Information Governance

Privacy by Design and by Default Procedure

Date of current issue:	28 May 2024
Date of next review:	27 May 2026
Responsible Officer:	Senior Information Risk Officer (SIRO)
Validated by:	IG Board
References:	Related laws, policies & procedures are detailed within the Information Governance Legal, Statutory, Regulatory and Policy References Standard.

Document Control

Lead/contact	Steve Cheung (DPO)
Owner (Director)	Ro Cutmore SIRO
Version	Version 5
Status	Approved
Reviewed by	BPAS Information Governance Board (IGB)
Review date	28 May 2024
Ratified by	BPAS Policy Ratification & Oversight Group (PROG)
Ratification date	7 June 2024
Issue date	June 2024
Next review date	27 May 2026
Target audience	All levels of BPAS management External Regulators
Distribution	Intranet for latest version of document. Printed copies may not be the most recent version.
Dissemination plan	BPAS-wide Internal Comms newsletter/bulletin. Intranet news.

Version History

Version	Date	Author	Status	Notes / Comments
1	2019	Jill Craig Sinead Booth	Published	
2	2022	Steve Cheung	Published	
3	2023	Steve Cheung	Published	
4	May 24	Steve Cheung	Draft	Process Requirements added Updated reference to new e-form screening questions New link to updated DPIA template Expanded list of champions to include project leads, IT services and procurement services Document format updated in compliance with BPAS Policy Ratification & Oversight Group (PROG) requirements. Document control added Version history added
5	June 2024	Laura Stanley	Published	

Contents

1. Introduction

1.1 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’.

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

1.3 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?

2.1 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.

2.2 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?

3.1 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.

3.2 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. This 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
- Project Leads
- Procurement
- IT services
- The Senior Information Risk Owner (SIRO)
- The Data Protection Officer (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.

BPAS must only use processors that provide sufficient guarantees to meet the data protection legislation requirements. It is essential that such due diligence is undertaken prior to sharing personal information with third parties, through exercises supplier assessments, Data Protection Impact Assessments etc.

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 data protection 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 i.e, in advance of process operations and system designs etc.

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 is legally required to complete a DPIA for processing that is ***likely to result in a high risk*** to individuals. This includes some specified types of processing.

Screening questions to help decide when to do a DPIA can be found at https://bpas1968.sharepoint.com/:w:/r/Documents/Governance,%20Risk%20Management%20%26%20Client%20Safety/CQC%20Responses/Well%20Led%20Inspection/Improvement%20Plan/Workbooks%20and%20Project%20Gantt/Integrated%20Research%20Strategy/Evidence/Embedded%20Research%20Culture/Patient%20Focus%20Group/DPIA%20-%20Oct%202023_DP.docx?d=w62e438f45cf94488a6dc001ef9fd7959&csf=1&web=1&e=B2Barv

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
- ✓ ensure that the relevant information asset owner understands and acknowledges those risks prior to processing

7. When is a DPIA required?

Screening questions to help decide when to do a DPIA can be found at https://bpas1968.sharepoint.com/:w:/r/Documents/Governance,%20Risk%20Management%20%26%20Client%20Safety/CQC%20Responses/Well%20Led%20Inspection/Improvement%20Plan/Workbooks%20and%20Project%20Gantt/Integrated%20Research%20Strategy/Evidence/Embedded%

20Research%20Culture/Patient%20Focus%20Group/DPIA%20-%20Oct%202023_DP.docx?d=w62e438f45cf94488a6dc001ef9fd7959&csf=1&web=1&e=B2Barv

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.

It is essential to consider the wider context when assessing the risk of the processing activity, for example a customer feedback exercise may seem relatively low risk but if you consider this in the of context of termination of pregnancy services, a mere questionnaire could reveal that an individual has had a termination, if it is pieced together with an email address or name.

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. DPIA Process requirements

Use the below list as a checklist to ensure you have undertaken the relevant steps:

- ☐ We use the BPAS DPIA https://bpas1968.sharepoint.com/:w:/r/_layouts/15/Doc.aspx?sourcedoc=%7B7F598A52-7DA9-405B-8F0D-98E4143E55FC%7D&file=Data%20Privacy%20Impact%20As
- ☐ We engage the data protection officer in good time about new DPIAs or processing activity, where possible 12 weeks in advance
- ☐ 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 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 as Information Asset Owners 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.

10. Advice and support

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

Technical support for IT considerations can be sought from xx

11. Equality Impact Assessment

Question	Yes/ No	Comments
1. **Does the CPP affect one group less or more favourably than another based on:**		
• Race	No	
• Ethnic origins	No	
• Nationality	No	
• Gender (including gender reassignment)	No	
• Culture	No	
• Sexual orientation	No	
• Disability (including learning disabilities, • physical disability, sensory impairment • and mental health problems)	No	
• Age	No	
• Religion or belief	No	
2. **Is there any evidence that some groups are affected differently?**	No	
3. **If you have identified potential discrimination, are there any valid exceptions, legal and/or justifiable?**	No	
4. **Is the impact of the document likely to be negative? If so, can the impact be avoided?**	No	
5. **What alternative is there to achieving the document without the impact?**	N/A	
6. **Can we reduce the impact by taking different action?**	N/A	