Data Protection Impact Assessment Policy

University College of Osteopathy

Core Documentation Cover Page					
Data Protection Impact Assessment Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Aug 2018 SMT	To reflect updated guidance published by the Information Commissioner's Office	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Aug 2020 Or in line with legislative changes
V2.0	Dec 2019 PRAG Chair	Administrative Amendments to reflect the new Committees' structure	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Aug 2020 Or in line with legislative changes
V3.0	May 2021 IGSSG	Minor Amendments to better reflect ICO guidance, update GDPR legislation changes following Brexit and updated DPIA Form using the sample template currently provided by the ICO.	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	May 2024 Or in line with legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	X
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

Data Protection Impact Assessment (DPIA) Policy

CONTENTS

1. Introduction 4
2. Data Protection Impact Assessments (DPIAs) 4
3. When to Conduct a DPIA 4
4. Privacy Risks 5
5. DPIA Risk Assessment 7
6. DPIA process 7
7. Conducting Effective DPIAs 8
8. Responsibilities for Conducting DPIAs 9
9. Reducing Privacy Risks 9
10. Consulting the ICO about DPIAs 9
11. Monitoring the DPIA 10
12. Communicating the Outcome of DPIAs to Stakeholders 10

Appendix 1: DPIA Template 11

Submitting controller details 11
Step 1: Identify the need for a DPIA – Screening Checklist 12
Step 2: Describe the processing 14
Step 3: Consultation process 17
Step 4: Assess necessity and proportionality 18
Step 5: Identify and assess risks 19
Step 6: Identify measures to reduce risk 19
Step 7: Sign off and record outcomes 20

Data Protection Impact Assessment Policy & Guidance

1. Introduction

1.1 This policy and guidance document ensures that a Data Protection Impact Assessment (DPIA) is undertaken routinely as part of the development of any new projects or reviews of current projects to consider any impacts on individuals' privacy appropriately and consistently from the outset and assures a 'privacy by design' approach to projects.

1.2 This policy and guidance document aligns with guidance published by the Information Commissioner's Office (ICO)[1].

2. Data Protection Impact Assessments (DPIAs)

2.1 A DPIA is a process that systematically and comprehensively analyses the processing of data and helps to identify and minimise data protection risks.

2.2 DPIAs consider not only compliance risks but broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus of a DPIA is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

2.3 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether remaining risks are justified and acceptable.

2.4 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 to demonstrate accountability and building trust and engagement with individuals whose data is being processed.

2.5 A DPIA may cover a single processing operation or a group of similar processing operations.

2.6 A DPIA is a project development requirement and serves the purpose of influencing project plans to mitigate privacy risks.

2.7 A DPIA is not a one-off exercise and but an ongoing process which should be reviewed regularly.

3. When to Conduct a DPIA

3.1 A DPIA should be carried out before any processing of personal data starts and carried out alongside the planning and development process of the project.

3.2 A DPIA should be carried out where types of processing are likely to result in high risk to individuals' interests. Subsequently, a DPIA must be carried out if the project plans to:

a) Use systematic and extensive profiling with significant effects;

b) Process special category or criminal offence data; or

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

c) Systematically monitor publicly accessible places on a large scale.

d) Use innovative technologies (in combination with any of the criteria from the European guidelines);

e) Use profiling or special category data to decide on access to services;

f) Profile individuals on a large scale;

g) Process biometric data (in combination with any of the criteria from the European guidelines);

h) Process genetic data (in combination with any of the criteria from the European guidelines);

i) Match data or combine datasets from different sources;

j) Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);

k) Track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);

l) Profile children or target marketing or online services at them; or

m) Process data that might endanger the individual's physical health or safety in the event of a security breach.

3.3 In cases where it is not clear whether a DPIA is required a DPIA should be carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law and demonstrates good practice.

3.4 A DPIA should be undertaken when it can have an effective impact on a project. Preferably this would be at an early stage in a project to ensure that potential problems are identified early and can be built into the project's development plan. This approach will also be time and cost efficient.

3.5 If a DPIA identifies a high risk where measures cannot be taken to reduce the risk, the ICO must be consulted. The ICO will review the DPIA and advise on whether the risk is acceptable, whether further action needs to be taken, advise whether the processing should not be carried out or may ban the processing. In these cases, the DPFIO will be the primary contact with the ICO.

4. Privacy Risks

4.1 A privacy risk is the risk of harm to an individual arising through an intrusion into privacy where "privacy" in this context relates to an individual's right of being let alone in the following respects:

a) Physical Privacy whereby an individual is able to maintain their own physical space or solitude and where intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

b) Informational Privacy whereby an individual is able to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others and where intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information, collection of information through the surveillance or monitoring of how people act in public or private spaces and through the

monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

4.2 Normally most DPIAs will be related to Informational Privacy where risks may arise due to personal information being:

a) Inaccurate, insufficient or out of date.
b) Excessive or irrelevant.
c) Kept for too long.
d) Disclosed to those who the person it is about does not want to have it.
e) Used in ways that are unacceptable to or unexpected by the person it is about.
f) Not kept securely.

4.3 For the purposes of a DPIA, Privacy Risks are categorised into three groups as shown in Table 1. These lists include examples and are not exhaustive.

4.4 Risks to individuals can be categorised in different ways and it is important that all types of risk are considered – these range from risks to physical safety of individuals, material impacts (such as financial loss) or moral (for example, distress caused).

TABLE 1: DPIA PRIVACY RISK CATEGORIES & POSSIBLE RISKS

Category	Possible Risks
1. Risks to Individuals	Inadequate disclosure controls increase the likelihood of information being shared inappropriately. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. New surveillance methods may be an unjustified intrusion on their privacy. Measures taken against individuals as a result of collecting information about them might be seen as intrusive. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect. Identifiers might be collected and linked which prevent people from using a service anonymously. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk. If a retention period is not established information might be used for longer than necessary. If released could cause harm and distress to data subjects.
2. Corporate Risks	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. Problems which are only identified after the project has launched are more likely to require expensive fixes.

	The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business. Data losses which damage individuals could lead to claims for compensation.
3. Compliance Risks	Non-compliance with the Data Protection Act (DPA). Non-compliance with the General Data Protection Regulations (GDPR). Non-compliance with the Privacy and Electronic Communications Regulations (PECR). Non-compliance with sector specific legislation or standards. Non-compliance with human rights legislation.

5. DPIA Risk Assessment

5.1 The focus of a DPIA is on identifying any potential harm to individuals and to what extent by assessing the risks the processing poses to individuals' interests and freedoms.

5.2 Risks assessed by a DPIA include those that could lead to physical, material or non-material damage, especially where the processing of individuals' data may lead to:

a) Identity theft or fraud.

b) Discrimination.

c) Financial loss.

d) Reputational damage.

e) Loss of confidentiality.

f) Unauthorised reversal of pseudonymisation.

g) Significant economic or social disadvantage.

h) Loss of public trust.

i) Instances where individuals may be deprived of their rights and freedoms.

j) Instances where individuals are prevented from exercising control over their personal data.

5.3 A DPIA assesses whether the risk of the data processing is likely to result in "high risk" by considering both the likelihood and severity of the potential harm to individuals.

6. DPIA process

6.1 The DPIA process consists of the stages described in Figure 1.

6.2 The advice of the Data Protection & Freedom of Information Officer must be sought when you conduct a DPIA.

6.3 Individuals and stakeholder should be consulted throughout the DPIA process as identified in the DPIA.

6.4 The DPIA should be undertaken following the stages described in Figure 1.

6.5 The DPIA template provided in Appendix 1 should be used to record the progress and outcomes of each stage in order to ensure that the process is consistent for all projects, that all privacy risks are carefully considered and that those affected by the project are provided with the opportunity to give their feedback.

6.6 A DPIA must be undertaken before any type of processing that is likely to result in high risk.

FIGURE 1: THE STAGES OF A DPIA

7. CONDUCTING EFFECTIVE DPIAS

7.1 An effective DPIA requires a good understanding of the relationship between an individual and the organisation within the context of the project being developed including the consideration of:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people.

7.2 This means seeing the project from the perspective of those whose privacy may be at risk to enable the project to be designed to minimise privacy risks and around their legal rights and expectations.

7.3 Relevant legislation will also therefore need to be considered to ensure that the DPIA is effective, including:

- The Data Protection Act 2018 (DPA)
- The UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998 (HRA)

8. Responsibilities for Conducting DPIAs

8.1 The project manager / head of department is responsible for conducting a DPIA in liaison with the UCO's Data Protection & Freedom of Information Officer (DPFIO).

8.2 The DPFIO should also be consulted if a new project is being considered or developed to advise on whether a DPIA is needed.

9. Reducing Privacy Risks

9.1 There are many different steps which can be taken to reduce a privacy risk. Some of the more likely measures include amongst others:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

10. Consulting the ICO about DPIAs

10.1 If the DPIA identifies a high risk and measures cannot be put in place to reduce that risk the ICO must be consulted before the processing of that data can begin.

10.2 If a DPIA needs to be consulted on by the ICO, the DPFIO shall act as the contact point between the UCO and the ICO.

10.3 The UCO shall act on the ICO's advice.

11. MONITORING THE DPIA

11.1 DPIAs shall be kept under review and revisited when necessary, for example if the type of data being processed changes or the purpose for the data processing changes.

11.2 DPIAs shall be reviewed at least annually to ensure that any privacy impact risks are revisited and amended where necessary.

11.3 It shall be the responsibility of the project manager / head of department in liaison with the DPFIO to undertake the review of the DPIA, the outcome of which shall be considered by the Information Governance & Information Security Steering Group and noted by the Senior Management Team.

12. COMMUNICATING THE OUTCOME OF DPIAS TO STAKEHOLDERS

12.1 Where a DPIA has been completed a summary report informing stakeholders of the outcome may be published to stakeholders. This will inform them that a DPIA process was undertaken and what mitigations have been put in place to assure their privacy. DPIA summary reports may be published on the UCO's website or intranet as appropriate for the stakeholder.

APPENDIX 1: DPIA TEMPLATE

DPIA TEMPLATE

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

CONTENTS

Submitting controller details 11

Step 1: Identify the need for a DPIA 12

Step 2: Describe the processing 14

Step 3: Consultation process 17

Step 4: Assess necessity and proportionality 18

Step 5: Identify and assess risks 19

Step 6: Identify measures to reduce risk 19

Step 7: Sign off and record outcomes 20

SUBMITTING CONTROLLER DETAILS

Name of Controller	
Subject / Title of DPO	
Name of Controller Contact /DPO (delete as appropriate)	

STEP 1: IDENTIFY THE NEED FOR A DPIA – SCREENING CHECKLIST

To determine whether a DPIA needs to be undertaken review the following questions. If you answer "Yes" to any of the questions you will need to complete a DPIA.		
DPIA Screening Criteria	**Yes**	**No**
1. Does the project involve the processing of personal data?		
2. Does the project plan to carry out any other: a) evaluation or scoring? b) automated decision-making with significant effects? c) systematic monitoring? d) processing of sensitive data or data of a highly personal nature? e) processing on a large scale? f) processing of data concerning vulnerable data subjects? g) innovative technological or organisational solutions? h) processing that involves preventing data subjects from exercising a right or using a service or contract?		
3. Will the processing use systematic and extensive profiling or automated decision-making to make significant decisions about people?		
4. Will the processing involve special-category data or criminal-offence data on a large scale?		
5. Will the processing systematically monitor a publicly accessible place on a large scale?		
6. Will the processing use innovative technology in combination with any of the criteria in the European guidelines?		
7. Will the processing use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?		
8. Will the project involve profiling on a large scale?		
9. Will the project involve the processing biometric or genetic data in combination with any of the criteria in the European guidelines		
10. Will the processing include combining, comparing or matching data from multiple sources?		
11. Will the project process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines?		
12. Will the project process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines?		
13. Will the project process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?		
14. Will the project process personal data that could result in a risk of physical harm in the event of a security breach?		
15. Does the project change the nature, scope, context or purposes of our current processing?		

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

STEP 2: DESCRIBE THE PROCESSING

1. Describe the nature of the processing by answering the following questions:
a) How will you collect the data?
b) How will you use the data?
c) Who will have access to the data?
d) Will you be sharing the data with anyone? Who? Where? Why?
e) Will you be using any data processors? Who? Where? Why?
f) Is a Data Sharing Agreement needed?
g) If the data is being transferred outside of the UK is this covered by an adequacy decision, appropriate safeguards, or exemption?
h) How long will you keep the data for?
i) How will you delete the data?
j) How will you store the data?
k) What security measures will be / are in place to keep the data secure?
l) Will any new technologies be used to process the data?
m) Will you be using any novel types of processing?
n) Referring to Step 1, what screening criteria identify that the process is likely to be high risk?
o) Have you produced and attached a data flow map for this processing?

2. Describe the scope of the processing by answering the following questions:
a) What is the nature (type and variety) of the personal data that will be processed?
b) Will the data include any special category or criminal offence data?
c) How much data will you be collecting and using?
d) How often will you be collecting the data?
e) How many individuals are / will be affected?
f) How long will the data processing be in effect for?
g) What geographical area(s) does the processing cover?
3. Describe the context of the processing by answering the following questions:
a) What / who is the source of the data?
b) What is the nature of your relationship with the individuals?
c) Would the individuals expect you to use their data in this way?
d) Do the individuals include children or other vulnerable groups?
e) How much control will individuals have over their data?
f) Do you have any previous experience of this type of data processing?

g) What is the current state of technology in this area?
h) Are there prior concerns over this type of processing or security flaws?
i) Is the processing novel in any way?
j) Are there any current issues of public concern that you should factor in?
k) Does the processing comply with any UK GDPR codes of conduct (once any have been approved under Article 40) or UK GDPR certification schemes?
l) Have you have considered and complied with relevant codes of practice?
4. Describe the purposes of the processing by answering the following questions:
a) What do you want to achieve by processing this personal data? What are your legitimate interests?
b) What is the intended effect on individuals?
c) What are the benefits of the processing – for you, and more broadly for society as a whole?

STEP 3: CONSULTATION PROCESS

1. Consider how to consult with relevant stakeholders by answering the following questions: *You should seek and document the views of individuals (or their representatives) unless there is a good reason not to.*
a) Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so (for example, if consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable).
b) Who else do you need to involve within your organisation?
c) Do you need to ask your data processors to assist?
d) Do you plan to consult information security experts, or any other experts (for example, IT or legal experts, sociologists or ethicists)?
e) Do you need to carry out a more general public consultation process, or targeted research (for example, if the DPIA covers a plan to collect the personal data of individuals you have not yet identified)? This could take the form of market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

1. Describe compliance and proportionality measures, in particular:
a) What is your lawful basis for processing?
b) Does the processing actually achieve your purpose?
c) Is there another way to achieve the same outcome?
d) How will you prevent function creep?
e) How will you ensure data quality and data minimisation?
f) What information will you give individuals?
g) How will you help to support their rights?
h) What measures do you take to ensure processors comply?
i) How do you safeguard any international transfers?

STEP 5: IDENTIFY AND ASSESS RISKS

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

STEP 6: IDENTIFY MEASURES TO REDUCE RISK

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

STEP 7: SIGN OFF AND RECORD OUTCOMES

Item	Name/position/date	*Notes*
DPIA completed by:		
DPIA signed off by Senior Manager:		
Measures approved by IGSSG:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by IGSSG:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:		*The DPO should also review ongoing compliance with DPIA*