DATA PROTECTION

GUIDANCE SERIES – 006

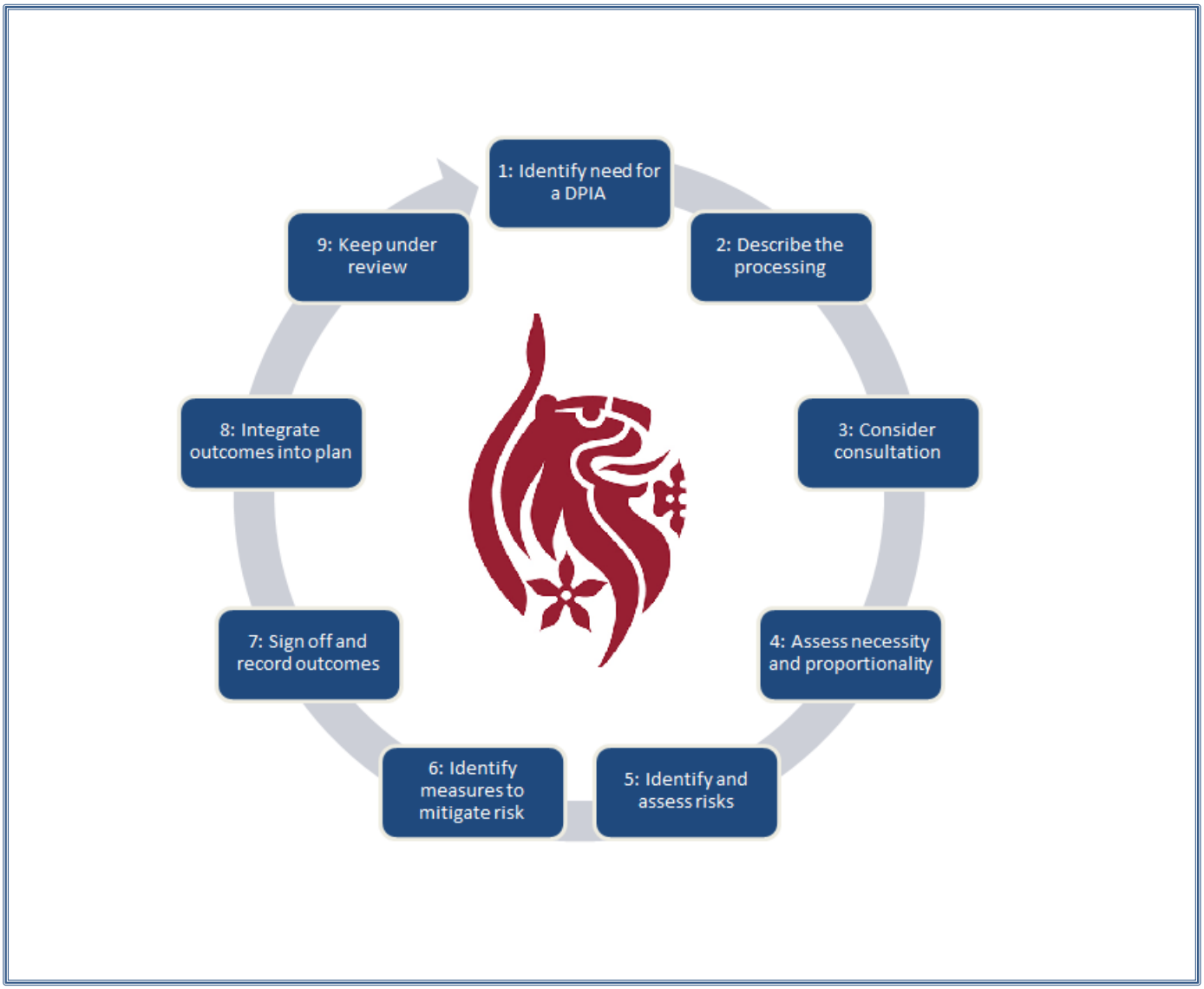
Data Protection Impact Assessment (DPIA)

This document sets out how to undertake a DPIA. This is an important document as it demonstrates our accountability with the GDPR. We must be able to demonstrate our compliance and this is what a DPIA does,

A DPIA is a tool that is used to identify and reduce the data protection risks of processing activities. This helps us to design more efficient and effective processes for handling personal data. This helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational and financial damage which might otherwise occur.

It is all about taking a 'data protection by design and default' approach, considering data protection and privacy issues upfront in everything we do. This ensures that we comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

CHECKLIST



Identify a Need

A DPIA screening checklist must be completed where you are undertaking a change which will impact upon personal data (change the way it is handled, new processor etc).

A DPIA must be carried out whenever there is a change that is likely to involve a new use; or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset is being introduced. Though a DPIA will be required where new IT systems or support services are to be procured.

The screening checklist will enable us to identify whether or not we will require you to undertake a DPIA. A completed screening checklist is to be sent to dataprotection@dmu.ac.uk.

Describe the Processing

The description must include the a) **nature**, b) **scope**, c) **context** and d) **purposes of the processing**.

This is often referred to as information flows, where in summary:

- describe the collection, use and deletion of personal data ; and
- identify individuals who are likely to be affected by the project.

You may wish to include accompanying documents such as a flow diagram or a similar method of describing data flows, a stakeholder map or similar.

Nature

Is about:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

Scope

The scope of the processing is what the processing covers. This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

If your change involves contracting to a third party processor, some of this information also forms part of the contract with that third party processor.

Context

Context is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern; and
- Whether you have considered and complied with relevant codes of practice.

Purpose

The purpose of the processing is the reason why you want to process the personal data. This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole.

Consider Consultation

We need to consult with all relevant internal stakeholders, in particular anyone with responsibility for Information Security. We are also required to consult with external stakeholders, who include potential contractors who may process information.

Where it is not appropriate to consult individuals then this is to be recorded as part of the DPIA, with a clear explanation. Examples would be where we might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

Assess Necessity and Proportionality

We need to prove that our plans help to achieve our purpose, but also looking for other reasonable ways to achieve the same result. There is also a need for continuous improvement – merely like for like change is not sufficient, we have to show improvement. This is probably the most important aspect of the DPIA as it directly links to the GDPR principles.

Our DPIA form includes details of how we ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, we have included the relevant details of:

- your lawful basis for the processing;

  Principle 1 (a), from the GDPR Article 5 - Lawfulness, fairness and transparency

  What is the legal basis for processing?
  How will individuals be told about the use of their personal data?
  Do you need to amend your privacy notices?
  If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

- how you intend to provide privacy information to individuals;

  Principle 1 (a), from the GDPR Article 5 - Lawfulness, fairness and transparency

  How will individuals be told about the use of their personal data?
  Do you need to amend your privacy notices?

- how you will prevent function creep;

  Principle 1 (b), from the GDPR Article 5 – Purpose Limitation

  Does your project plan cover all of the purposes for processing personal data?
  Have potential new purposes been identified as the scope of the project expands?

- how you intend to ensure data minimization;

  Principle 1 (c), from the GDPR Article 5 – Data Minimisation

  Adequate – sufficient to properly fulfil our stated purpose
  Relevant – has a rational link to that purpose; and
  Limited to what is necessary – we do not hold more than our need for that purpose.

- how you intend to ensure data quality ;

  Principle 1 (d), from the GDPR Article 5 – Accuracy
  If you are procuring new software does it allow you to amend data when necessary?
  How are you ensuring that personal data obtained from individuals or other organisations is accurate?
  How will you maintain accuracy over time?

- how long do you intend to retain information for;

  Principle 1 (e), from the GDPR Article 5 – Storage Limitation

  What retention periods are applicable for the personal data you will be processing?
  Are you procuring software which will allow you to delete information in line with your retention periods?
  Could you set the software to automatically delete information on its disposal date?

- how will you ensure it will be kept secure?

  Principle 1 (f) from the GDPR Article 5 – Security

  Do the new or current systems provide adequate protection against the security risks you have identified?
  What training and instructions are necessary to ensure that all staff know how to operate a new system securely?
  Are you limiting staff access to those who require it?
  If you are transferring data, how will this be done securely?
  How will you protect the data at rest?

- how you implement and support individuals rights;

  GDPR Articles 12-23 – Individual Rights

  How can you take account of rights requests/objections?
  With the lawful basis you have chosen – can you comply with the rights?

- measures to ensure your processors comply *(Art 26 – 30*); and

  GDPR Articles 26 – 30 - Joint Controllers… Processor… Records of Processing Activities
  This is relatively straightforward and requires you to understand the proposed relationship between the two parties and the type of agreement required. Please refer to Guidance 007- Contracts.

- safeguards for international transfers (Art 44 – 49).

  GDPR Articles 44 – 49 – Transfers… Safeguards... Derogations

  Where data is to be transferred outside of the EU/EEA, please refer to Guidance 007- Contracts

Identify and Assess Risks

We are required to consider the potential impact on individuals and any harm or damage that might be caused by our processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- reidentification of pseudonymised data; or
- any other significant economic or social disadvantage

We must make an 'objective assessment' of the risks. You might find it helpful to use a structured matrix such as the one below to think about likelihood and severity of risks.

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Identify Measures to Mitigate Risks

Against each risk identified, we need to record the source of that risk. We should then consider options for reducing that risk:

- are new systems sufficient and is there training ;

  Principle 1 (f), from the GDPR Article 5 – Integrity and Confidentiality

  Do the new systems provide adequate protection against the security risks you have identified?
  What training and instructions are necessary to ensure that all staff know how to operate a new system securely?
  If you are transferring data, how will this be done securely?
  How will you protect the data at rest?

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological and / or organizational measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

The above is not an exhaustive list, and if you are in doubt you must contact dataprotection@dmu.ac.uk.

Concluding the DPIA

We should record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to contact the Data protection Officer at DMU (via the Information Governance Team).

The DPIA is a 'living' process, and you will need to manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and reassess if anything changes. For example:

- Assess new risk
- Identification of a security flaw
- New technology
- New public concern