Data Protection Impact Assessment Policy

Author:	Mike Godfrey
Date:	12/10/2018
Document Security Level:	PUBLIC
Document Version:	1.0
Review Date:	Q1 2020

Data Protection Impact Assessment Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Mike Godfrey	GDPR	Final Draft	28/08/18			
1.0	Mike Godfrey	GDPR	Review Additions	01/10/18	Information Governance Committee		13/09/2018

Data Protection Impact Assessment Policy

Contents

Data Protection Impact Assessment Policy

Introduction

This policy sets out the University's systemic approach to DPIAs and forms part of the continuing compliance programme.

Purpose

The University of Plymouth needs to collect personal information to effectively carry out everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, students, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details and categorised personal data.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or statutory bodies. However, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), UK data protection laws and any other relevant data protection laws and codes of conduct (herein collectively referred to as "the data protection laws").

To ensure that the method of collecting the data and the storage within the database, all systems must be tested against the Document Protection Impact assessment (DPIA). DPIAs are required for assessing risks within the University of Plymouth's handling of personal data, especially when the processing poses a risk to the rights and freedoms of individuals. DPIAs also need to be revisited periodically and involve key players within your organization.

Definitions

Term	Definition
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her for the agreed purposes(s).
Cross Border Processing	The processing of personal data which: - o takes place in more than one Member State; or o which substantially affects or is likely to affect data subjects in more than one Member State
Data Controller	The Data Controller, natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Officer (DPO)	The person within the organisation who is responsible for ensuring that the organisation is compliant with the GDPR
Data protection laws	Means for the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 (*referred to as the Act*) and any other relevant data protection laws that the University of Plymouth complies with.
Data Subject	Is an individual who is the subject of personal data
GDPR	General Data Protection Regulation *(EU) (2016/679)*
Genetic data	Is personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Personal data	Is any information relating to an identified or identifiable natural person *('data subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Recipient	Is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Supervisory Authority	Is an independent public authority which is established by a Member State
Third Party	Is a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

Data Protection Impact Assessment Policy

Objectives

O1.1. To ensure that all risks are identified, and where possible eliminated, in the system that collects and stores personal data

Responsibilities

Role	Responsibility
Database Owner	For running the DPIA assessment
DPO	For ensuring the accuracy of the DPIA and recording the risks

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows the University to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA has to be done, how it should be carried out, It is the responsibility of the Database Owner to carry out a DPIA. As part of the process the Data Protection Officer must be consulted but it is not the Data Protection Officer who carries out the DPIA.

The impact assessment covers not only the protection of personal data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessments (PIA). The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project. Conducting a DPIA should benefit the University by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders. The term project is used in a broad and flexible way and means any plan or proposal. Examples of the types of projects that need a DPIA are:

- A new database storing and accessing personal data
- A data sharing initiative where two or more groups seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action (e.g. identifying students believed to be at risk)
- A new surveillance system such as CCTV
- A new database where the data is captured by form

When does a DPIA need to be done?

A DPIA should be completed as part of the initial phase of a project or at the point of creating an asset or process that involves personal data to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also, if there is a change to the risk of processing for an existing project/asset/process a review should be

carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks.

What do I need to do during a DPIA

This section is for those projects/assets/processes which includes the use of any personal data. If it involves the processing of personal data then you should start by completing the screening questions Part 1 on the DPIA form. If the answer to all these questions in 'No' then the remainder of the assessment does not need to be completed.

If the response to any of the screening questions is 'Yes' you should go on to complete Part 2 of the impact assessment form.

Once PT1 and if required PT2 is complete the DPIA form is attached to the asset in Flowz or stored in the project's documentation.

The DPIA Process

For further information about building privacy into a project/asset/process during the design stage please see Data Protection by Design and by Default in the Data Protection Policy document.

Once the risks are identified and outcomes and actions agreed it is important that that person leading the DPIA ensures that the necessary actions are implemented. As the project develops or the asset/process is launched and embedded, the privacy risks should continue to be assessed to ensure that adequate protections remain in place.

Once the DPIA process has been completed the outcomes will be recorded in a register maintained by the Data Protection Officer. The register will record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

Annex A: Example Form for DPIA

Asset/process/project title	
DPIA author	
Contact details	
Asset/process owner or Project Sponsor	
Faculty/Directorate	
Date created	
Date of last review	

Step One - Identify the need for a DPIA

Screening question	**Yes/No**
Does your data processing involve evaluating or scoring individuals (including profiling and predicting)?	
Does your data processing involve automated decision-making that may have a significant effect on an individual?	
Does your data processing involve systematic monitoring?	
Does your data processing involve special category or criminal personal data?	
Does your data processing involve processing personal data on a large scale?	
Does your data processing involve datasets that have been matched or combined?	
Does your data processing involve the personal data of vulnerable people?	
Does your data processing involve the use or application of innovative technological or organisational solutions?	
Does your data processing involve the transfer of personal data outside of the European Union?	
Does your data processing prevent individuals from exercising a right or using a service or contract?	

If ‘yes’ has been answered to any of the questions in step one, please proceed to step two as a full DPIA is required.

Step Two – Full DPIA

Context

Outline the asset/process/project – what is the purpose, what does it aim to achieve and what are the benefits.

Describe the information flows

Include the nature of the data, how it will be collected, accessed, stored, shared and retained including reference to IT. It may be useful to refer to a flow diagram or another way of explaining data flows.

Identify and assess the privacy risks

List key privacy risks

Risk ID	Privacy risk	Impact	Likelihood

Identify and approve controls

List the actions to be taken to reduce the identified risks and the expected outcome of those actions, e.g. is the final impact on individuals after implementing each solution a reasonable and proportionate response to the aims of the asset/process/project?

Risk ID	Control(s) identified	Expected outcome

Assign responsibility for implementing controls

Risk ID	Control(s)	Responsible officer	Deadline for implementation	Completion date

Reassess and accept the risks

Risk ID	Privacy risk	Impact after control	Likelihood after control	Risk accepted by

Consultation

Provide details of any consultation which has taken place
