Ombwdsmon
Ombudsman
Cymru • Wales

Data Protection Impact Assessment Policy

Mae'r ddogfen hon hefyd ar gael yn y Gymraeg.
This document is also available in Welsh.

Contents

1. Purpose

1.1. The Public Services Ombudsman for Wales takes the privacy of personal data very seriously. We have measures in places to understand what personal data we hold and to ensure that it is adequately protected.

1.2. With so much information being collected, used and shared, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively.

1.3. Our obligations under the UK General Data Protection regulation (UK GDPR) require us to consider data protection and privacy issues upfront for any personal data we process. A Data Protection Impact Assessment (DPIA) is a tool to achieve this and is considered a key element of a 'Privacy by Design' approach. [1] Completion of a DPIA will assist us to identify and minimise our privacy risks to comply with our data protection obligations and meet individuals' expectations of privacy. This policy and associated guidance and forms sets out the key components involved.

1.4. This policy sits within the Public Services Ombudsman for Wales' (PSOW) information governance strategic framework.

2. Scope

2.1. This policy should apply to all PSOW staff (including permanent, contract and temporary staff and individuals or organisations contracted directly by PSOW).

3. What is a DPIA?

3.1. A DPIA is a process of systematically and comprehensively identifying data protection risks of a project, process or system. These risks can then be analysed to minimise or address the risk.

3.2. These risks may be legal, financial, reputational or compliance risks, but the focus should be on the risks to individuals, such as the potential for any significant disadvantage or harm. The DPIA must consider the likelihood and

[1] ICO DPIA Guidance

severity of any impact on individuals. A risk does not have to be eradicated but it must be reduced to a level that PSOW accepts.

3.3. It is an obligation under UK GDPR to conduct a DPIA for any processing that is likely to result in a high risk to individuals' interests. If after undertaking a DPIA the risk remains high and the risk cannot be mitigated, then the ICO must be consulted before the processing is started.

3.4. DPIAs should be embedded into organisational processes. PSOW has an Information Asset Register which lists the information assets we hold, and these are grouped by business function. A DPIA should be linked to an information asset and recorded within the Information Asset Register. A DPIA should not be a one-off assessment but one that is regularly reviewed.

4. Other Definitions

4.1. **Initiative** - any proposal considering change, for example a new policy, process, procedure, project, IT system or procurement activity.

4.2. **Privacy** – in its broadest sense the right of an individual to be free from intrusion.

4.3. **Information Asset** – is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. They have recognisable and manageable value, risk, content and lifecycles.[2]

4.4. **Information Asset Register** - is a list of information assets held by PSOW. The register enables us to understand and manage risks associated with each information asset.

4.5. **Personal data** - information which enables us to identify an individual, either from the information provided or when put together with other information which may be available. Personal data may also include special categories of personal data that are considered more sensitive and may only be processed in more limited circumstances.

[2] Information Asset factsheet, The National Archives, 2017

5. Roles and responsibilities

Role	IG Responsibility
All Staff	Any staff member who is involved in the development of a project, initiative and systems needs to be aware of this policy and to understand when a DPIA maybe required. They should keep the DPIA under review throughout the project and consult with the IGM.
Information Asset Owners (IAO)	IAOs are senior/responsible individuals working in a relevant business area. They need to understand and address risks to information assets they 'own' by understanding what information is processed in their business area, how and why. They must provide assurances to the SIRO on the security and use of information assets and that DPIAs are carried out for any new projects, systems and processes.
Role	**IG Responsibility**
Information Asset Assistants (IAA)	IAAs support IAOs in ensuring that policies and processes are followed, recognise actual or potential information security risks. They ensure that the information asset register is kept up to date and support the IAO in completing DPIAs.
Management Team (MT)	MT oversees compliance with information governance, security standards and this policy. They are responsible for approving PSOW's IG Strategic Framework and annual action plans which include the review of information assets identified within PSOW's Information Asset Register.
Information Governance Manager (IGM)	The IGM is the organisation's statutory Data Protection Officer (DPO) and is responsible for monitoring organisational compliance with data protection legislation including this policy. They are responsible for the implementation of this policy and must be consulted in relation to any DPIAs undertaken.
Chief Information Security Officer (CISO)	The COODOI is the CISO whose role is to ensure the security of the PSOW information, including cyber security and resilience of PSOW networks. Working with the SIRO and DPO to advise on how best to manage risk whilst exploiting

	technology to deliver the organisation's strategic objectives. The SIRO and CISO are responsible for approving a DPIA.
Senior Information Risk Owner (SIRO)	The CLADOI is the SIRO whose role is to lead a culture of good information management. They are responsible for ensuring that identified information risks are managed and management plans implemented. The SIRO and CISO are responsible for approving a DPIA.

6. Benefits of a DPIA

6.1. Whilst the completion of a DPIA is not a legal requirement, it is an effective way to demonstrate how personal data processing complies with the data protection legislation. The ICO may also ask whether a DPIA has been undertaken.

6.2. A DPIA ensures that the least privacy intrusive options are explored to minimise individuals in a negative way. It helps to identify what information needs to be included in a privacy notice, which aids transparency, making it easier to explain to individuals why their information is being used. This should lead to increased confidence about the way personal information will be processed.

6.3. Completing a DPIA in the early stages of an initiative will ensure privacy issues are identified early on. Most importantly, inappropriate solutions are not implemented that later need to be reversed, which could be costly.

6.4. Carrying out a DPIA should benefit PSOW through better policies and systems being produced and improving relationships with individuals.

7. The DPIA Procedure

7.1. The DPIA procedure comprises 8 steps.

- Identify the need for a DPIA.
- Describe processing and information flows.
- Consider consultation.

- Identify and assess risks.
- Identify mitigation measures.
- Sign off and record outcomes.
- Integrate outcomes into plan.
- Keep under review.

7.2. The time and resources dedicated to a DPIA should be scaled to fit the nature of the initiative.

8. When is a DPIA needed?

8.1. A DPIA may be needed for any initiative involving personal data processing. It should be undertaken from the start of a new initiative to ensure that potential problems are identified at an early stage, when addressing them will be simpler and less costly and the direction of work can be influenced. The DPIA should continue to be considered through to implementation.

8.2. It is important to also consider a DPIA for any proposed change to an existing initiative. A change to any existing process or system also includes the cessation of any activity or arrangement. For instance, when a contract comes to an end so that arrangements for the secure disposal or transfer of any data may be considered. For procurement activity the DPIA should be completed prior to tender to ensure all relevant privacy risks are considered when preparing tendering specifications.

8.3. A DPIA is required before beginning any processing that is 'high risk'. The DPIA procedure starts with checking whether the initiative involves any processing that automatically requires a DPIA or other factors which may indicate that the risk is likely to be high. For example, using an external supplier to process personal data.

8.4. If the outcome of the screening is that a DPIA is not needed the reason for this should be documented. It may be necessary to review this decision in the future. Even if a DPIA is not needed you may find the flow mapping and risk assessment tools beneficial for project management.

9. Undertaking a DPIA

9.1. Having concluded that a full DPIA is required, the DPIA Template should be completed. This explains what is required at each step. An explanation needs to be provided for any section not completed.

9.2. It is the responsibility of the lead of an initiative to identify the need for a DPIA and complete it.

9.3. **Describing processing and information flows.** This step involves describing the nature, scope, context and purpose of the processing:

- **Nature** – How the data will be collected, used, stored, deleted and shared with?
- **Scope** – The type of data involved and whether this includes special category or criminal conviction data. How much data will be collected and used and how long it will be kept? The number of people affected.
- **Context** – PSOW's relationship with the individuals. How much control they will have and whether they would expect us to use their data as proposed. Do they include children or other vulnerable groups?
- **Purpose** – Why is PSOW processing the data? What is the intended effect on individuals? What are the benefits for PSOW?

9.4. It may be helpful to use a flow diagram to map the information flows from the start of the process through to the conclusion of the processing. This allows for an effective assessment of privacy risks through the lifecycle of the processing.

9.5. **Consider consultation** to understand whether the processing is necessary and proportionate. You should consider seeking the views of individuals or their representatives who may be affected by the processing. It is important to consider consultation with internal and external stakeholders and anyone responsible for any part of the processing. It may be necessary to seek expert advice, such as legal and information security expertise.

There is no specific requirement to consult but it may help to identify and assess the data protection and other risks.

9.6. **Identify & assess risks** throughout the lifecycle of the processing. For instance, risks around the accuracy or security of the personal data and any unnecessary intrusion on individuals' right to privacy. There may also be risks to the organisation such as legal compliance, financial or reputational risks.

9.7. **Identify mitigation measures** to reduce or eliminate the risk, taking account of any costs and benefits and whether these may be appropriate. For example:

- Deciding not to collect certain types of data.
- Anonymising or pseudonymising the data where possible.
- Developing guidance or processes to avoid risks.
- Training staff.
- Using different technology or adding extra levels of security.
- Changing privacy notices so that individuals know what to expect.

9.8. **Sign off and record outcomes** from the risk assessment. It may not be possible to eliminate or reduce the risk so this needs to be recorded. Some risks, including a high risk may be considered acceptable given the benefits to the PSOW. However, the ICO must be consulted if the risk remains high and may be difficult to mitigate.

It may also be necessary to update the PSOW's Risk Register. The DPIA Template needs to be signed off by the Information Asset Owner. The IGM's advice should be documented and if you decided not to follow their advice the reasons for this must also be recorded.

9.9. **Integrate outcomes into plan** so that clear actions and action owners are identified. Action plans will need to be monitored through to implementation. It may be that this feeds directly into the project management documentation. It may be necessary to go through the DPIA cycle again and adjust the action plan.

10. Consultation with the ICO

10.1. The ICO must be consulted before going ahead with the processing where the residual risk is high, and it is not possible to reduce or eliminate the risk.

10.2. The processing cannot go ahead until the ICO has been consulted and it can take between 8 and 14 weeks for the ICO to respond.

10.3. The IGM will contact the ICO sending a copy of the DPIA.

11. Review of DPIAs

11.1. The DPIA should be kept under review and repeated if there is a substantial change to the nature, scope, context or purposes of the processing.

12. Disclosure and publication of DPIAs

12.1. Whilst it is not a legal requirement to disclose or publish completed DPIAs, disclosure or publication demonstrates accountability and transparency. It can provide trust and confidence in PSOW's processing of personal information.

12.2. Access to a DPIA may be requested under the Freedom of Information Act 2000 so may need to be disclosed unless an exemption applies.

12.3. Publication will need to be considered on a case-by-case basis ensuring that no sensitive information is disclosed. A decision regarding publication should be taken by the Information Asset Owner in conjunction with the Information Governance Manager, SIRO and CISO.

12.4. The IGM should be consulted before any decision to disclose or publish a DPIA is made.

13. Monitoring and Compliance

13.1. The effectiveness of this policy will be monitored by the Information Governance Manager with reports as required to Management Team.

13.2. As a principle of good practice DPIAs and other risk assessments may be reviewed whenever an information asset is reviewed to ensure that the PSOW's Information Asset Register is kept up to date.

13.3. The IGM in conjunction with IAOs and Management Team reviews information security incident trends to ensure that adequate controls are in place appropriate to any data protection risks. Reviews of any relevant DPIAs may be reviewed as a result.

14. Review of this policy

14.1. The policy will be reviewed every 3 years and will be published internally and externally.

15. Further information

15.1. PSOW's DPIA Process Guidance supports those staff undertaking DPIAs and provides step-by-step instructions for what is required throughout the process. A copy of the DPIA screening questionnaire and DPIA Template Form is included as well as an example of a completed DPIA.

15.2. Advice and guidance can be provided by the Information Governance Manager (IGM) and the IGM must be consulted during the DPIA process.

15.3. External resources:

- Data Protection Impact Assessments, ICO guidance.
- Detailed DPIA guidance from the ICO.