General Data Protection Regulations
Information Governance File Note

Date: August 2017
Name: Amanda Holloway, Information Governance Lead
Subject: **Data Protection by Design and Data Protection Impact Assessments (DPIAs)**

It has always been good practice to adopt privacy by design approach and to carry out a Privacy Impact Assessment (PIA). However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

What is 'privacy by design'? Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

The ICO would like to see more organisations integrating core privacy considerations into existing project management and risk management methodologies and policies.

NHS organisations are required to have PIAs in place in order to comply with the current Information Governance Toolkit. Partner organisations, for example local authorities, will now be required to do the same.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;

- where a profiling operation is likely to significantly affect individuals; or

- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. You should therefore

start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally? You should also familiarise yourself now with the guidance the ICO has produced on PIAs https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
as well as guidance from the Article 29 Working Party
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

Example PIA Template(s) and guidance documentation exists locally for use by Cambridgeshire and Peterborough Information Sharing Framework colleagues. Each organisation will need to embed the required processes to satisfy their own internal governance requirements.

Which Provisions:

GDPR Articles 35, 36 and 83 and Recitals 84, 89-96

What's new?

ICO's Data Protection definition:	**GDPR definition:**
Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. PIAs are an integral part of taking a privacy by design approach.	The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

What is a DPIA under GDPR?

Article 35 defines as:
Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
Recital: 75, 84, 89

Can we carry on as we are?

- Yes, but
- Re-name as DPIAs.
- Must check whether current PIA processes meet the requirements of GDPR.
- Include section where high risk has been identified to consult and record ICO opinion.
- Ensure governance processes for sign off are robust.

Is a DPIA required every time?

NHS organisations are required to have PIAs in place in order to comply with the current Information Governance Toolkit. Partner organisations, for example local authorities, will now be required to do the same.
A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

• where a new technology is being deployed eg building new IT systems for storing or accessing personal data;
• where a profiling operation is likely to significantly affect individuals eg embarking on a data sharing initiative; or
• where there is processing on a large scale of the special categories of data or using data for new purposes.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

DPIA Checklists

The ICO has produced the following guidance on PIAs
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf