www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough of Windsor and Maidenhead

Data Protection Impact Assessment

Independent Adult and Discretionary Advocacy Service

Laurel Sanderson
Commissioning - Adults
24.08.2023

Contents

Introduction and guidance

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project or new purpose for processing personal data.

A properly conducted DPIA will identify privacy issues and protections from the outset negating the requirement to retrofit systems at further expense and protect against a breach of the Data Protection Act 2018 resulting in reputational damage and fines of up to £17,000,000.

A DPIA should be carried out whenever there is a change that is likely to involve a new use or significant change in the way that personal data is handled, for example a redesign of an existing process or service or a new process or information asset being introduced, which is "likely to result in a high risk" to the data subject. The purpose of this assessment is to identify the risks that may arise through the project and propose methods to mitigate against the risks.

The GDPR states that a DPIA must be carried out in the following instances:

- Where it is proposed to use systematic and extensive profiling with significant effects.
- Where it is proposed to process special category or criminal offence data on a large scale; or
- Where it is proposed to systematically monitor publicly accessible places on a large scale.

The Information Commissioner's Office requires a DPIA to be carried out in following the additional, circumstances:

- Using innovative technology
- Processing personal data in a new way that is not already depicted in a privacy notice.
- Using profiling or special category data to decide on access to services
- Using profiling of individuals on a large scale
- Processing biometric and genetic data
- Matching or combining data sets from different data sources
- Collecting personal data from a source other than the individual without providing them with a privacy notice.
- Tracking individuals' location or behaviour
- Profiling children or target marketing or online services at them
- Processing data that might endanger an individual's physical health or safety in the event of a security breach.

Where a DPIA is carried out, it should address the following:

- A description of the proposed processing and the purposes –what personal data will be collected; who will have access; how it will be stored; who it will be disclosed to

- An assessment of the necessity and proportionality of the processing
- An assessment of the risks to the rights of the individuals affected
- The measures envisaged to address the risks and demonstrate compliance with the GDPR.

The Council's Data Protection Officer (DPO) must be consulted at the design phase of any new system or process that includes processing of personal data. dpo@rbwm.gov.uk

The DPO will record all completed DPIAs in the Record of Processing Activity register. (RoPA)

Stages of a Data Protection Impact Assessment

Stage 1: The initial screening questions (Appendix A)

This section is to be completed by the service manager or project lead responsible for delivering the proposed new system or change of purpose for the personal data processing.

The purpose of the screening questions is to ascertain if a DPIA is required.

Stage 2: Data Protection Impact Assessment (Appendix B)

To be completed by the Project Manager or Project Lead responsible for delivering the new system/proposed change. The completed form will be assessed by the Data Protection Officer who will advise on the next stage. There are four possible outcomes:

1. The DPIA is incomplete and will have to be repeated or further information obtained.

2. The DPIA has highlighted low value risks and includes appropriate actions considered through the project to mitigate these risks.

3. The DPIA has identified medium to high value risks which require an action plan to be put in place to resolve. Consideration of Caldicott Guardian and SIRO involvement required.

4. The DPIA has identified no risks, and no further information needs to be obtained.

Stage 3: Identified risks, proposed mitigations, and action plan (Appendix C)

Where the initial DPIA identifies further information governance issues, an action plan should be developed on how the risks will be mitigated. This will include:

- identified risks
- proposed solutions

- action assigned
- timescale for resolution

The Council's Data Protection Officer and SIRO should be included at an early stage where high risks to the rights and freedom to data subjects have been identified.

Stage 4: Sign-Off (Appendix D)

The sign off form must be completed by Heads of Service and returned to RBWM's DPO. DPO@rbwm.gov.uk

Screening Questions (Appendix A)

These questions are intended to help decide whether a DPIA is necessary. Answering 'Yes' to the screening questions below represents a potential information governance risk that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.

Q	Category	Screening question	
1.1	Identity	Will the project involve the collection of new information about individuals?	☒ Yes ☐ No
1.2	Identity	Does the project/process include the processing of "Special categories of personal data"?	☒ Yes ☐ No
1.3	Identity	Will the project compel individuals to provide information about themselves?	☒ Yes ☐ No
1.4	Multiple Organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☒ Yes ☐ No
1.5	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☒ Yes ☐ No
1.6	Data	Have you introduced new ways of processing/using personal data, even where your reasons for processing the data have not changed?	☒ Yes ☐ No
1.7	Data	Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	☐ Yes ☒ No
1.8	Data	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☒ Yes ☐ No

1.9	Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	☒ Yes ☐ No
1.10	Data	Will the project require you to contact individuals in ways which they may find intrusive?	☐ Yes ☒ No
1.11	Approval	Has this project/process already been started as a pilot without a screening or DPIA being undertaken?	☐ Yes ☒ No

If you have answered 'Yes' to any of the questions above, please proceed with the DPIA. (Appendix B)

If you have answered 'NO' to all the questions above a DPIA is not required.

Data Protection Impact Assessment Inception. (Appendix B)

DPIA Reference Number: Provided by the Data Protection Officer.
Project Title: Independent Adult and Discretionary Advocacy Service
Project Purpose: The provision of independent advocacy is a legal requirement for local authorities under the Care Act 2014, the Mental Capacity Act 2005 (amended 2019), the Mental Health Act 1983 (amended 2007) and the Health and Social Care Act 2012. This project is to commission a new Independent Adult and Discretionary Advocacy Service that that meets RBWM's statutory obligations and the needs of RBWM residents. This replaces two existing commissioned services with contract expiry dates of 30.06.2024. The Screening Questions in Appendix A have been completed on the basis that a new Provider will take on the Contract commencing 01.07.24. Should the incumbent provider take on the Contract commencing 01.07.24 there will be no change to existing data processing arrangements.
Implementing Organisation: The Royal Borough of Windsor and Maidenhead
Head of Service/Nominated Officer Name: Lynne Lidster Contact: lynne.lidster@rbwm.gov.uk
Implementation Date: 01.07.2024

2.1	**Is this a new or changed use of personal information that is already collected?**	☒ New ☐ Changed

	Purpose of the processing:
	Personal information is collected by the Provider of adult advocacy to deliver the Service as outlined below:
	
	• Independent Care Act Advocacy (ICAA)
	• Independent Health Complaints Advocacy (IHCA)
	• Independent Mental Capacity Advocacy (IMCA) support, including:
	  ○ Deprivation of Liberty Safeguards (DoLS)
	  ○ Liberty Protection Safeguards (LPS) from 16 years old upwards (once implemented)
	  ○ Relevant Person's Representative (RPR)
	  ○ Rule 1.2 Representative
	  ○ Litigation Friend
	• Independent Mental Health Advocacy (IMHA)
	• Discretionary advocacy:
	  ○ Self-advocacy for people with learning disabilities, including facilitation of the Learning Disability Partnership Board (LDPB) and self-advocacy groups
	  ○ Carer advocacy support
	  ○ Non-statutory advocacy projects
	
	Service delivery requires the collection of data to determine eligibility for the Service or to advocate effectively on behalf of the person receiving advocacy.	

2.2	**What personal data will be collected?** ☒ Forename ☒ Surname ☒ DOB ☒ Sex ☒ Email ☒ Address ☒ Postcode ☒ Age ☒ Gender ☒ Telephone ☐ Other unique identifier (please specify): ☐ Other administrative data (please specify): Click or tap here to enter text. **Special categories of personal data:** ☒ Racial or ethnic origin ☒ Religious or philosophical beliefs ☐ Political opinions ☐ Trade union membership ☒ Health or sex life ☒ Sexual orientation ☐ Genetic data ☐ Biometric data ☐ Financial ☒ Commission or alleged commission of an offence ☒ NHS Number ☒ Proceedings for any offence committed or alleged ☒ Description of other sensitive data collected: Care Group (mental health, learning disability, autism, substance misuse, older person, physical disability, cognitive or sensory impairment, carer (including young carer), young person aged 16-18 in transition to Adult Services). Details of the issues with which the person requires advocacy support. Details of their 'substantial difficulties, including any communication difficulties and reasonable adjustments … already made for them' (eligibility question to determine whether they meet the criteria for an advocate). Referrer's details (name, contact details). Details of any professionals (including any existing advocates) involved with the person and any family/friends actively involved in their care. Any risks or behaviours that may affect lone working.	
2.3	**Does the information involve processing children's data?** **Does the information involve processing adults' data?**	☒ Yes ☐ No ☒ Yes ☐ No
2.4	**What is the lawful basis that the personal information is collected and/or shared?** ☒ Consent of individual ☒ Legislative/Statutory requirement	
2.5		

<table>
<tr><td></td><td colspan="3">How will individuals be informed about the proposed uses of their personal data?
The Contract requires that the Provider has policies and procedures in place to check that informed consent was provided before referral and to check on first contact with Advocacy Partners that they have consented to the referral.</td></tr>
<tr><td>2.6</td><td colspan="3">How will you manage Individual complaints? The Provider will have in place a complaints policy and process. The Contract monitoring process will note any complaints and compliments received by the Provider and follow up as necessary. If the referred individual states that they did not/ do not consent to the referral – the Provider will have systems in place in order to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example the individual lacking capacity to make the decision on consent – and a best interests decision under the Mental Capacity Act affirms the necessity to proceed).</td></tr>
<tr><td rowspan="5">2.7</td><td colspan="2">Are other organisations involved in processing the personal data?
If yes, please list below</td><td>☒ Yes
☐ No</td></tr>
<tr><td>RBWM</td><td colspan="2"></td></tr>
<tr><td>Adults and children’s advocacy providers</td><td colspan="2">Optalis</td></tr>
<tr><td>Manor Green School</td><td colspan="2">Achieving for Children</td></tr>
<tr><td>NHS</td><td colspan="2">Care homes</td></tr>
<tr><td>2.8</td><td colspan="2">Does the proposal include employing external individuals?

If yes, have they signed a 3rd party disclosure agreement?
Template agreements are available from the DPO dpa@rbwm.gov.uk</td><td>☐ Yes
☒ No

☐ Yes
☐ No</td></tr>
<tr><td>2.9</td><td colspan="2">Has a data flow mapping exercise been undertaken?</td><td>☐ Yes
☒ No</td></tr>
<tr><td>2.10</td><td colspan="2">How will the personal data be collected?

The Provider will collect information from referrals received. RBWM, Optalis, the NHS and other referring agencies (including self-referrals or referrals from carers, friends, members of the public) will send information via the prescribed referral routes.</td><td></td></tr>
</table>

	The Provider and the Commissioner will be joint data controllers. The Provider will use information received via referrals in order to make contact with referred Advocacy Partners to offer appropriate advocacy services. Advocacy Partners may be eligible for more than one statutory advocacy Service and/ or non-statutory advocacy so may seamlessly move within and between the Service Elements. For example, an Advocacy Partner may be referred for an Independent Mental Capacity Advocacy due to lacking capacity to make the decision to move from hospital to residential care. Inherent within that there may be a requirement to assess their needs under the Care Act 2014 and so they may also be eligible for Independent Care Act Advocacy as well as for an Independent Mental Capacity Advocate. The Provider will make decisions on eligibility for aspects of the Service based on information received in the referral and additional information gathered in its own assessment of the Advocacy Partner's circumstances. Personally identifiable information (PII) will only be shared by the Provider with others: • on a case-by-case basis where it is necessary in order to advocate on the Advocacy Partner's behalf or to meet the Advocacy Partner's health or social care needs • where they have the consent of the Advocacy Partner to do so (or where they have a lawful basis to do so, for example, under the Mental Capacity Act in order to fulfil the advocacy role) • via the most appropriate method (such as telephone call or secure email to, for example, the Adult Services Safeguarding Hub, the allocated social worker, relevant hospital ward or care home staff). Anonymous Service usage data will be shared with the Commissioner on a quarterly basis. This does not contain any PII. RBWM is not prescriptive on how the Provider will store information, only that its systems for doing so are compliant with GDPR. The Contract will also specify compliance with record retention lengths and the requirement to delete information once retention periods have been met. The highest data processing risk is the sending of PII information via non secure email either from referrer to the	

	Provider or from the Provider to another agency. The Provider will be required to ensure that they send information securely and referral information will make clear that information must be sent securely to them or if that is not possible to refer by phone. The potential for an online web-based referral form, removing the necessity for referrals via email, will be explored with the Provider. The Provider may receive a referral for an adult with capacity to make a decision about the receipt of the Service where they have not provided consent to be referred. The Contract will need to ensure that the Provider has procedures in place to check that informed consent was provided before referral and to check on first contact with individuals that they have consented to the referral. If the individual states that they did not/ do not consent to the referral, the Provider will have systems in place to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example, the individual lacking capacity to make the decision on consent and a best interests decision under the Mental Capacity Act affirms the necessity to proceed). If the Advocacy Partner has consented and withdraws their consent for their information to be held/ processed by the Provider, then the Provider will need to ensure that they have systems in place to manage this scenario and delete the individual data. Additionally appropriate mechanisms will be required to capture anonymous Service usage data if the Advocacy Partner has received any Service Element prior to consent being withdrawn. The Provider may receive a referral for an adult lacking capacity to make a decision about the receipt of the Service. The Contract will need to ensure that the Provider has procedures in place to check that there is a lawful basis to proceed without consent. Where appropriate and the Advocacy Partner has capacity, advocates are encouraged to complete an Advocacy Agreement form with their Advocacy Partners, setting out the issues that will be dealt with by the advocate. This document can be reviewed at any time, and advocates are always clear with Advocacy Partners about the issues they can and cannot deal with. Wherever possible, if an issue is not appropriate to be dealt with by an advocate, the Advocacy Partner will be signposted to another agency.	

	Advocacy Partners will be asked to complete a permission to share agreement at the point of engagement with the Service and at regular intervals thereafter, but no less than annually. Information will be held in accordance with the Provider's data protection policies, which in turn will be compliant with the terms and conditions of the Contract.	
2.11	**Where will the information be stored?** Personal data will held by the Provider. Storage will be, at a minimum, compliant with relevant legislation as set out in the terms and conditions of the Contract. The Provider will hold electronic and paper files to support the delivery of the Service. A range of IT systems or applications are available to providers. If not already secured, the specific system will be secured by the Provider once the Contract is awarded. IT systems will need to reflect the requirements as set out in the Specification.	
2.12	**Appropriate access controls** Does the system involve accessing personal data held in other systems or locations?	☐ Yes ☒ No
2.13	**Retention/disposal schedules** Has an appropriate retention period been identified and applied to the information? *If no, please get advice from the DPO.* Retention periods will be set by the Provider's own data protection policies, but will be, at a minimum, compliant with statutory timescales. If the individual states that they did not/ do not consent to the referral – the Provider will have systems in place in order to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example the individual lacking capacity to make the decision on consent – and a best interests decision under the Mental Capacity Act affirms the necessity to proceed). If the Advocacy Partner has consented and withdraws their consent for their information to be held/processed by the Provider – then the Provider will need to ensure that they have systems in place to manage this scenario and delete the Advocacy Partner's data. Additionally appropriate mechanisms will be required to capture anonymous	☒ Yes ☐ No

	Service usage data if the Advocacy Partner has received any Service Element prior to consent being withdrawn.	
2.14	**Data quality** How will the information be kept up to date and accurate? The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the Contract. The terms and conditions of the Contract clearly set out the requirements to be compliant with data protection laws, including ensuring that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected.	
2.15	**Right to rectification/deletion** If you are procuring new software, does it allow you to amend/delete personal data when necessary?	☐ Yes ☐ No
2.16	**Please state by which method the information will be transferred?** ☒ Email ☒ GCSx Email ☐ Courier ☒ Post (External) ☒ Post (Internal) ☒ By Hand ☒ Telephone ☐ Fax ☐ CD/DVD ☐ USB ☐ Portable HDD ☐ Web access storage ☐ Wireless Network ☐ Cloud **The information will be transferred as:** ☒ Person-identifiable ☐ Pseudonymised ☒ Anonymised	
2.17	**Who will have access to the personal information?** Access to files will be set out in the Provider's own policies and procedures but will be, at a minimum, compliant with relevant legislation as set out in the terms and conditions of the Contract. Members, attendees and presenters at meetings, such as the Learning Disability Partnership Board, self-advocacy groups, support groups or other advocacy groups, meetings or events will have access to each others' names and Care Group (when this data is relevant to the Service provision). **What security and audit measures have been, or will be, implemented to secure access to and limit use of personal identifiable information?**	

	The highest data processing risk is the sending of PII information via non secure email either from referrer to the Provider or from the Provider to another agency. The Provider will be required to ensure that they send information securely and referral information will make clear that information must be sent securely to them or if that is not possible to refer by phone. The potential for an online web-based referral form removing the necessity for referrals via email will be explored with the Provider. Anonymous Service usage data will be shared with the commissioner on a quarterly basis. This does not contain any PII.	
2.18	**What staff training will be provided?** Employed staff and volunteer training will be set out in the Provider's own policies and procedures but will be, at a minimum, compliant with relevant legislation as set out in the terms and conditions of the Contract.	
2.19	**What disaster recovery and business contingency plans are in place?** Disaster recovery and business contingency plans will be set out in the Provider's own policies and procedures but will be, at a minimum, compliant with relevant legislation as set out in the terms and conditions of the Contract.	
2.20	**Subject Access Requests** Are arrangements in place for recognising and responding to requests from individuals for a copy of the personal data processed?	☒ Yes ☐ No
2.21	**Are there any new or additional reporting requirements for this project?** ☒ Yes ☐ No Who will be responsible for running the reports? The Provider. Who will receive the report or where will it be published? The Commissioner will receive anonymous quarterly performance monitoring reports will be shared with appropriate Optalis and NHS staff and any Advocacy Partners invited to commissioning support/ Contract monitoring meetings, but will not be published or publicly available. The Mental Capacity Act and Deprivation of Liberty (DoLS) Lead will receive person-identifiable reports detailing out of area DoLS cases being processed	☒ Yes ☐ No

	by the Provider, which will not be published or publicly available. Which format will the reports be in? ☒ Person-identifiable ☐ Pseudonymised ☒ Anonymised	

2.22	**Additional comments and notes:**

Identified risks, proposed mitigations, and action plan (Appendix C)

A 'privacy risk' is the risk that a proposal will fail to meet individual's reasonable expectations of privacy. Calculating risk is not simply about assessing whether the project will be legally compliant. It's possible to comply with the law and for the behaviour still to affect whether our residents reasonable privacy expectations are met. Risks to an individual will often directly equate to risks to the Council. Consider not only the direct risks from the proposal, but also any knock on effects. A DPIA doesn't set out to identify and eliminate every possible risk to an individual from using their personal information or otherwise impacting on their privacy.

Identified risks

Risk Ref	Issue	Who is the risk to?	Proposed Solution
1	The sending of PII information via non secure email either from referrer to the Provider or from the Provider to another agency.	Advocacy Partner	The Provider will be required to ensure that they send information securely and referral information will make clear that information must be sent securely to them or if that is not possible to refer by phone. The potential for an online web-based referral form, removing the necessity for referrals via email, will be explored with the Provider.
2	Provider data protection compliance	Advocacy Partner/ RBWM	The Provider must have a current Data Protection Policy and Procedures and comply with any notification requirements and observe all their obligations under the Data Protection Act 1998 ('DPA') and the UK General Data Protection Regulation ('UK GDPR'), which arise in connection

			with the Service. In the event of a personal data breach the Provider must initiate the relevant procedure which must include the completion of a risk assessment. The Provider will take steps to contain the breach and mitigate against any reputational damage to RBWM and will put processes in place to help prevent it from happening again.
Ref.	Click or tap here to enter text.	Click here.	Click here to enter text.
Ref.	Click or tap here to enter text.	Click here.	Click here to enter text.

Solutions to be implemented

Risk Ref	Approved Solution	Result[1]	Approved by
Ref.	Click or tap here to enter text.	Choose.	Click here.
Ref.	Click or tap here to enter text.	Choose.	Click here.
Ref.	Click or tap here to enter text.	Choose.	Click here.
Ref.	Click or tap here to enter text.	Choose.	Click here.

Agreed actions

Action to be taken	Completion Date	Responsible for action
Click or tap here to enter text.	Date.	Click here.
Click or tap here to enter text.	Date.	Click here.
Click or tap here to enter text.	Date.	Click here.
Click or tap here to enter text.	Date.	Click here.

Other identified risks

Other risks which have been identified which do not relate to Privacy but need to be escalated, e.g. Business Continuity, Health & Safety.

Risk	Escalated to	Date
Click or tap here to enter text.	Click here.	Date.
Click or tap here to enter text.	Click here.	Date.

Click or tap here to enter text.	Click here.	Date.
Click or tap here to enter text.	Click here.	Date.

*Is the risk reduced, eliminated or accepted?

Sign off Form (Appendix D)

Signatories required once the DPIA has been completed.

Head of Service	
Name:	Lynne Lidster
Signature:	Lynne Lidster
Date:	28.11.23

Data Protection Officer	
Name:	Samantha-Lea Wootton
Signature:	Samantha-Lea Wootton
Date:	29.11.23

Senior Information Risk Owner	
Name:	Click or tap here to enter text.
Signature:	Click or tap here to enter text.
Date:	Click or tap here to enter text.

Email completed DPIA to the DPO DPO@rbwm.gov.uk