Meeting the Requirements

Data Protection Impact Assessments

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

A Data Protection Impact Assessment (DPIA) is a tool that is designed to help organisations identify, analyse and reduce data protection risks in relation to their processing activities. The UK GDPR introduced the requirement to complete a DPIA for processing likely to result in a high risk to individuals' interests. DPIAs also form an essential part of the accountability obligation under the UK GDPR.

Article 35 of the UK GDPR says:

> *"1. 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."*
>
> *"3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
>
> *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
>
> *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
>
> *(c) a systematic monitoring of a publicly accessible area on a large scale."*

A DPIA does not have to eliminate every risk posed by the processing, but it should help you to reduce the risk and establish if the level of risk is acceptable in relation to the anticipated benefit. By considering the data protection risks of the intended processing before it begins, it will also support compliance with the data protection by design and default obligation under UK GDPR.

DPIAs can also bring broader compliance benefits to the organisation, as they can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations. For example, they can determine the type of technical and organisational measures you need to put in place in order to ensure your processing complies with the data protection principles and can reassure individuals that the organisation is protecting their interests and have reduced any negative impact on them as much as you can.

The ICO page on 'Data Protection Impact Assessments' provides further guidance.

How do we reach Attainment Level 1?

The organisation should have a process embedded within its policies and procedures for identifying when a DPIA is required to be undertaken and how to undertake one.

A DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to the rights and freedoms of individual(s). However, it is good practice to undertake a DPIA when the process/project involves large-scale processing of sensitive personal information. A DPIA is not a one-off exercise and should be seen as an ongoing process and be regularly reviewed.

In addition to the individual leading on the process or project, you should also involve:

- the appointed DPO for the organisation;
- information security staff where appointed;
- relevant processors;
- where relevant, other experts or legal advisors;
- the views of the individuals unless there is a good reason not to.

Note: See 'Table One' for details on responsibilities for the DPIA.

Your DPIA must:

- begin before you start processing and run alongside the planning and development process;
- describe how and why you intend to use the personal information, 'Table Two' sets out the nature, scope, context and purposes of the processing;
- detail how you will ensure data protection compliance, 'Table Three' sets out to assess necessity, proportionality and compliance measures;
- consider the potential impact on individuals, 'Table Four' explains how you can identify and assess risks to individuals;
- identify any additional measures to mitigate those risks, 'Table Five' details some options for consideration to reduce likely risks.

There should be a clear DPIA policy and procedure which are easy for staff to locate. See 'Table Six' for the ICO's expectations on the policy and procedure.

The organisation should take a data protection by design and by default approach to managing risks and, as appropriate, you should build DPIA requirements into policies and procedures. See 'Table Seven' for the ICO's expectations.

Note: The ICO have produced detailed guidance on 'Data Protection Impact Assessments' including a sample 'DPIA template' which can be used or adapted.

An 'All Wales DPIA template' has also been developed by the Information Governance Management Advisory Group. This template is quite extensive therefore you should only complete the sections appropriate to your processing/project.

The organisation does not have to eliminate every risk; you may decide to accept a high risk because it is either not possible to mitigate or because the costs of mitigation are too high. The organisation's DPO should be consulted when developing a DPIA; they should be able to help with identifying the level of risk and assess the necessity and proportionality of the processing. They will be able to advise on compliance and any measures required to be undertaken and help inform and assist in the development of privacy information to meet specific needs of the project/service.

How do we reach Attainment Level 2?

DPIAs are an integral part of taking a 'privacy by design' approach and are a way for organisations to systematically and comprehensively analyse processing and help identify and minimise data protection risks. All staff should be made aware of the policy and procedures and the importance to undertake the DPIA process before the project or processing begins. Staff should be aware that by following the process, it will help the organisation demonstrate that appropriate measures have been taken to ensure compliance with the requirements of the UK GDPR.

DPIAs should be signed off by the nominated individual, with a record of the outcomes detailed in the DPIA Register. The ICO must be consulted if a DPIA identifies a high risk and the organisation can't take measures to reduce that risk. In such situations, processing can't begin until the ICO has been consulted. See 'Table Eight' for the ICO's expectations on DPIA risk mitigation and review.

Note: The ICO provides some examples of processing 'likely to result in high risk'

How do we reach Attainment Level 3?

The DPIA process and documentation should be reviewed regularly to ensure it remains appropriate for its intended use. It is good practice to regularly maintain a register for all completed and ongoing DPIAs. This will enable the organisation to keep track of the DPIAs they have undertaken and those which they have also been involved in. DPIAs should be reviewed every two years unless a change in process has been identified by either the DPO or project lead within that time.

Health Boards and Trusts should regularly report DPIA figures to the relevant Board/Committee to ensure appropriate assurance, governance and oversight.

Supporting Resources

All Wales Data Protection Impact Assessment (DPIA) Template - *A template DPIA for any proposed changes or projects that affect processing of personal data*

ICO: Data protection impact assessments - *Guidance on DPIA's*

ICO: Data Protection by Design and by Default – *The UK GDPR requires you to put in place appropriate technical and organisational measures*

ICO: The Accountability Framework - *Accountability is one of the key principles in data protection law*

ICO: Guide to the UK General Data Protection Regulation

ICO: Introduction to data protection

ICO: Children and the UK GDPR - *Practical guidance for organisations who are processing children's personal information*

The National Archives: Information Assurance

The National Archives: Managing information risks

Summary Requirement

Attainment Level	Summary Requirement
1	A process to facilitate completion of Data Protection Impact Assessments (DPIAs) to highlight potential risks for new projects/services is in place and any residual high risks are reported to the ICO. All DPIAs are collated to form a register and this is regularly maintained
2	A DPIA process is recognised and embedded throughout the organisation for existing processing of personal data and is formally signed off by a nominated person
3	DPIA documentation is regularly reviewed and compliance with the process is reported to the Management Team