

---

## **Data Protection Impact Assessment Policy & Process**

## Contents

1. Purpose .....	3
2. Scope .....	3
3. Definitions.....	4
4. Roles and responsibilities .....	5
5. Benefits of a DPIA .....	6
6. The DPIA process .....	7
7. Questions about the process.....	9
8. Monitoring and review .....	10
9. Appendix A: Identifying the need for a DPIA.....	11
10. Appendix B: Describing the process and mapping the information flows	13
11. Appendix C: Considering consultation and identifying risks .....	15
12. Appendix D: Sign off and record outcomes .....	18

## 1. Purpose

- 1.1. This policy sits within the Public Services Ombudsman for Wales (PSOW) information governance framework.
- 1.2. A Data Protection Impact Assessment (DPIA) is a key element of data protection by design and by default.<sup>1</sup> The process helps to analyse, identify and minimise data protection risks of a project and demonstrate compliance with our data protection obligations. This policy and process sets out the steps involved.
- 1.3. It is an obligation under 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.
- 1.4. 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.
- 1.5. 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

## 2. Scope

- 2.1. This policy applies to any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity. It provides a process which will enable:
  - identification of the need to complete a DPIA through a set of screening questions,

---

<sup>1</sup> [ICO DPIA Guidance](#)

- the collection of sufficient information about an initiative to complete a DPIA and
  - privacy risks identified by the DPIA to be documented and considered.
- 2.2. The process should be followed from the start of an 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.
- 2.3. Although this policy is aimed at new initiatives, information asset owners may wish to use it as a tool to review existing arrangements identifying and addressing privacy risks as a continuous improvement activity.

### 3. Definitions

- 3.1. **Initiative** - any proposal considering change, for example a new policy, process, procedure, project, IT system or procurement activity.
- 3.2. **Privacy** – in its broadest sense the right of an individual to be free from intrusion.
- 3.3. **Data Protection Impact Assessment (DPIA)** – a process which assists us in identifying, minimising and addressing the privacy risks associated with any new initiative.
- 3.4. **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.<sup>2</sup>

---

<sup>2</sup> [Information Asset factsheet](#), The National Archives, 2017

- 3.5. **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.

### 4. Roles and responsibilities

- 4.1. The **Management Team** has overall responsibility for the strategic direction and governance of PSOW and that operational management complies with all legal, statutory and good practice guidance requirements.
- 4.2. The **Senior Information Risk Owner (SIRO)** is responsible to the Management Team for ensuring the information security assurance and risk management plan is implemented and reviewed and its effect monitored. The DPIA is one element of the management of information risk. Information risk needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.
- 4.3. **Information Asset Owners (IAOs)** and **Information Asset Assistants (IAAs)** are responsible for specific electronic or paper information assets (names detailed in the [Information Asset Register](#)). They are the first point of contact for the completion of a DPIA. They are also responsible for signing off privacy solutions and recording relevant risks in the appropriate risk register. The Information Asset Owner may delegate responsibility for this to the Information Asset Assistant.
- 4.4. The **Information Governance Manager (IGM)** is responsible monitoring internal compliance with the Data Protection Act 2018 and the General Data Protection Regulations in respect of any personal data processed by the PSOW.

This includes the arrangements required for communication and training as well as arranging monitoring of the policy. The IGM can provide advice about conducting a DPIA.

- 4.5. **All staff** must follow the requirements of this and related information governance policies. Particular care should be taken of the privacy impact of working with contractors.

### 5. Benefits of a DPIA

- 5.1. Whilst the completion of a DPIA is not a legal requirement, the ICO may often ask an organisation whether they have carried out a DPIA. It is an effective way to demonstrate how personal data processing complies with the data protection legislation.
- 5.2. We can increase public and employee confidence in the way we will use their information. An initiative which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.
- 5.3. A DPIA will demonstrate transparency and may make it easier to explain to individuals why their information is being used.
- 5.4. It will support our legal obligations under data protection legislation.
- 5.5. 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 have to be reversed, which could be costly.
- 5.6. Carrying out a DPIA should benefit PSOW through better policies and systems being produced and improving relationships with individuals.

## 6. The DPIA process

- 6.1. The DPIA process is flexible. There are seven steps in the process and an overview of these are set out below.
- 6.2. The time and resources dedicated to a DPIA should be scaled to fit the nature of the initiative.

1

**Identify the need for a DPIA.** Use the [screening questions](#) in appendix A, to determine whether you need to complete DPIA.

2

**Describe the processing and information flows.** Use the [form and flowchart tool](#) in appendix B to map the information flow from start to end. Explain what the initiative is, provide the context. Whose data is collected and what data is involved (personal / special categories of personal data)? Why do you need the data and who will you share it with? Explain the legal basis for the processing. How long will it be kept for?

3

**Consider consultation.** In order to consider whether the processing is necessary and proportionate you'll [need to consult](#) with relevant key internal and external stakeholders. You should work together to [consider the risks](#) (they may even identify others you have not identified) and mitigations. Can you achieve the same outcome in the least intrusive way possible? How will you ensure data quality and data minimisation? What information will you give to individuals? How will you ensure that their information rights are supported? What measures will you take to ensure processors comply? What action do you need to agree jointly with other data controllers? Will any of the data leave the UK, if so, how will you ensure you safeguard international transfers?

**4 Identify the privacy and related risks.** On the flowchart [mark the privacy and other potential hotspots](#) in the process. For instance, there will be some risks to individuals relating to the accuracy or security of the data and any unnecessary intrusion on their privacy. There may also be risks to the organisation such as legal compliance, financial or reputational risks. List these risks in the first column of the [risk assessment](#).

**5 Identify and evaluate solutions to manage risk.** Use the [risk assessment](#) to analyse the consequence or benefit of the risk. Explain how you could address each risk. Assess whether this action would eliminate or reduce the risk. It may be that we need to accept some level of risk. Are there additional actions that need to be taken such as need to consider any other actions to reduce the risk further?

**6 Sign off and integrate outcomes into a plan.** Use the [sign-off sheet](#) to record the decision-making process. The DPIA must be signed off by the Information Asset Owner. The risk register may also need to be updated. Use the action plan to monitor progress with any actions arising from the risk assessment. It may be that this feeds directly into the project documentation.

**7 Keep under review.** You need to keep the DPIA under review and repeat it if there is a substantial change to the nature, scope, context or purposes of the processing.



## 7. Questions about the process

### 7.1. **When should I consider the need for a DPIA?**

A DPIA should begin early in the life of an initiative and should continue to be considered through to implementation. It's important to consider a DPIA (starting with the [screening questions](#)) for any new initiative or when there is a proposed change to an existing process or system etc. 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.

### 7.2. **Who should conduct the DPIA?**

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

### 7.3. **How do I know whether a DPIA is needed or not?**

This starts with a series of [screening questions](#). If you answer 'yes' to any of the questions, then it will be necessary to complete the full DPIA.

### 7.4. **What do I do with the completed screening questions and/or DPIA?**

These should be sent to the Information Governance Manager who will store these within the [information asset register](#) for future reference.

Whilst it is not a requirement to publish completed DPIAs to our website, the ICO recommends that to so aids transparency. Publication will need to be considered on a case by case basis ensuring that no sensitive information is disclosed.

## Data Protection Impact Assessment Policy & Procedure

A decision regarding publication should be taken by the Information Asset Owner in conjunction with the Information Governance Manager and SIRO.

### 7.5. **Why do I need to describe the information flow?**

Understanding the information flows involved is essential to a proper assessment of privacy risks. Sometimes we focus on one aspect rather than considering the process holistically. Use the tools in appendix B(b) to help you [map the information flows](#) and the process involved from start to finish.

## 8. Monitoring and review

- 8.1. The effectiveness of this policy will be monitored by the Information Governance Manager with reports as required to the SIRO and Management Team. The policy will be reviewed on a biennial basis.



## Data Protection Impact Assessment Policy & Procedure

### DPIA screening questions

No	Question	No	Yes	Comments
1.	Will the project involve processing personal information and / or special categories of personal data?			
2.	Will the project involve the use of an external supplier to process personal data?			
3.	Will the project involve any data about vulnerable people who may be unable to easily consent or exercise their information rights, including objecting to the processing or requesting access to information?			
4.	Will the project involve transferring personal data outside of the UK?			
5.	Will the project involve collecting new personal data about people that we're not already collecting?			
6.	Will the information be shared with organisations or people we're not already sharing the information with currently?			
7.	Will information previously obtained be used for a new purpose?			
8.	Will the project involve using technology that may be considered intrusive e.g. biometrics, facial recognitions?			
9.	Will the project involve making decisions that would have a significant impact on an individual?			
10.	Will the project mean contacting individuals in ways that they may find intrusive?			
11.	Will the project involve collecting data from someone other than the individual who we have not directly provided a privacy notice to?			

## 10. Appendix B: Describing the process and mapping the information flows

Complete the information below and then use the tools to produce a high-level flowchart mapping the flow of information from the point it is obtained to the last step in the process. You don't need to describe every step just the key steps. The IGM can provide other flowcharts examples which you may find useful.

### a) Describing the processing

Explain what data is involved. Whose data is collected and what data is involved (personal / special categories of personal data)?

Why do you need this information? Explain the legal basis for the processing.

Could be one or more of the following:


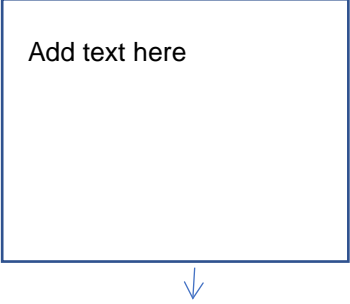
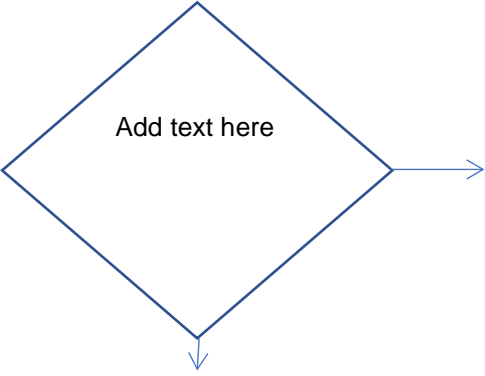
- a) Individual has consented or it is necessary for:
- b) Contract performance
- c) Complying with a legal obligation
- d) protecting vital interests of someone
- e) carrying out statutory duties [state legislation]
- f) pursuing legitimate business purposes

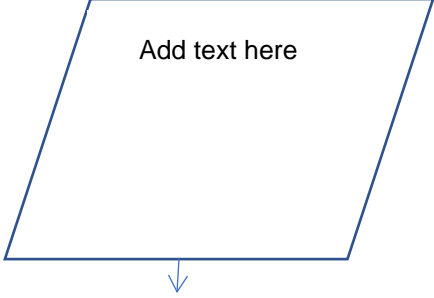
There are other grounds for processing special categories of personal data

How long will the information be kept for? Is this captured in the record retention schedule?

## b) Mapping the information flows

Using the tools below map a high-level flowchart describing the process from start to finish. You should also explain where the information has been obtained from and who it will be shared with. The IGM can provide other flowcharts examples which you may find useful.

	Use this symbol at the beginning and end of your flowchart.
	Use this symbol to explain a step in the process.
	Use this symbol when there's a decision point.

	<p>Use this symbol to explain when data is input to / output from the system</p>
---	--

### 11. Appendix C: Considering consultation and identifying risks

This section focusses on working with key stakeholders to consider whether the processing is necessary and proportionate. You should work together with them to identify potential risks. They may even identify others you have not. Use the [risk assessment](#) below to record the risks, consequences/benefits of the risk, risk level and mitigations.

You may find it helpful to refer to [section 6](#) of the DPIA Policy and Process, which sets out a series of questions for you to consider. This may assist your discussions with stakeholders about potential risks and mitigations with stakeholders.

#### a) Considering consultation

Who are the stakeholders you need to consult with and why?

### b) Identifying and recording risks

Use the flashpoint symbols below to indicate privacy issues which needs addressing on the flowchart that you created in appendix B. On the risk assessment add the relevant number and record the risk. There may be more than one risk per flashpoint so split them into 1a, 1b etc. The IGM can provide other flowcharts examples which you may find useful.



Copy and paste the flash symbol onto your flowchart. Change the number so you can refer to these in the risk assessment.



### c) Exploring risk consequences (or benefits)

On the [risk assessment](#) record the risks that you have identified and what the consequence (or benefit) is of that risk. Use the key to score the likelihood and impact of the risk.

### d) Identifying measures to manage risk

Complete the rest of the risk assessment by identifying measures that will eliminate or reduce the risks that you have identified. If further actions are required record these along with an action owner. It may not be possible to eliminate the risk and you may need to seek agreement about a level of risk acceptance.

### e) Recording outcomes

Outcomes and actions arising from the risk assessment need to be signed off by the Information Asset Owner(s). Use the sign-off table to record these. Actions arising from the risk assessment should feed into any project management documentation.



# Data Protection Impact Assessment Policy & Procedure

## Risk Assessment template

<b>[Name of project / initiative here]</b>	Version:	<input type="text"/>	Creation date:	<input type="text"/>	Document Owner:	<input type="text"/>	
Information Asset Owner:	<b>[Name]</b>			Approved date:	<input type="text"/>	Review due:	<input type="text"/>

Ref	The Risk What can happen and how it can happen	Consequence/Benefit of event happening	Inherent Risk			Mitigating Actions / Opportunities	Residual Score			Further Action Required	Action Owner	Risk Agreed by IAO? (Y/N)
			I	L	S		I	L	S			
1.												
2.												
3.												
4.												
5.												
6.												
7.												

Key		
<b>I</b>	<b>Impact</b>	Score 1-3 with 3 being significant impact and 1 being least impact
<b>L</b>	<b>Likelihood</b>	Score 1-3 with 3 being highly likely and 1 being least likely
<b>S</b>	<b>Score</b>	Multiply impact by likelihood to get score

## Data Protection Impact Assessment Policy & Procedure

### 12. Appendix D: Sign off and record outcomes

It's important to seek senior management sign off as to the appropriateness of the risk treatment. They will need to consider what level of risk can be tolerated and at what point the risk is unacceptable. It will be necessary to consider the viability of the initiative if the risk cannot be tolerated. It may also be worth consulting the ICO for advice.

Item	
<p><b>Risk assessment author comments:</b>                  [Include reference to integration of actions into project / action plan and outcomes from consultations – if there was any difference of opinions record these below.]</p>	
Name of author:	Date:
<p><b>Summary of Data Protection Officer (DPO) advice:</b> [Include reference to compliance, measures and whether processing can proceed.]</p>	
Name of DPO:	Date:
<p><b>Information Asset Owner (IAO) comments:</b> [Have measures been approved? Have residual risks been accepted? If the residual risk remains high have you consulted the ICO before proceeding? Have you accepted the DPO's advice? If not explain your reasons.]</p>	
Name of IAO:	Date:
<p><b>This DPIA will kept under review by:</b></p>	<p>Name: Review due:</p>