scale1
- processes biometric or genetic data in combination with any of the criteria in the European guidelines
- involves combining, comparing or matching data from multiple sources
- processes personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines
- processes personal data in a way that involves tracking individuals' online or offline locations or behaviour, in combination with any of the criteria in the European guidelines

---

[1] 'Large scale' is not defined in law, but the application of any definition within a DPIA should take into account: the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; and/or the geographical extent of the processing activity. The consideration of these factors, separately and in combination, within the DPIA should identify whether the data processing is on a large scale.

[2] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

- processes children's personal data for profiling or automated decision-making or for marketing purposes or when offering online services directly to them, or

7. processes personal data that could result in a risk of physical harm in the event of a security breach

8. The University will also conduct DPIAs where such use is considered best practice, and as early as possible in any project's or activity's lifecycle. In line with the risk-based approach embodied by the GDPR, this is where the processing:

- is part of any major project which requires the processing of personal data
- involves evaluation or scoring
- involves systematic processing of sensitive data or data of a highly personal nature
- includes personal data on a large scale
- includes data concerning vulnerable data subjects
- uses innovative technological or organisational solutions, or
- prevents data subjects from exercising a right or using a service or contract

9. Where the University decides not to carry out a DPIA, the reasons for not doing so will be documented.

Content of a DPIA

10. A DPIA will:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks, and
- include the views of data subjects and other stakeholders where appropriate. If the views of data subjects are not sought the University will document its justification for not seeking the views of data subjects, for example, if doing so would compromise the confidentiality of business plans or would be disproportionate or impracticable

DPIA Outcomes

11. The Data Protection Officer will support staff in completing the DPIA, using a standard Data Protection Impact Assessment template (.docx), and the advice and recommendations of the Data Protection Officer will be recorded.

12. The risks associated with the project or activity will be recorded in the DPIA, along with measures to mitigate the risks. These risks and any other associated actions will then be incorporated into appropriate risk registers and/or into the overall planning for the project. The project should not start until mitigating measures are in place.

13. If high risks are identified that cannot be mitigated, and that are not accepted, the University may consult the ICO before starting the processing.

14. The DPIA will be signed off by the Head of Department/Section.

Document Control Panel

Field	Description
Title	Data Protection Impact Assessment Policy
Policy Classification	Policy
Security Classification	Open
Security Rationale	N/A
Policy Manager Role	Information Assurance Manager
Nominated Contact	dpo@essex.ac.uk
Responsible UoE Section	Office of the Vice-Chancellor
Approval Body	University Steering Group
Signed Off Date	November 2022
Publication Status	Published
Published Date	December 2022
Last Review Date	October 2022
Minimum Review Frequency	3-Yearly
Review Date	December 2025
UoE Identifier	0194

If you require this document in an alternative format, such as braille, please contact the nominated contact at dpo@essex.ac.uk