

## Data Protection Impact Assessment (DPIA) - Full Assessment

### Guidance for the Project Manager and Sponsor

The Data Privacy Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the people whose data you are dealing with and show how you will minimise the privacy risks. This template has been designed to incorporate the legal requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

**Use the pre-screening template first.** If that shows a high risk in processing the data then you must carry out this full DPIA.

Conducting a DPIA is a legal requirement under the GDPR particularly if the proposed processing is using new technologies and poses a high-risk to people's data. Further information and guidance on the DPIA is also available on the ICO website here: [ICO's PIA code of practice](#) and the Article 29 Working Party [here](#).

### GOVERNANCE ARRANGEMENTS

This DPIA will be submitted to the Corporate Information Governance Group (CIGG) and the advice of the Data Protection Officer (DPO) will be sought as part of that process. You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

#### 1. PROJECT SUMMARY

<b>Project Name</b>	ASC Assistive Technology Project	<b>Directorate and Service</b>	Adult Social Care – Transformation
<b>Project Sponsor and Position</b>	Sarah McClinton – Director of Adult Social Services	<b>Project Manager and Position</b>	██████████ Project Manager
<b>Project Start Date</b>	September 2018	<b>Project Go Live Date (anticipated/planned)</b>	March 2019
<b>Project End Date</b>	March 2019		

<b>Third parties involved/associated with the Project:</b>	PA Consulting (external company)	<b>Does this DPIA cover multiple projects?</b>	No
--	----------------------------------	--	----

**High Level description of the Project:**

- Explain what this project is in plain language. For example: “We would like to share data with a third party so that they can carry out research into how to improve people’s access to benefits.”]
- Attach the pre-screen DPIA. The conclusion to that will explain why it is necessary to carry out this DPIA.

The pre-screen DPIA is attached.

The Assistive Technology (AT) project seeks to maximize Camden’s AT offer by developing the current service, Careline, and engaging the relevant stakeholders, with the aim of increasing the referrals made to Careline. In particular, the aspiration is to expand the service to a wider range of users including younger cohorts and those with more complex needs. The overall aim of the project is to expand the use of AT in order to increase independence and improve choice and outcomes for residents whilst realising significant financial benefits for the Council. This will result in more people in Camden using AT to support them instead of traditional care and support services.

As well as re-designing the referral pathways and processes for Careline and delivering learning and development programmes, the project also seeks to develop a robust benefits framework and reporting tool to enable efficient and accurate reporting on KPIs.

We will be using a third party, PA Consulting, to design and build the benefits reporting tool. To do this, a small number of staff from PA Consulting will need to look at the data, which they can do when they come into 5PS or via a login process by remote connection. They will not have access to the data in any other way and nor will they be sent the data via email.

**2. DESCRIPTION OF THE PROJECT**

---

*Include here a plain English description of:*

- *the Project (set the context so that it is clear what you want to do)*

The project will build a benefits framework and reporting tool and dashboard so that Camden can track the benefits of using assistive technology to support people in adult social care. The data will be shared with a third party to enable them to design and build the reporting tool.

- *what will be done with the data (the processing activities)*

*Data will be used to populate a QlikSense dashboard for use by the ASC Transformation Board, Adult Social Care SMT and other ASC officers. Officers from PA Consulting will be required to access these data to allow for their work developing the benefits tracking mechanisms to be completed.*

- *the reasons why you need to process the data (the purpose)*

This project is an important component of LBC's Adult Social Care services' delivery of savings associated with LBC's current MTFS. Thus, the monitoring of the savings achieved by development of the new service constitute a significant business need. The additional support from an external partner is necessary to ensure that this work benefits from their expertise as well as to add capacity.

- *the benefits that this project will provide*

Overall the assistive technology project will benefit residents by supporting them to live independently and improve outcomes for them. The benefits reporting dashboard (which requires access to data by the third party) will enable Camden to accurately monitor the benefits that the project brings including significant financial savings for the council and improved outcomes and satisfaction for residents. This tracking is required to ensure delivery of savings committed to within ASC's response to LBC's current MTFS.

- *how the data will be processed (for example, who will carry out the processing and will they use software or other devices to do it)*

The data will be processed by PA Consulting using Camden laptops and servers. Work will be carried out on Camden laptops and will at no point leave the Camden Environment.

The following software will be used:

Databases: Mosaic, Jontek. Reporting tools: Business Objects and QlikView / QlikSense (nb Mosaic and Jontek are both SQL Server based, and modelling of data after its extraction and before its loading into Qlik may be carried out in an additional SQL Server layer). There will be no paper versions of client data as part of this processing.

- *how will the data be stored?*

Data will be stored outside of the case management system within QVD/QVW files servicing the dashboard. Modelling may also be carried out in a SQL layer between the databases and the dashboard. These data will be overwritten on a daily basis so any amendment or destruction may be managed within the case management system.

- *where have you obtained the data from?*

The personal data will be obtained from the case management system, Mosaic and Jontek; having been recorded in those systems by ASC Social worker and Careline staff as part of their BAU interaction with clients / data subjects.

- *How long will you be processing the data for and how often? For example, once a week for six months.*

PA Consulting will have access to the data referred to above for the duration of the project and no longer. The extraction of data from the source systems and visualisation of those data within a dashboard will be an ongoing mechanism by which service delivery and benefits realisation are monitored.

- *What is the volume of the data? For example, 150 records of service users.*

The data will include all individuals who are referred to Camden Careline, this currently includes 825 mosaic records but the aim is to greatly increase this number to over 3,000.

#### **Types of personal data to be processed and data flow map(s):**

##### **Personal data:**

*List the types of data that you intend to process and the types of data subject (for example, names, addresses of residents, service users etc):*

- *Refer to this guidance to assess what is personal data: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>*

Person Identifiers from the Jontek and Mosaic systems

Referral information, extracted from a Mosaic based form completed by a social worker on behalf of an ASC client  
Careline Service information (Jontek)  
Care Package information (Mosaic)  
Geospatial information regarding residence of clients  
(possibly: name, address and dates of birth)

**Special category data:**

*List the types of special category data and the types of data subject:*

- Refer to this guidance to assess what is special category data: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

No special category data will be processed however. Health conditions of a client may be broadly inferred from the services they receive and the 'primary support need' associated with their care package. Identity data will be managed to ensure that this does not have implications with regard to risk to privacy.

**Data Flows:**

- You may find it useful to use a flowchart, which you can attach at Annex A.

*The flowchart should show, for example: Data entry and exit points, location, user categories, data subject categories*

The exact nature of the data flow will be defined as part of the project. However, the basic premise will be the extraction of data from Mosaic and Jontek and the linking of those data within a Qlik environment where those data will be presented to strategic and operational audiences.

### **3. DATA PROTECTION PRINCIPLES**

**This section demonstrates how the project meets the data protection principles.**

- How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?

PA Consulting will be provisioned access to only those data required to carry out the project.

LBC officers will have oversight of the project to ensure that data are not being used for processes other than those referenced above.

- If the data was originally collected for one purpose and you intend to use it for another purpose, explain how you will inform the data subjects.

The data in question are collected as part of the processes by which Adult Social Care and Careline services are delivered. The proposed processing is intended to allow for effective monitoring and improvement of those services.

The use of data to improve services in this manner is articulated in LBC's corporate online privacy notice as well as the privacy notices used by the services. This processing is not out of the ordinary and it is assumed that we do routinely make residents / service users aware that we share personal data internally to improve service and in some circumstances work with third parties.

- How will you make sure that the data is kept accurate and up to date?

This will be managed in the source systems.

- How long will you keep the data for and how will you destroy it at the end of the retention period?

The retention schedule under the relevant division/service and record title is available at <https://lbcamden.sharepoint.com/sites/intranet/business-support/Pages/Retention-.aspx>. Supporting People divisions start on page 49. If needed, Carlos Carrington can assist with clarifying what the retention period should be.

This is ASC data captured in the course of the work ASC carries out and therefore is subject to the same retention schedules as all ASC data.

For Careline Telecare data on Jontek system, the retention period is CY + 6 years.

For Mosaic data of:

Adults under 65 with learning disabilities, it is 6 years after last contact.

Adults where Mental Health Act assessment has been completed - 10 years after last contact.

Other adults under 65 mental health cases - 6 years after last contact.

Adults where protection of vulnerable adults procedures have been used - 10 years after last contact.

Registration of vision impairment and disability - retain records and CV document until death. Following death the record and CV must be kept for a minimum of 3 years.

Adults where ASC director is authorised to manage a service users finances - 7 years from the data authorisation ceases.

Adult cases where financial assessment has been carried out and/or supporting people funding has been provided - 6 years from data debit/credit has been cleared except for cases identified following a risk assessment where a 2 year retention applies.

Other non-exceptional adults cases - 2 years after last contact.

Enquiries about adults which are recorded but which do not result in an assessment of need - 2 years after last contact.

Deceased adults where death is considered suspicious - 75 years after last contact.

Adults cases where adaptations provided and a legal charge is placed on a property (and Camden Council has made a contribution to the disabled facilities grant or other special circumstances - 25 years from completion of the adaptation or when debt repaid.

Adult cases where adaptations over £500 provided - 10 years from completion of the adaptation.

Return of equipment requiring maintenance and insurance eg stair lifts, bath lifts - 3 years after the equipment is returned.

- Have you cleared the information security arrangements with the Information Security Manager?

No, we are operating exclusively within the Camden environment.

The data that PA Consulting are viewing is held on Mosaic and Jontek which can only be accessed via Camden login and passwords. Mosaic and Jontek systems are password protected and held on Camden servers. A small group of PA Consulting will be provided with a login and password. There is no proposal to move the data outside of the Camden environment. PA Consulting staff will be operating within BAU reporting processes.

Record the Information Security manager's comments here:

#### 4. BASIS OF PROCESSING

##### Basis for processing:

- Which legal basis in Article 6 are you relying on? <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

Legal basis for processing - **Article 6 (1)(e) Public task** (the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law).

Legal basis for processing - **Article 9(2)(g) Public Interest** (processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject)

- If you think you need to rely on legitimate interests then ask the Information and Records Management Team for advice.

We are not relying on legitimate interests for this processing.

- If you are processing special category data, you will also need a legal basis under Article 9 to process this.

As above, no special category data will be processed however health conditions of a client may be broadly inferred from the services they receive and the 'primary support need' associated with their care package. However, identity data will be managed to ensure that this does not have implications with regard to risk to privacy.

- If you are processing criminal convictions data then you should speak to the Legal team as you need an additional legal basis to do this.

N/A



## 5. DISCLOSURES OF DATA

- Will you be giving this data to a data processor or a sub-processor? YES

Camden Council is the data controller. PA Consulting may be considered a processor for this work and they will be operating as LBC officers using LBC hardware/software, working in the LBC environment and following LBC practices. They will only be looking at the data when they come in to 5PS, or via remote connection.

- Tick here to agree that you will be entering into a data processing agreement with them

A small number of PA Consulting staff will be operating as LBC officers and use LBC hardware/software. They will be viewing the data when they come into 5PS or via remote connection.

- Will you be sharing data with a third party?

PA Consulting will be viewing data using logins and passwords. The data will be not be moved out of the Camden environment.

- List the third parties that you propose to share with

PA Consulting.

- Tick here to agree that you will be entering into a data sharing agreement with the third parties

PA Consulting will only have access to the data when they come to 5PS or via remote connection using LBC hardware.

**6. TRANSFERS OF DATA OUTSIDE OF THE EEA**

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/>

**Will any personal data be processed outside of the EEA?**

See a list of countries here: <https://www.gov.uk/eu-eea>

No

If your answer is yes, you must consult the DPO straight away.

**Comments of the data protection advisor:**

*To contain comments detailing the safeguards that need to be put in place.*

**7. DATA SUBJECT RIGHTS AND COMPLIANCE WITH CORPORATE POLICIES**

**[Information in Camden](#) contains the Council's policies and procedures on data protection compliance, including how to respond to requests from people to enforce their rights under data protection law.**

You must comply with the requirements in Information in Camden. Tick here to agree that you will be complying with IIC on Data Subject Rights [ **Ticked** ] If there is a reason why you cannot do this, please explain why here:

## 8. CONSULTATION WITH INTERESTED PARTIES

Is one of the outcomes of your project going to make a change which will have a direct effect on data subjects?, For example: introducing CCTV into a library? If so, contact the Information and Records Management Team for advice as you may need to consult with stakeholders.

**Record the comments of the data protection officer here:**



*Include advice on whether consultation is necessary and the steps to take.*

Clients will not be directly affected by this processing. LBC ASC clients will benefit more broadly from the service improvement which this work will facilitate.

## 9. RISK ASSESSMENT AND MITIGATION

**Risk** is a combination of **impact**- how bad the effect of the risk would be- and **probability** – the likelihood of the risk happening. Risk is assessed from the perspective of the data subject (as opposed to risk to the Council) and what the impact could be on them as a result of the proposed data processing. For each of the risks you identify:

1. think about how likely they are to occur and categorise them according to **Table 1 (e.g., rare, unlikely etc)**.
2. Then consider the impact each risk will have and categorise them according to **Table 2 (e.g., minor, moderate etc)**.

3. Then look at **Table 3** and see the risk level. Where the level says mitigations are needed, think about what these will be and how they will reduce the risk level down.

4. Enter the details in the grid below

There is more information on the council’s approach to risk here

[https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk\\_Management.aspx](https://lbcamden.sharepoint.com/sites/intranet/finance/Pages/Risk_Management.aspx)

<b>EXAMPLE</b>			
	<b>DESCRIPTION</b>	<b>RISK LEVEL BEFORE ANY MITIGATION</b>	<b>RISK LEVEL AFTER MITIGATION</b>
<b>SOURCE OF RISK</b>	Storage of personal data on laptops	6	4
<b>Potential impact on individual</b>	Laptop could be lost and personal data stolen.	Possible and minor (depending on the contents of the laptop)	Unlikely and minor
<b>Threats that could lead to illegitimate access, undesired modification and disappearance of data:</b>	The portability of the laptop could lead to a threat to the personal data if it is not secure or if staff are not aware of the potential dangers to personal data.		
<b>Any compliance or corporate risks?</b> Refer here to the corporate risk framework i.e. “you should also consider and apply the Council’s Risk Framework when assessing the risk of your project as a whole.”	Risk of breach or GDPR and corporate procedures on information security.		
<b>Where mitigations are required what are these?</b>	Ensure that laptops are encrypted and password		

	protected and staff are adequately trained.		
--	---	--	--

<b>Risk 1 -</b>	<b>DESCRIPTION</b>	<b>RISK LEVEL BEFORE ANY MITIGATION</b>	<b>RISK LEVEL AFTER MITIGATION</b>
<b>SOURCE OF RISK</b>	PA Consulting officers lose Camden laptops	low, because they are working exclusively in 5PS or working remotely)	Low
<b>Potential impact on individual</b>	Personal data stolen	Low	
<b>Threats that could lead to illegitimate access, undesired modification and disappearance of data:</b>	None		
<b>Any compliance or corporate risks?</b> Refer here to the corporate risk framework i.e. "you should also consider and apply the Council's Risk Framework when assessing the risk of your project as a whole."	Even if they are taking laptops away and working remotely, they will fall under the same risks and mitigations as Camden officers. ie – loss of laptop, encryption [REDACTED]	Low	Low
<b>Where mitigations are required what are these?</b>			

<b>Risk 2</b>	<b>DESCRIPTION</b>	<b>RISK LEVEL BEFORE ANY</b>	<b>RISK LEVEL AFTER MITIGATION</b>
---------------	--------------------	------------------------------	------------------------------------

		MITIGATION	
<b>SOURCE OF RISK</b>		Low	Low
<b>Potential impact on individual</b>	<b>Personal data stolen</b>		
<b>Threats that could lead to illegitimate access, undesired modification and disappearance of data:</b>	<b>None</b>		
<b>Any compliance or corporate risks?</b> Refer here to the corporate risk framework i.e. "you should also consider and apply the Council's Risk Framework when assessing the risk of your project as a whole."	This will fall under the same risks and mitigations as Camden officers and other IT/Data analysts who have access to personal data via qlik environment		
<b>Where mitigations are required what are these?</b>			

<b>Risk 3</b>	<b>DESCRIPTION</b>	<b>RISK LEVEL BEFORE ANY</b>	<b>RISK LEVEL AFTER MITIGATION</b>
---------------	--------------------	------------------------------	------------------------------------

		MITIGATION	
<b>SOURCE OF RISK</b>	PA Consulting access client data other than that necessary for the project.	Low	Low
<b>Potential impact on individual</b>			
<b>Threats that could lead to illegitimate access, undesired modification and disappearance of data:</b>			
<b>Any compliance or corporate risks?</b> Refer here to the corporate risk framework i.e. "you should also consider and apply the Council's Risk Framework when assessing the risk of your project as a whole."	This will fall under the same risks and mitigations as Camden officers and other IT/Data analysts who have access to personal data via qlik environment		
<b>Where mitigations are required what are these?</b>	Data will be provided by LBC reporting officers and access privileges to shared environments will be provisioned by LBC Business Intelligence team in alignment with standard operation procedure.		

**10. OVERALL RISK RATING, ONCE THE MITIGATING MEASURES HAVE BEEN PUT IN PLACE:**

<b>LOW</b>	<b>MODERATE</b>	<b>MEDIUM/ HIGH</b>	<b>HIGH</b>
------------	-----------------	---------------------	-------------

**ANNEX A  
DATA FLOW MAPS**

**ANNEX B Risk Assessment Tables**



**Table 1: Likelihood of Risk Occurring**

<b>Rare</b>	One-off failure
<b>Unlikely</b>	Possible that it may reoccur but not likely
<b>Possible</b>	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
<b>Likely</b>	Will reoccur on a regular basis, pointing to some failure in controls
<b>Almost Certain</b>	Wilful act, systemic failure in controls

**Table 2: Impact of Risk if it occurs**

<b>Negligible</b>	No personal data involved, or risk won't have any impact.
<b>Minor</b>	<ul style="list-style-type: none"> <li>• Short-term, minimal embarrassment to an individual</li> <li>• Would involve small amounts of sensitive personal data about an individual</li> <li>• Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)</li> </ul>
<b>Moderate</b>	<p><i>More than a minimal amount of sensitive personal data is involved at this level</i></p> <ul style="list-style-type: none"> <li>• Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family)</li> <li>• The potential of a financial loss for individuals concerned</li> <li>• Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services)</li> </ul>
<b>Major</b>	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns

<b>Catastrophic</b>	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)
---------------------	--

**Table 3: Risk Assessment**

	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
<b>IMPACT</b>	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Level of risk	
<b>1-3 Low Risk</b>	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
<b>4-6 Moderate Risk</b>	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
<b>8-12 Medium / High Risk</b>	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures

**15-25 High Risk**

Unacceptable

Immediate action must be taken to manage the risk

A number of control measures may be required

**ANNEX C**

--

**DPO ADVICE - add in anything not included above**