UNIVERSITY OF EXETER

Data Protection Impact Assessment (DPIA) Policy

Version:	**1**
Dated:	**01 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
V 0.1	May 2018	R Platt	Initial draft
V 1	May 2018	R Platt	Approved Version

Distribution

Name	Title

Approval

Version	Approval	Date
V 1.0	Information Governance & Security Steering Group	May 2018

Contents

1 Introduction

The University of Exeter is fully committed to protecting the personal data of its students, employees, suppliers and other stakeholders in accordance with the requirements of the General Data Protection Regulation (GDPR). We take the privacy of personal data very seriously and have initiated a variety of methods and controls to ensure we know what data we collect and hold and that we protect that data appropriately.

As part of this commitment, the University of Exeter ensures that, where appropriate, projects and personal data processing activities are subject to a Data Protection Impact Assessment (DPIA) as a key component of a ‘Privacy by Design’ approach.

The purpose of this assessment is to ensure that our use of personal data is fully understood, that risks to the rights and freedoms of individuals resulting from the processing of personal data are carefully examined and that all appropriate measures are put in place to protect these rights throughout the lifecycle of the processing.

This document sets out the policy for DPIA’s and, in conjunction with the associated forms and guidance, should be used to ensure that our obligations and policies in this area are met.

2 Responsibilities

The University of Exeter is the ‘data controller’ and the Council of the University, as the governing body, is ultimately responsible for compliance with current data protection legislation. The University will take the appropriate measures to ensure privacy by design and to protect data subject’s rights under the legislation.

2.1 Information Users

All members of the University are responsible for complying with all relevant data protection legislation and this policy. Where a concern about a data asset is identified this should be raised with the IAO and the information governance office to enable an assessment to take place.

2.2 Project Managers

Project Managers should ensure that any project that involves processing of personal data is assessed to identify if a DPIA is required and that the DPIA is maintained throughout the project until such time as appropriate to hand over to the IAO. They should ensure that the DPO is consulted, in a timely manner, in all issues relating to the protection of personal data.

2.3 Researchers

Researchers should ensure that a data management plan that incorporates a DPIA is completed for any project that involves processing of personal data. Where additional advice is required they should contact the Research Governance and Ethics office in the first instance who will liaise with the Information Governance

Office as required. Where a funding body requires the opinion of the DPO the researcher must ensure that the DPO is consulted, in a timely manner, to prevent any delays.

2.4 Information Asset Owners (IAO)

IAOs are responsible for ensuring their information assets are compliant with this policy and relevant data protection legislation. To provide assurance to the SIRO that appropriate controls are in place a DPIA should be carried out for all new projects, systems and processes that include the processing of personal data. The IAO should ensure that the DPO is involved in the DPIA process.

2.5 Senior Information Officers (SIO)

Director of College Operations and Directors of Professional Services have the responsibility of overseeing compliance and developing good data protection practice within their designated areas. They should ensure any new processing of personal data, or any significant changes within their area has an identified IAO, is assessed to identify if a DPIA is required and the that the DPO is consulted, in a timely manner, in all issues relating to the protection of personal data.

2.6 Senior Information Risk Owner (SIRO)

The University Registrar & Secretary also holds the role of SIRO. DPIAs provide the SIRO with assurance that the processing of personal data is carried out in a managed and secure way. The SIRO is responsible for approving a DPIA where significant risks to the University have been identified.

2.7 Data Protection Officer (Information Governance Manager)

In accordance with the GDPR the University has appointed a Data Protection Officer (the Information Governance Manager) to carry out the DPO role as defined in the legislation. The DPO assists the University by informing and advising on data protection obligations and providing advice regarding DPIAs, including monitoring the process and liaising with the ICO were required.

3 Data Protection Impact Assessment Policy

3.1 What is a DPIA

3.1.1 A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

3.1.2 DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

3.1.3 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

3.1.4 A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

3.1.5 DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

3.2 When do we need a DPIA

3.2.1 A DPIA is a process to help identify and minimise the data protection risks of a project. There are a number of criteria that determine when a DPIA should be carried out within the University of Exeter. .

3.2.2 A DPIA must be done before beginning any type of processing which is “likely to result in a high risk”. This means that although the actual level of risk has not been assessed, screening for factors that point to the potential for a widespread or serious impact on individuals must take place.

3.2.3 The GDPR says we must do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

3.2.4 The ICO also requires us to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’);
- track individuals’ location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual’s physical health or safety in the event of a security breach.

3.2.5 The University of Exeter requires all projects to review if a DPIA is required. A DPIA must be completed for all projects where one or more of the following applies:

a) involves the collection of new information about individuals

b) using information about individuals for a purpose it is not currently used for, or in a way it is not currently used

c) involves you using new technology that might be perceived as being privacy intrusive

d) may result in you making decisions, or taking action against individuals in ways that can have a significant impact on them

e) involves information about individuals of a kind particularly likely to raise privacy concerns or expectations

f) require you to contact individuals in ways that they may find intrusive

g) you are required to have this work signed off by the Data Protection Officer

If there is uncertainty regarding whether it is appropriate to carry out a DPIA for a specific project, by default the project team should err on the side of caution and ensure that one is performed. The Data Protection Officer may be consulted for clarification and further guidance may have been issued by the ICO, in which case this should be consulted also.

3.2.6 The University requires a DPIA to be completed or reviewed when a significant change is made to the way personal data is processed, such as a significant system upgrade.

3.1.4 The SIRO or DPO may request a DPIA is completed or reviewed following a security incident or breach, where a concern has been raised or where risks have been identified that require appropriate management.

3.1.5 The University does not require all legacy information assets to have a DPIA, however they are a useful tool to provide assurance of data protection compliance and can be implemented if it is appropriate.

3.3 At what point do we begin a DPIA

3.3.1 A DPIA should be started in the early stages of a project, before any processing has started and before a system has been identified. It should run alongside the planning and development process. This risk assessment helps identify controls to mitigate risks which should then be included in the requirements of a potential system. It may be useful at this point to have this reviewed by the DPO and/or the Head of IT Security for advice with both technical and non-technical requirements.

3.3.2 By starting a DPIA at the early stages risks and required controls to ensure legal compliance and security can be developed from outset, ensuring that privacy is developed by design. If a DPIA is left until late in a project there may be additional controls or manual work arounds needed to ensure compliance which can have substantial costs associated. A DPIA can also help with data minimisation, identifying information that may not be required and therefore minimising of cost of controls that may not be required.

3.3.3 The DPIA should be maintained throughout the project, be regularly reviewed and updated as work progresses to ensure new risks are included as soon as they are identified and controls are developed. Before the project goes live the DPIA should have a review by the DPO and Head of IT Security to ensure risks are managed to an appropriate level.

3.3.4 Where a project has high risks the DPIA may require the SIROs approval and the project manager should consult the DPO for further advice.

3.3.5 In the event that the results of the DPIA indicate a high level of risk that cannot be mitigated, the GDPR requires that the ICO is consulted before any processing takes place. The project manager should consult the DPO for advice and to facilitate this process.

The ICO has eight weeks (extendable by a further six weeks) to provide a judgement on the proposed processing and, if appropriate, give details of what must be done to make the processing acceptable under the GDPR, or ban the processing altogether.

3.4 How do we carry out a DPIA

The DPIA is a process to help you identify and minimise the data protection risks of a project. The DPO must be included in the process and can provide appropriate advice. The process is designed to be flexible and scalable. A light touch DPIA may be appropriate for low level processing where there is minimal risk.

The following documents should be used for the DPIA (guidance will be provided by the Information Governance Office):

- DPIA Report
- DPIA & Risk Register

These should be treated as living documents and recorded on the University Information Asset Register (IAR). The DPIA & risk assessments should be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves or introduction of new or changed IT services. Any significant changes may need to be readdressed to the Data Protection Officer.

Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

For further information on how the University assesses and manages risk, please see guidance available (you may also contact the University Risk & Compliance Officer):

http://www.exeter.ac.uk/cgr/insuranceauditandrisk/managing-reporting-risk/riskownerandriskfacilitatorresources/

Once the risk plan has been approved, the necessary actions should be tracked and completed as part of the day to day control of the project. In the event that any actions are delayed or cannot be completed, the implications of this to the protection of the personal data involved must be assessed by management and a decision taken about what to do next. If the untreated risk is sufficiently serious, this may have a significant impact on the viability of the project from a compliance viewpoint and advice should be sought from the DPO.

The process of DPIA is fundamental to the implementation of a successful project that handles personal data and is a significant part of the GDPR legislation. Only by fully understanding the risks to the data subject with regard to our processing of personal data can we hope to ensure that the controls we have in place are sufficient to provide an appropriate level of protection and meet the high standard expected of us.

By following this process the University of Exeter will go some way to ensuring that the risks that it faces in the day to day operation of its business are effectively managed and controlled.

4 Further Information and related policies

4.1 Related Policies and Guidance

This policy should be read in line with associated standards, policies and arrangements including:

Associated policies

- Privacy and Personal Data Protection Policy

University Guidance and Standards

- DPIA Report
- DPIA and Risk Register
- DPIA Guidance

External Resources

- ICO Guide to Data Protection Impact Assessments
- General Data Protection Regulation

For further information contact the University's Information Governance Office.