St Georges, University of London

Privacy by Design Procedure

1 Introduction

1.1 The aim of this Procedure is to make sure that St Georges, University of London, (SGUL) has considered all aspects of confidentiality and data protection when procuring any new system, new business process or research project and that all staff involved are aware of their individual responsibilities.

1.2 The Information Asset Owner / Project Manager / Principal Investigator must ensure that the Data Protection Officer (DPO) is involved at the earliest possible stage so that they can provide advice on potential issues that may arise and ensure that the appropriate Information Security actions are taken and if required relevant clauses appear in any subsequent contract or service level agreement.

2 Introducing a New System

2.1 When introducing a new system the DPO & Head of IT Services must be informed so that an IT assessment can be carried out to establish the following:

2.1.1 the objectives of the new system / process.
2.1.2 the requirements / benefits.
2.1.3 the justification for a new system/process.
2.1.4 whether the requirements are achievable using existing systems.
2.1.5 the minimum hardware requirements needed to run the system e.g. network infrastructure, servers, PCs, software compatibility.
2.1.6 will the new system link to any existing systems?
2.1.7 resource needed to successfully implement the system.
2.1.8 support and maintenance is required.
2.1.9 how many people will use the system, how many sites?
2.1.10 will non-SGUL staff require access to the system/process?
2.1.11 what are the training implications?
2.1.12 what is the cost?
2.1.13 what are the estimated capital costs and on-going revenue costs?
2.1.14 will the project comply with privacy laws and regulations.?
2.1.15 How will the project affect the privacy of individuals?
2.1.16 Can the objectives be achieved whilst also protecting individual's privacy?
2.1.17 Is a Data Protection Impact Assessment (DPIA) required?

3 Introducing a New Business Process

3.1 The DPO is to be involved at the earliest possible stage to advise on potential IG issues.

3.2 When introducing a new process, an assessment must be carried out to establish:

3.2.1 Whether the changes could damage SGUL reputation
3.2.2 Will there be a risk to confidential information?
3.2.3 Will there be a risk to corporate information?
3.2.4 Is a DPIA required? (Section 4)

St Georges, University of London

Privacy by Design Procedure

4 Introduction of a new Research Project

4.1 When using information about people in health research in the UK, you need to be aware of the legal framework and how this might impact on what you intend to do. Guidance on using personal data in research can be found in the MRC ethics series: Using information about people in health research: https://mrc.ukri.org/documents/pdf/using-information-about-people-in-health-research-2017/

4.2 The DPO is to be involved at the earliest possible stage to advise on potential IG issues.

4.3 Is a DPIA required? (Section 5)

5 Data Protection Impact Assessment (DPIA)

5.1 Any personal data processing activity MUST comply with the requirements of the DPA 2018. A DPIA is a process which helps the appropriate information asset owner / Project Manager / Principal Investigator to assess privacy risks to individuals in the collection, use and disclosure of information. The DPIA must be carried out for a new system, new business process or research project, both internal and partnership, that require the collection and / or use of personal data.

5.2 Why should a DPIA be completed?

5.2.1 To identify privacy risks to individuals.
5.2.2 To identify whether a sharing agreement is required with partner organisations.
5.2.3 To identify privacy and Data Protection compliance liabilities for the organisation.
5.2.4 To protect SGUL's reputation.
5.2.5 To instil public trust and confidence in your project.
5.2.6 To avoid expensive, inadequate "bolt- on" solutions.

5.3 Initial Screening;

5.3.1 To assist staff in assessing whether a DPIA is required a DPIA initial screening questionnaire has been developed for use by staff at the outset of a new project / process. If the completed questionnaire identifies that a DPIA is required then the full DPIA Form must be completed. The DPO can provide advice and guidance on how to complete one.

5.4 When should I start a DPIA? DPIAs are most effective when they are started at an early stage of an implementation of a system, process or project when:

5.4.1 the project is being designed;
5.4.2 you know what you want to do;
5.4.3 you know how you want to do it;
5.4.4 you know who else is involved, and while you can still change your mind!
5.4.5 before decisions are set in stone;
5.4.6 Before you have procured systems or information assets;

5.4.7 Before you have signed contracts, Memorandums of Understanding or sharing agreements.

5.5 **Responsibility for completing the DPIA**

5.5.1 The IAO / Project Manager / Principal Investigator is responsible for completing the DPIA for a new system implementation, process or research project.

5.5.2 Once completed the DPIA must be submitted via the DPO to the Information Governance Steering Group (IGSG) for review.

5.6 **Consultation, Approval and Ratification Process for the DPIA**

5.6.1 The IGSG will review the DPIA for privacy risks associated with the project/system/process before ratifying the system/process.

5.6.2 Contentious DPIAs will be referred, as appropriate to either the Director JRES or the Executive Board for final approval.

6 Sharing Agreements

6.1 Where a new process involves routinely sharing personal identifiable data with another organisation a sharing agreement must be in place to establish:

6.1.1 What information will be shared – full details
6.1.2 The lawful basis for sharing the data
6.1.3 Who will have access to it
6.1.4 How access will be granted
6.1.5 Security of transfer
6.1.6 Location of the data
6.1.7 Retention period and disposal arrangements
6.1.8 Incident reporting procedures

6.2 The sharing agreement must form an appendix to the relevant contract. A signed copy of all sharing agreements must also be sent to the DPO.

7 Responsibilities for Developing Sharing Protocols

7.1 The Information Asset Owner or Principal Investigator is responsible for the development and implementation of Sharing Protocols that affect their information assets. They are to ensure that once they have implemented a Sharing Protocol that it is reviewed and updated annually.

7.2 The DPO is to be kept informed of any sharing protocol being used, when they are reviewed and any changes made to them.

8 Contracts

8.1 The application of the individual process outlined in this procedure must be considered in all contracts and service level agreements to ensure they have the appropriate Data Protection clauses.

8.2 It is vital that these processes, where appropriate, are completed before:

8.2.1 Decisions are set in stone;
8.2.2 Systems are procured;
8.2.3 Contracts/ Memorandums of Understanding/agreements are signed.