**Information Governance**

**Privacy by Design & by Default Procedure**

|  |  |
| --- | --- |
| **Date of Implementation:** | March 2019 |
| **Date of Current Issue:** | April 2021 |
| **Date of Review:** | April 2022 |
| **Responsible Officer:** | SIRO |
| **Validated By:** | BPAS Information Governance Board (IGB) |

Contents

[1. Introduction 3](#_Toc3965771)

[2. What is data protection by design? 3](#_Toc3965772)

[3. What is data protection by default? 3](#_Toc3965773)

[4. Who is responsible for complying with data protection by design and by default? 4](#_Toc3965774)

[4.1 BPAS Staff 4](#_Toc3965775)

[4.2 Data Processors 4](#_Toc3965776)

[5. How can we achieve privacy by design & by default? 4](#_Toc3965777)

[6. What is a Data Protection Impact Assessment? 5](#_Toc3965778)

[7. When is a DPIA required? 5](#_Toc3965779)

[8. How do data protection by design and by default link to data protection impact assessments (DPIAs)? 6](#_Toc3965780)

[9. Advice and support 6](#_Toc3965781)

[Appendix 1 – Data Protection Impact Assessment Screening Questions. 7](#_Toc3965782)

[1. DPIA awareness checklist 7](#_Toc3965783)

[2. DPIA screening checklist 7](#_Toc3965784)

[3. DPIA process checklist 9](#_Toc3965785)

[Appendix 2 – DPIA Template 10](#_Toc3965786)

[Step 1: Identify the need for a DPIA 10](#_Toc3965787)

[Step 2: Describe the processing 10](#_Toc3965788)

[Step 3: Consultation process 12](#_Toc3965789)

[Step 4: Assess necessity and proportionality 13](#_Toc3965790)

[Step 5: Identify and assess risks 13](#_Toc3965791)

[Step 6: Identify measures to reduce risk 14](#_Toc3965792)

[Step 7: Sign off and record outcomes 15](#_Toc3965793)

# 1. Introduction

Data Protection legislation requires BPAS to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.

Data protection by design is about considering data protection and privacy issues upfront in everything BPAS do. It will help BPAS ensure that the organisation is complying with the fundamental data protection principles and requirements.

This procedure is based on the key principles set out in the relevant legislation and on the Information Commissioners Guidance (ICO).

# 2. What is data protection by design?

Data protection by design is ultimately an approach that ensures BPAS consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

Essentially BPAS are required to:

* put in place appropriate technical and organisational measures designed to implement the data protection principles; and
* integrate safeguards into our processing so that we meet information legislation requirements and protect individual rights

# 3. What is data protection by default?

Data protection by default requires BPAS to ensure that we only process the data that is necessary to achieve our specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

BPAS have to process some personal data to achieve specific purposes, for example the provision of health care. Data protection by default means BPAS need to specify this data before the processing starts, appropriately inform individuals and only process the data BPAS need for purposes specified. It does not require BPAS to adopt a ‘default to off’ solution.  It requires BPAS to adapt its approach in accordance with the nature of the processing.

# 4. Who is responsible for complying with data protection by design and by default?

## 4.1 BPAS Staff

All BPAS staff are required to comply with data protection by design and by default. These requirements should be championed by:

* Information Asset Owners
* Information Asset Administrators
* System Owners
* The SIRO
* The DPO
* The Caldicott guardian

## 4.2 Data Processors

If BPAS use another organisation to process personal data on our behalf, then that organisation is a data processor.

We cannot rely on data processors to assist BPAS with in satisfying our data protection by design obligations; however BPAS must only use processors that provide sufficient guarantees to meet the data protection legislation requirements.

# 5. How can we achieve privacy by design & by default?

There are several steps that BPAS can take to ensure that we meet our obligations, including but not limited to:

* A proactive approach to data protection and anticipating privacy issues and risks before they happen
* Raising awareness
* Ensuring that data protection is a standing item on senior management and operational meetings
* Design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.
* Embed data protection into the design of any systems, services, products and business practices, ensuring that data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services
* Put in place strong security measures from the beginning, and extend this security throughout the ‘data lifecycle’ – i.e. process the data securely and then destroy it securely when it is no longer needed.
* Ensure that whatever business practice or technology we use operates according to its premises and objectives, and is independently verifiable.
* Privacy notices - ensuring transparency to individuals, such as making sure they know what data we process and for what purpose(s).
* Completing Data Protection Impact Assessments in good time

# 6. What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. BPAS must do a DPIA for processing that is ***likely to result in a high risk*** to individuals. This includes some specified types of processing.

See Appendix 1 for screening questions to help decide when to do a DPIA.

A DPIA must:

* describe the nature, scope, context and purposes of the processing;
* assess necessity, proportionality and compliance measures;
* identify and assess risks to individuals; and
* identify any additional measures to mitigate those risks

# 7. When is a DPIA required?

DPIAs must be completed **before** BPAS begin any type of processing that is “likely to result in a high risk”. This means that we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, where there is a plan to:

* use systematic and extensive profiling with significant effects;
* process special category or criminal offence data on a large scale; or
* systematically monitor publicly accessible places on a large scale.

# 8. How do data protection by design and by default link to data protection impact assessments (DPIAs)?

A DPIA is a tool that helps identify and reduce the data protection risks of processing activities. They can also help to design more efficient and effective processes for handling personal data.

DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organisational measures we need in order to ensure our processing complies with the data protection principles.

However, a DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to rights and freedoms, though it is good practice to undertake a DPIA anyway. In contrast, data protection by design is a broader concept, as it applies organisationally and requires BPAS to take certain considerations even before we decide whether our processing is likely to result in a high risk or not.

# 9. Advice and support

For any advice and support around privacy impact assessments and data protection impact assessments please contact the Data Protection Officer.

# Appendix 1 – Data Protection Impact Assessment Screening Questions.

The ICO have produced the following checklists please consider these to help you decide when a DPIA may be required:

## 1. DPIA awareness checklist

* We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
* Our existing policies, processes and procedures include references to DPIA requirements.
* We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
* We have created and documented a DPIA process.
* We provide training for relevant staff on how to carry out a DPIA.

## 2. DPIA screening checklist

We consider carrying out a DPIA in any major project involving the use of personal data.

We consider whether to do a DPIA if we plan to carry out any other:

* evaluation or scoring;
* automated decision-making with significant effects;
* systematic monitoring;
* processing of sensitive data or data of a highly personal nature;
* processing on a large scale;
* processing of data concerning vulnerable data subjects;
* innovative technological or organisational solutions;
* processing that involves preventing data subjects from exercising a right or using a service or contract.

**We always carry out a DPIA if we plan to:**

* use systematic and extensive profiling or automated decision-making to make significant decisions about people;
* process special-category data or criminal-offence data on a large scale;
* systematically monitor a publicly accessible place on a large scale;
* use innovative technology in combination with any of the criteria in the European guidelines;
* use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit;
* carry out profiling on a large scale;
* process biometric or genetic data in combination with any of the criteria in the European guidelines;
* combine, compare or match data from multiple sources;
* process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
* process personal data in a way that involves tracking individuals’ online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
* process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
* process personal data that could result in a risk of physical harm in the event of a security breach.
* We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
* If we decide not to carry out a DPIA, we document our reasons.

## 3. DPIA process checklist

* We describe the nature, scope, context and purposes of the processing.
* We ask our data processors to help us understand and document their processing activities and identify any associated risks.
* We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
* We ask for the advice of our data protection officer.
* We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.
* We do an objective assessment of the likelihood and severity of any risks to individuals’ rights and interests.
* We identify measures we can put in place to eliminate or reduce high risks.
* We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
* We implement the measures we identified, and integrate them into our project plan.
* We consult the ICO before processing, if we cannot mitigate high risks.
* We keep our DPIAs under review and revisit them when necessary.

# Appendix 2 – DPIA Template

The ICO have created the below template to ensure we consider the all the key privacy impacts, this is the version BPAS staff must use.

## Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
|  |

## Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
|  |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
|  |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
|  |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?  |
|  |

## Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
|  |

## Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
|  |

##

## Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.  | Likelihood of harm | Severity of harm | Overall risk  |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

## Step 6: Identify measures to reduce risk

|  |
| --- |
| Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5 |
| Risk  | Options to reduce or eliminate risk | Effect on risk | Residual risk | Measure approved |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |

## Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| Item  | Name/position/date | Notes |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |