Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit
IGDC • DHCW

Expectations Guidance Document

1.7 - Risks and DPIAs

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Risks and DPIAs section of the Welsh Information Governance Toolkit (WIGTK).

You will need to consider the processes the organisation has in place, along with your staff's awareness for this section.

The need to identify, assess and manage privacy risks is an integral part of accountability. Understanding the risks of the way you use personal data is central to creating an appropriate and proportionate privacy management framework. A Data Protection Impact Assessment (DPIA) is a key risk management tool, and an important part of integrating 'data protection by design and by default' across your organisation. It will help you to identify, record and minimise the data protection risks of projects.

Please note, in this section of the WIGTK you will be required to upload copies of the relevant policies if you have ticked that your organisation has them available.

Minimum Expectations

DPIA process

Staff within your organisation should be aware of the DPIA process, including:

- When a DPIA is required,
- The steps that need to be followed,
- Who to go to for advice and guidance on DPIAs, and
- Who finalises the DPIA within the organisation.

A DPIA should be undertaken where new processing, or the use a new technology/system is proposed. A DPIA must be undertaken where processing is likely to result in a high risk to individuals. This includes, monitoring publicly accessible places on a large scale, therefore, a DPIA must be completed for any surveillance systems in place, if this has not been completed prior to the implementation of the system, a DPIA should be completed in retrospect.

Commented [LN1]: I have added this in from the Tooltip notes

Article 35(3) of the UK GDPR sets out the types of processing that require a DPIA, this includes:

- The use of systematic and extensive profiling with significant effects;
- Processing special category or criminal offence data on a large scale; or
- Systematically monitor publicly accessible places on a large scale.

Additionally, the Information Commissioner's Office (ICO) offers an extensive list of examples of processing "likely to result in high risk".

The DPIA should take into account the nature, scope, context and purposes of the processing, and whether it is likely to result in a high risk to the rights and freedoms of individuals.

The DPIA should be undertaken by the controller, prior to the processing, and assess 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 risks.

Role of the Data Protection Officer (DPO)

Under the UK GDPR, you must appoint a Data Protection Officer (DPO) if:

- you are a public authority or body (except for courts acting in their judicial capacity),
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking), or
- your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

The appointed DPO must fulfil the requirements stated under Article 39 of UK GDPR including having expert knowledge of data protection law and practices. One of the tasks stipulated within Article 39 is:

> "to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35"

The DPO will need to provide advice on DPIAs and monitor their performance across the organisation.

DPIA Register

The organisation should maintain a DPIA register to help monitor and track the progress and outcomes of all DPIAs. This includes those completed and in progress as well as those which were started and then later withdrawn.

As a minimum, the register should include:

- Title
- Description
- Organisation Role
- Project Status
- Outcomes

Reviewing, finalising, and signing off DPIAs

The organisation's DPIA procedure should describe how and who should agree any risks identified in the DPIA.

The responsibility for completing DPIAs should be with a member of staff who has enough authority over a project to effect change.

DPIAs should be signed off by the nominated individual, with a record of the outcomes detailed in the DPIA Register. This should be detailed within the organisation's DPIA procedure.

Consulting the Information Commissioners Office (ICO)

Under Article 36 of UK GDPR, the ICO must be consulted if a DPIA identifies a high risk to the rights and freedoms of individuals, and the organisation cannot take measures to reduce that risk. In such situations processing cannot begin until the ICO have been consulted on the matter.

When to consult the ICO and how to do this should be detailed in the organisation's DPIA procedure.

For more information please see the ICO website - Do we need to consult the ICO? | ICO

Risk registers – HB/Trusts/SHAs only

The organisation should identify and manage information risks in an appropriate risk register.

This should include clear links between corporate and departmental risk registers and the risk assessment of information assets.

There should be formal procedures in place to identify, record and manage risks associated with information assets in an information asset register.

Risk Management Processes – HB/Trusts/SHAs only

The organisation should adopt a risk management process. The risk management process should include:

- Identification
- Risk appetite
- Escalation
- Assessment
- Actions
- Review

This formal policy should set out how the organisation and its data processors manage information risk and monitor compliance with the information risk policy.

Any risks associated with information assets should be recorded within the organisation's information asset register. The process for this should be outlined within the organisation's risk management policy or information asset procedure.

The board, or highest senior management level, has overall responsibility for data protection and information governance. Any high-level risks should also be reported to the senior management team within the organisation.

The organisation should have an effective process in place to ensure senior management are provided with regular updates on a variety of IG matters, including any risks.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Risk Management Processes – GPs and CPs only

The organisation should adopt a risk management process. The risk management process should include:

- Identification
- Risk appetite
- Escalation
- Assessment
- Actions
- Review

This formal policy should set out how the organisation and its data processors manage information risk and monitor compliance with the information risk policy.

Information Assets and Reporting to Senior Management

Commented [LN2]: Just added this title in here to split them up a little

Any risks associated with information assets should be recorded within the organisation's information asset register. The process for this should be outlined within the organisation's risk management policy or information asset procedure.

The board, or highest senior management level, has overall responsibility for data protection and information governance. Any high-level risks should also be reported to the senior management team within the organisation.

The organisation should have an effective process in place to ensure senior management are provided with regular updates on a variety of IG matters, including any risks.

DPIAs and Privacy Information

DPIAs are an integral part of taking a 'privacy by design' approach and is a way for organisations to analyse processing systematically and comprehensively, to help identify and minimise data protection risks.

DPIAs should take into consideration whether the processing is covered by the existing privacy information, or if there is a need to update, or create new privacy information for the project or service.

Review of Policies and Procedures

It is important to ensure that all DPIA policies and procedures are regularly reviewed to ensure they are kept up to date and adapted when required in line with current legislation and any changes within the organisation.

Publishing DPIAs – HB/Trusts/SHAs only

Although it is not a legal requirement to publish DPIAs, the organisation should consider the benefits of publication, which may include:

- demonstrating compliance
- building trust and confidence of service users

The ICO expects the organisation to have a DPIA review process.

If your organisation does publish DPIAs, you should ensure any sensitive details are removed as necessary.

Reporting DPIA Figures – HB/Trusts/SHAs only

The board, or highest senior management level, has overall responsibility for data protection and information governance.

Therefore, the organisation should have an effective process in place to ensure senior management are provided with regular updates on a variety of IG matters, including DPIA figures.