Data Protection Impact Assessment Template

DPIA: Paris Replacement Project

Describe the project and the need for a DPIA

Explain broadly what the 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 including relevant information from (or link to) the screening.

Paris system replacement
Selecting and implementing a replacement for the Paris ASC case management system. This will involve specifying requirements of the system (with the assistance of a consultant), selection of the replacement (via tender process), implementation & testing (with selected provider), full implementation and move to BAU.

A full DPIA is needed due to the nature and volume of the data involved. Although there is no change in the nature of processing, the risks involved with transfer and implementation of a system of this nature can be significant.

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?

The system includes sensitive personal data regarding: race or ethnic origin, religious or philosophical beliefs, health, criminal convictions, sex life, and sexual orientation. All these categories require special protection under data protection legislation and require legal bases for processing under both Article 6 and Article 9 of the UK GDPR.

There is a high volume of data. Data will be collected and used in the same way as currently. Retention will be investigated as part of the tender process although the Optalis retention schedule will be used as a basis for this specification. We will need to be able to fulfil information rights requests including DSARs and Right to Erasure.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of the project management process.

You can use consultation at any stage of the DPIA process.

Both Optalis and RBWM DPOs are being consulted throughout the project management process. A DP workshop has been completed with the Optalis DPO and the tender specification consultant (24/05/2022).

The RBWM Transformation Team will appoint a Project Manager and consultations between relevant RBWM and Optalis staff will continue throughout the project.

The Optalis DPO has been involved throughout the tender process including system demonstrations on 22 & 23/02/2023. The DPO will continue to be involved as required throughout data transfer and implementation.

Describe the information flows

You should describe the collection, use, storage and deletion of personal data here. Include a flow diagram that includes the data items (the elements of personal data), the formats in which they are stored (e.g. digital, hard copy, photo etc.), the methods by which the data items move from one location to another, and the locations where data items are stored and where processing happens. You should also say how many individuals are likely to be affected by the project.

Public cloud is the preference at this stage (i.e. we host the data on our own MS Azure or AWS account) – we will need assurance on integrity, security, accessibility, and storage location.

The council is procuring an integrated case management and finance system, hosted securely by system supplier in a secure data centre with Node 4 Data Centre security accreditation. This ensures that data is securely hosted and backed up at separate locations for business continuity and rollback should the need arise.

Practitioners across Adult Social Care will collect personal, demographic and service data and input data into the system for the sole purpose of provision of service under the Care Act 2014. The system will hold structured and unstructured data, documents, photos and other media types securely on the hosted servers with user permission-controlled access to the system.

Data flow diagram, system architecture and data centre certification will be attached prior to contract award.

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? Does the processing 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?*

Local authorities have a statutory responsibility placed upon them by the secretary of state to provide care and support to service users and their carers and promote wellbeing in their communities. As such, there is legal obligation to collect and process information about our clients, their carers, or representatives to enable the local authority to evaluate their assessed needs and provide services appropriate for them based on their eligibility.

From the point of contact through the customer journey, the council has statutory powers to collect and process information that is proportionate and necessary to provide services. Detailed information on the legal bases for processing each piece of data in Optalis is contained in the Record of Processing Activity (RoPA).

Clients and their representatives are provided with the Optalis Privacy Notice and, where necessary, consent form to continue their journey with the council / Optalis. In certain circumstances, they have the right not to consent to sharing their information under DPA and GDPR.

In processing client data, the Optalis data retention policy is taken into consideration and the DPA principles are applied. Retention periods are set according to the Optalis Data Retention Schedule much of which is based on the NHSX Records Management Code of Practice V7 2021.

The local authority and Optalis are joint Data Controllers, and the CMS provider is the data processor as the host of the database. The CMS provider role is limited to secure migration of the initial data into the system and for the management of the database within the contract. The contract ensures that the data is processed lawfully, and the supplier has the necessary safeguards in place to protect data confidentiality and processing in accordance with the contract. The contract will enforce confidentiality, DPA and GDPR.

Regarding Data Quality, the procured system will be compliant with relevant ISO standards. All suppliers on the Framework being used for procuring the new system meet ISO27000 and other certifications standards to be eligible suppliers on the Framework. As such, the system will have the ability to hold quality data in structured and unstructured formats. However, data quality responsibility lies with the local authority, the Information Asset Owner, and those responsible for inputting data into the system. Training will be provided to all users of the new system, but the users and their managers will need to ensure compliance with internal data quality principles and adopted procedures to ensure valid, accurate and timely data is entered on the system.

Documents to attach prior to contract award:
Information Security Management System (ISMS)
Certification The ISO 27001

Identify the privacy and related risks
Identify the key privacy risks and the associated compliance and corporate risks as necessary. For larger-scale DPIAs you should record this information on a more formal risk register.

Annex one can be used to help you identify the DPA related compliance risks.

Risk Ref	Source of risk and potential impact on individuals	Likelihood of harm 1-5 (Low to high)	Consequence of harm 1-5 (Low to high)	Overall risk *L * C*
PR1	Data transfer – information migrated incorrectly, errors in new system data, data not fully migrated. Significant impact on individuals if records incorrect / incomplete / missing, both data protection and customer care implications. Data breaches if information inaccurate / incomplete / lost.	Unmitigated 3 **Mitigated 1**	4 **4**	12 **4**
PR2	Test data – information not anonymised / pseudonymised resulting in access to live information by individuals not requiring access to the data for their job role. Security breaches due to unauthorised personnel accessing records Difficult to anonymise / pseudonymise live data due to information contained throughout Paris records.	Unmitigated 3 **Mitigated 1**	3 **1**	9 **1**
PR3	System security – potential for cloud-based solution meaning that data would not be internally hosted on council-controlled servers. Server access could be vulnerable, only assurance would be via audit of host's facilities and thorough due diligence of accreditations (e.g. ISO27001). Potential risk of significant data breaches.	Unmitigated 3 **Mitigated 2**	5 **5**	15 **10**
PR4	Legacy data – data left on Paris system for substantial time following implementation of new solution. Risk of retaining out of date information / duplicate data	Unmitigated 3 **Mitigated 1**	3 **2**	9 **2**
PR5	Legacy data – Paris system not maintained; access procedures lack robustness. Systems that have no current use can suffer 'redundancy oversight' where the reduced number of users are not maintained, and the normal leaver / access processes are not followed rigorously. This can leave the system open to attack as access is no longer regularly monitored.	Unmitigated 3 **Mitigated 1**	4 **2**	12 **2**

PR6	Financial data – data uploaded incorrectly / with errors resulting in incorrect financial records for individuals. Data breaches if information missing or incorrect. Financial impact if billing information incorrect.	Unmitigated 3 **Mitigated** **2**	4 **4**	12 **8**
PR7	Staff – use of contract or interim staff for project; due diligence procedures (used in recruitment of permanent staff) not followed. Access to data by unchecked personnel resulting in breaches, theft of data, and potential misuse.	Unmitigated 3 **Mitigated** **1**	4 **4**	12 **4**
PR8	External Staff - use of contract or interim staff for project; data protection training not undertaken. Lack of knowledge / understanding resulting in data breaches	Unmitigated 3 **Mitigated** **1**	4 **2**	12 **2**

Risk Matrix

Risk Matrix:	**Likelihood**				
Consequence	**1 - Rare**	**2 - Unlikely**	**3 - Possible**	**4 - Likely**	**5 - Almost Certain**
1 - Negligible	**1**	**2**	**3**	**4**	**5**
2 - Minor	**2**	**4**	**6**	**8**	**10**
3 - Moderate	**3**	**6**	**9**	**12**	**15**
4 - Major	**4**	**8**	**12**	**16**	**20**
5 - Catastrophic	**5**	**10**	**15**	**20**	**25**

Data Protection Impact Assessment Template

Identify privacy solutions

Describe the actions you could take to reduce or eliminate the risks identified as Med or High above, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk ref	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Residual risk:** Low/Med/High	**Measure approved?** Y/N
PR1	The data migration strategy will clearly set out what is in scope and out of scope for migration. Our approach is that 'in scope' data migration will be cleansed as much as possible and signed off by relevant stakeholders before it is migrated into the new system. Following every data transfer, to supplier via agreed transferred solutions e.g. SFTP, will be received and confirmed by supplier and when migration run has been completed, the migration team will validate that the data transferred matches data migrated so the risk of data loss, inaccurate or incomplete data in production environment will be almost non-existent as it data run will be tested, validated and signed off. Where information is noted as transferred to supplier but missing during testing will be reported to supplier via agreed process and resolved before we can proceed to the next stage of the process.	Reduced	Low	
PR2	It will be impossible to test and validate anonymised data against live date as data cannot be reconciled.	Reduced	Low	

	Everyone on the project would have either signed up to the council's/ Optalis' information security/ confidentiality policy. The project manager will continue to remind staff about data protection responsibility and information security. The data migration and testing strategy will set out the data migration and testing approach and principles which the team will follow to minimise/mitigate associated risks.			
PR3	Potentially secure cloud-hosted servers are more secure than internally hosted servers. The SoR requires the hosted system to be held in a Node 3+ security compliant Data Centre and meet relevant security standards including ISO27001. Data will be regularly backed up. Accessibility will be tightly controlled with user-based permissions that comply with relevant password security policies. However, cyber security risks cannot be fully mitigated in the current climate. Local Authorities remain significant targets.	Accepted	Medium	
PR4	The data migration strategy will set out what is in scope for migration and what is out of scope. A cut-off date for migration will be set when it is time to transfer data to supplier. If the approach is that Paris is retained as an Archive, system whatever data is kept at the cut-off date is the current data at the time off cut off and does not require any further update once migration is completed and the remaining data would need to remain in a fixed state.	Reduced *Will be revisited as the project progresses*	Low	

	If the decision is to migrate everything into the new system, then the data will be fully migrated, and Paris decommissioned once AfC data is also migrated.			
PR5	Once the new system is live and migration work is completed. Access to the legacy Paris system will be reduced to only the Applications team and RBWM IT team. If the system is retained as an Archive system, it would be isolated from the network to ensure there is not risk to active systems on the network. Access for reference or SAR will be made on a need-to-know basis and request sent to Applications team who will either access the system on behalf of the requester or grant time limited access to the system. If no data is retained in Paris as archive, the system will be closed and decommissioned.	Reduced *Will be revisited as the project progresses*	Low	
PR6	If the information held on current system is accurate, the risk of migrating inaccurate information to the new system will be extremely low. However, if the information currently held is inaccurate, then the risk of migrating the incorrect data to the new system is no greater that what it is currently. As stated above, the data migration strategy included data quality approach, where we will, in collaboration with practitioners, finance and other colleagues try to correct identified errors before they are migrated into	Reduced	Low	

	the new system. The testing process to be adopted will ensure that data is validated, tested, and signed off before it is migrated into the new system. The cooperation of the teams are necessary to achieve quality data.			
PR7	DBS check is no longer a mandatory requirement for recruitment of agency staff who do no not have direct access to vulnerable people. However, interim staff do sign up to DPA and confidentiality and if there is an HR requirement for DBS check, it should be applied.	Reduced	Low	
PR8	Ensure rigorous application of training requirements for external personnel	Reduced	Low	

Data Protection Impact Assessment Template

Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Item	Name / date	Notes
Measures approved by		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by	Sam Linton, Optalis DPO 22/03/2023	If accepting any residual high risk, consult the DPO / ICO before going ahead
Data Protection advice provided	Sam Linton, Optalis DPO 22/03/2023	DPO should advise on compliance, privacy solutions and whether processing can proceed
Summary of DPO advice: **Processing can proceed. Risks should be closely monitored, and high-level privacy measures applied. No compliance issues.**		
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 be kept under review by:	Sydney Martindale, Project Manager Sam Linton, Optalis DPO	DPO should also review ongoing compliance with DPIA

Annex 1 - Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the GDPR.

Principle 1

Personal data shall be processed fairly and lawfully and transparently

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do we need to amend our privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Check that you are not using existing data in a way that is not compatible with the original purpose it was collected for.

Principle 3

Personal data shall be adequate, relevant and limited to what is necessary for the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

What is the minimum personal data you need that doesn't compromise the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data shall not be kept for longer than necessary

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that employees know how to operate a new system securely?

Will the project require you to transfer data outside of the EEA? You should check any contracts or Terms and Conditions carefully to ensure the details of any data processing are covered off properly and you are satisfied that any required data sharing agreements are in place.

If you will be making transfers, how will you ensure that the data is adequately protected?