UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 16

Data Protection Impact Assessment (DPIA) Quick Guide (GUIDANCE FOR MANAGERS/PRINCIPAL INVESTIGATORS)

What is a DPIA?

A Data Protection Impact Assessment (formerly known as a Privacy Impact Assessment) is a tool to help identify, manage, and minimise the data protection risks of a new project or initiative.

Why are DPIAs required?

- They can help identify risks and fix problems at an early stage before new data processes have been embedded. This can also bring associated financial benefits as a result of identifying problems early leading to simpler and less costly solutions.
- They are also an aid to transparency and can help reassure individuals that you are protecting their interests and reducing any negative impacts as much as possible.
- They support our requirement to embed data protection at the core of our business processes (known as data protection by design and default).
- They are a legal requirement for any data processing that is likely to result in high risks to the rights and freedoms of individuals.
- They are an essential part of our accountability obligations in documenting how personal data is used (data processing).
- Failure to carry out a DPIA can leave the University open to enforcement action by the Information Commissioner's Office (ICO) including fines.

When do I need to consider a DPIA?

You need to complete a DPIA when your data processing will result in a high risk to an individual's rights and freedoms. A "high risk" is when there is a chance of harm to an individual, because the risk is likely or the potential harm is severe.

You **MUST** do a DPIA if you are doing any of the following:

- Systematic or extensive profiling with significant effects (such as profiling an individual based on aspects of their personal life and taking a significant action based on this).
- Large scale use of personal data.
- Processing involving data relating to criminal offenses.
- Public monitoring (such as the use of CCTV).

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 16

What types of processing are likely to involve higher risks?

- Using new technologies
- Automated decision making leading to the denial of a service.
- Combining, comparing or matching personal data from multiple sources
- Processing where the individual has not been made aware of the data
- Tracking geolocation or behaviour including in the online environment
- Large scale profiling
- Biometrics
- Targeting of children or vulnerable adultsadults
- Risk of physical harm
- Genetic data
- Special Category Data

What does carrying out a DPIA involve?

Step	What to do
Step 1: Identify the need for a DPIA	In the first instance do contact Information Assurance Services for advice. Check whether you'll require a DPIA based on the mandatory requirements above. Complete a screening questionnaire in OneTrust
Step 2: Describe the processing	Describe: • The nature of processing – what you plan to do with the data • The scope of the processing- what the processing covers and type of data • The context of processing – what the wider picture is, impact and what the processing is trying to achieve • The purpose of processing – why you want to process personal data and is processing personal data necessary
Step 3: Consider consultation	You should seek the views of individuals unless there is a good reason not to. If you choose not to you should clearly document this decision. If your DPIA decision (i.e. to carry out data processing) is at odds with the views of individuals (i.e. it may require sharing data to third parties) you need to document the reason why this decision was made. You may also need to consult other parties including a data processor (e.g. Does the data processor have appropriate technological controls in place to manage the storage and processing of your data). IT Services will be a stakeholder involved in this process (particularly for processing involving an IT system).

Step 4: Assess necessity and proportionality	Consider whether your plans help to achieve your purpose and whether there might be any other reasonable ways to achieve the same result.
Step 5: Carry out a risk assessment to include the identification of risks, risk mitigation measures, recording outcomes	Consider the impact on individuals and any harm or damage that might be caused by the processing – this could be physical, emotional or material. You should include an assessment of security risks and the potential impact of a breach (including its likelihood and severity). For each risk you should record the source of the risk and what options are available for reducing that risk. This might include: not collecting some types of data; reducing the retention period of the data; training staff; using a different technology; or anonymising or pseudonymising where possible. The Project Lead/Principal Investigator should document what additional measures you plan to take; how the risks have been addressed; the overall residual risk after taking risk reduction measurers; whether you need to consult the ICO. Once documented this should be shared with IAS to confirm whether processing is compliant and can go ahead.
Step 6: Integrate outcomes into project plan	The Project Lead/Principal investigator should: • Identify who is responsible for any associated actions • Monitoring on-going performance of the DPIA • Consult the Information Assurance Services and the Data Protection Officer • Publish the DPIA where possible (or appropriate) to aid transparency and accountability (you can redact an commercially sensitive information) • Embed the findings of a DPIA into a Data Management Plan (if the activity relates to a research activity).
Step 7: Keep your DPIA under review	Keep it under review on an annual basis and update it if there is a substantial change to the processing.

To complete a DPIA please visit the following link for the current process.

Further information:

- If you need further information or have questions about DPIAs please email the Information Assurance Services team on ias@le.ac.uk
- Further guidance on preparing for the Data protection Act 2018/General Data Protection Regulation is available at: https://www.le.ac.uk/gdpr