

# Data Protection Impact Assessment

A council-wide information document

Covid 19 – HealthIntent and council data for Covid vaccinations

5<sup>th</sup> May 2021

PUCO-44295.3029

This template and additional guidance may be found on the [DPIA SharePoint Page](#)



# 1 PROJECT AND STAKEHOLDER INFORMATION

## 1.1 Project/Programme/Work outline

Project Name	Covid 19 – HealthIntent Council data for Covid Vaccination Follow Ups
The Purpose of the Project	<p>This is a pilot to share the council's contact data with the NHS via HealthIntent to undertake a linkage (within HealthIntent) and see how well we do at getting additional contact details for the &gt;70s (mobiles / addresses that are different to EMIS).</p> <p>This will exclude ASC clients as the NHS has already provided their vaccination status to councils already and they are in the process of following up with ASC clients directly.</p> <p>If the pilot is successful, i.e. the data linkage works and yields contact details not already held by GPs, the plan is to expand the processing to other age groups and other councils across NCL.</p> <p>The Islington template is being used as it is a joint Islington Camden public health initiative although this DPIA focuses on Camden</p>
The desired outcomes of the project	To improve vaccination uptake in the estimated 20% of the over 70s in the area who have yet to have the vaccine.
How is the processing of data necessary to the work?	<p>GP Data for patients has been used to contact for the purposes of vaccination take-up, but a large number of patients have not responded. This may be due to data quality (patients not informing GPs of changes), "ghost" patients (patients who have moved away or registered elsewhere but not informed GPs) or because they do not wish to engage.</p> <p>To ensure that we have up-to-date data as far as possible, the local authority will share with the GPs records they have for patients who the GPs has been unable to contact.</p> <p>Small-scale research with Age UK / Manor Gardens indicates that of the 20% of the age group still unvaccinated, 10% are uncontactable. The other 10% are hesitant / waiting to see. The hope is that the data-matching will greatly improved GP outreach to this target group.</p>

<p>How much data will you be using and how often?</p>	<p>It is under 4000 patients. However, the plan is to supply all name, address and telephone numbers we have on file from the multiple data sources, therefore if an individual has three different addresses recorded across council systems, we will supply a copy of each variation in a flat-file.</p>
<p>Will the project collect new data or does it use existing data in a new way?</p>	<p>It takes existing council data, some of which is already shared with the NHS via HealthIntent for Covid 19 purposes (Council tax, Housing data, ASC) and some which isn't (Parking, My e-account) for data-matching purposes within the HealthIntent System.</p>
<p>When is the processing expected to start? If the project is time limited, please note the expected end date</p>	<p>Mid May Initially a one-off transfer of data.</p>

**1.1.1 Project/Programme/Work Description**

*You may use this box to provide a detailed description of the processing or to provide any additional information you feel is relevant.*

## 1.2 Project Stakeholders

Role	Participant (name(s))		
Project manager/ Person responsible for delivery	Mahnaz Shaukat		
Senior Responsible Officer for the Project	Sudip Trivedi		
Information Asset Owner	For guidance click <a href="#">here</a> Jenny Rowlands		
If the project requires the use of council datasets which belong to other directorates, please specify the directorate and the Information Asset Owner here.	Council Tax – Mark Stewart Council Housing, Leaseholders – Mary McGowan Accessible Transport – Rhys Mackinson Parking – Kate Robertson Electoral services – Clare Oakley		
Does the NHS National Data Opt Out apply to any of the datasets?	Is the project subject to Confidential Advisory Group (CAG) approval for purposes under Regulation 2 or 5 of the Control of Patient Information Regulations (2002), under s251 of the NHS Act 2006?  No		
Are there any joint data controllers in the project?	For guidance click <a href="#">here</a> Yes		
Name(s) of Digital Services representatives	Not applicable		
Is any of the project subject to a contract?	<b>Yes</b>	<input checked="" type="checkbox"/>	<b>No</b>
If Yes, please state the contract number and contract term.	<b>Contract Number</b>		The Data Processing Deed of Contract between NLP and NCL Clinical Commissioning Group
	<b>Contract Term</b>		

## 2 SCREENING QUESTIONS

Screening Questions	Y/N
Is there a requirement under GDPR to carry out a DPIA? See the guidance <a href="#">here</a> for further details. If you answer "Yes" to this question you do not need to answer the remainder of the screening questions and may proceed to Section 3 of this form.	Y
Does the project involve new or significantly changed processing of personal data about each individual?	Y
Will the project compel individuals to provide information about themselves?	N
Will information about individuals be shared with organisations or people who have not previously had routine access to the information?	Y
Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	N
Will the project result in you making decisions or treating individuals in ways which can have a significant impact on them?	N
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, sex life or sexual orientation or other information that people would consider to be private?	N
Will the project require contact with individuals in ways they may find intrusive, for example, unexpected telephone calls?	Y
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	Y
<b>Comments</b>	
<i>You may use this space to provide any supplementary comments regarding the answers you have given above.</i>	

If **all** questions are "**NO**", please return this document to the Information Governance Team at [dp@islington.gov.uk](mailto:dp@islington.gov.uk) and **do not** complete the remainder of this Data Protection Impact Assessment.

If **any** of the screening questions have been answered "**YES**", then please continue with the remainder of the Data Protection Impact Assessment.

### 3 DATA PROTECTION IMPACT ASSESSMENT

#### 3.1 Dataflow Map

Data Mapping Assessment	Y/N
<p>Has a Records of Processing Activity (ROPA) exercise been carried out?</p> <p><i>If "Yes" please provide a copy of the ROPA log entries when you submit this assessment. If "No" please ensure this is completed before processing starts. Speak to your local <a href="#">Information Lead</a> for guidance. <b>Please note that DPIAs will NOT be approved without at least an initial draft of ROPA being completed prior to submission.</b></i></p>	N

#### 3.2 Transfers of Data

<p>Is personal data transferred in an identifiable form?</p> <p><i>If yes, please use this space to describe how the information moves either internally, between departments or externally if other organisations are involved.</i></p> <p><i>Where is the data stored at the start of its journey and will it be moved to different locations? Who will have access to the data at different stages?</i></p> <p><i>Who are the recipients of the data? Consider internal and external recipients, including teams outside of your immediate team.</i></p>	<p>Yes, Name, address, telephone number and DOB (where available) will be sent in flat-file to NHS via usual secure email route. Data matching will occur with HealthInent.</p>
<p>Please describe all the media used for the transfer of data. NB This could be in a number of formats: courier, post, email, FTP.</p>	<p>Flat File CSV via secure mail</p>

#### 3.3 Controllers and Processors

	Y/N
<p>Are multiple organisations involved in the processing of the data?</p> <p><i>For guidance click <a href="#">here</a></i></p> <p><i>If you have answered "Yes" please fill out the table below. If you have answered "No" please move on to the next question.</i></p>	Y

Name of organisation	Controller or Processor?
Camden Council and GP Practices	Controllers
NCL Hospital Trusts	Controllers
GP Federations	Processors acting on GP/Controller instruction
NCL CCG	Data Processor acting on behalf of the Controllers
NEL CSU	Sub- Processor

Cerner Ltd	Sub-Processor
Cerner Corporation (USA)	Sub-Processor providing ICT resilience support to Cerner Limited (UK)

### 3.4 Describe the specific classes of data to be collected or processed

Personal data is any information which identifies a living person. Add "Y" to each field where applicable, otherwise leave blank.

<b>Personal Data</b>	<b>Y</b>	<b>Comments</b>
Name	Y	Full Name
Address data / postcode	Y	Both address and Postcode
Email Address	Y	Where available. Used to validate the over 70's cohort
Date of Birth	Y	Where available
Government issued ID – passport, driving licence		
Payroll Number		
HR / Employment data		
NHS Number		
Housing Data		
Online identifiers, including IP address and cookies		
Location data, GPS etc.		
<b>Special Category Data / Elevated Risk</b>	<b>Y</b>	<b>Comments</b>
Ethnicity		
Political Opinion / Affiliation		
Religious Beliefs		
Trade Union Membership		
Physical or Mental Health		
Sexuality / Sexual Life		
Criminal Offences		
Biometrics: Fingerprints, Retina, DNA profile		
Bank, credit card or financial details		
National Insurance Number		
Pension, Benefit or Tax Data		
Health and/ or Social Services Records	Y	By implication that the data matching concerns those who have not taken up the vaccination.
Children's data, child protection, school records, adoption		

<b>Please specify any other types of data not</b>	Telephone Number(s)
---	---------------------



<b>listed in the previous table.</b>	
--------------------------------------	--

### 3.5 Data Source(s)

If the data has not come from the data subject, where does the personal data come from?

Source	Comments
Previously collected by department carrying out the change	N
Previously collected by another Islington Council department	Y
Previously provided by a partner agency (eg, NHS, Police, Department of Work and Pensions)	Yes, will be matched with data held within HealtheIntent.
Does this project affect only data which will be collected once the change is made	N. Snapshot of council data currently held.

#### 3.5.1 Data Source Description

<p><i>You may use this box to provide a detailed description of the data sources for complex projects or projects using linked data sources.</i></p>
--

### 3.6 Who will access the data?

Categories of users	How users access the system and their intended use of the system
Council staff	Digital and data analysts and Camden council will compile the source data ready for transfer
Third party staff	NHS analysts conducting data-matching within HealtheIntent
Members of the public	N

### 3.7 The Data Protection Principles

Principle	Comments and risks
<p>Are you processing data as a statutory duty and if so, under what legislation?</p>	<p>You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of guidance that sets it out clearly: for example, “Duty to levy and collect Council Tax under Section 1 of the Local Government and Finance Act (1992)”</p> <p><b>Sharing of Health and Social Care Records</b>                      The Regulation 3(4) notice under the Control of Patient Information Regulations 2002 allows this sharing for the purposes of the pandemic. This work will be conducted under the instruction of the Director of Public Health for the local authority.</p> <p>Under the data protection regulations the processing of personal data for the purpose of health and social care provision is permitted under:                      The DPA section 8(c) – “the exercise of a function conferred on a person by an enactment or rule of law”, specifically the COPI Notice, NHS Act 2006 and the Health and Social Care Act 2012. This allows the legal basis of:                      UK GDPR Article 6(1)(e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</p> <p><b>And for special category personal data:</b></p> <p>The DPA section 10 (1) (c) – health and social care via Schedule 1 Part 1 section 2 “Health or social care purposes” satisfying DPA section 10 (2) of permitting the legal basis of:                      UK GDPR Article 9(2)(h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’</p> <p>The Common Law Duty of Confidentiality in processing and accessing Personal Confidential Data will be respected. The sharing will support the delivery of direct care for individuals and by health and care professionals with a legitimate right of access to the data.</p> <p>Each Partner shall be made aware of its obligation under the Health and Social Care (Safety and Quality) Act 2015, which inserted section 251A and B into the Health and Social Care Act 2012 and introduced a legal duty on health or adult social care commissioners or providers to share patients/service users’ information where doing so will facilitate health or social care and is in the patient/service users’ best interest.</p> <p><b>Sharing of non-health and social care records</b>                      The legal justification above is only suitable for health and social care records. For the other databases the legal justification is as follows.</p> <p>The Locality Act 2011 section 1 confers on local authorities the general power to undertake, activities for “the benefit of the authority, its area or persons resident or present in its area.” The restrictions on this power have been reviewed and are not applicable to this sharing.</p> <p>The Local Authority has determined that ensuring everyone is offered vaccination against the serious public health threat is a benefit to the area and persons resident or present. The Director of Public Health has agreed</p> <p>Under the data protection regulations the processing of personal data for the purpose of health and social care provision is permitted under:                      The DPA section 8(c) – “the exercise of a function conferred on a person by an enactment or rule of law”, specifically the COPI Notice, NHS Act 2006 and the Health and Social Care Act 2012. This allows the legal basis of:</p>

	<p>UK GDPR Article 6(1)(e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</p> <p><b>And for special category health personal data which is limited to the fact of non-vaccination:</b></p> <p>The DPA section 10 (1) (c) – health and social care via Schedule 1 Part 1 section 2 “Health or social care purposes” satisfying DPA section 10 (2) of permitting the legal basis of:</p> <p>UK GDPR Article 9(2)(h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’ Conducted under the supervision of the director of public health.</p> <p>Health and Social Care Act 2012 2B 3C</p> <p>“Each local Authority must take steps as it considers appropriate for improving the health of people in its area. The steps that may be taken under subsection (1) or (2) include...</p> <p>...(3c) providing services or facilities for the prevention, diagnosis or treatment of illness;”</p>
<p>Data is processed lawfully, fairly and in a transparent manner in relation to the data subject. Examples include:</p> <ul style="list-style-type: none"> <li>• Consent of data subject,</li> <li>• Contract with data subject,</li> <li>• Council under legal obligation,</li> <li>• Necessary to protect the vital interests of data subject,</li> <li>• Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</li> </ul>	<p><i>You will need to identify the legal basis using the GDPR article 6 (for personal data) and/or article 9 (for special category data) as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.</i></p> <p><i>Consent is not always necessary – however, where this is intended to be obtained, please provide a copy of the consent statement and a description of where consent is stored,</i></p> <p><a href="#"><u>(ICO Guidance on Lawful Basis for Processing)</u></a></p> <p><b>Article 6 Condition:</b> The processing of personal data into the HealthIntent system is permitted under the following paragraph:</p> <p>Article 6(1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</p> <p><b>Article 9 Condition</b></p> <p>And for special category health personal data which is limited to the fact of non-vaccination:</p> <p>The DPA section 10 (1) (c) – health and social care via Schedule 1 Part 1 section 2 “Health or social care purposes” satisfying DPA section 10 (2) of permitting the legal basis of:</p> <p>UK GDPR Article 9(2)(h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’ Conducted under the supervision of the director of public health.</p>
<p>The data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes</p>	<p><i>How will you ensure that personal data is only processed for its original intended purpose and not processed for additional purposes? How will function creep be prevented?</i></p> <p>Processing is carried out by health professionals under the instruction of the director of public health. Data matching will be carried out within HealthIntent system which is the approved solution for STP population health management NCL. Overarching DPIA has been carried out by NHS and is included alongside</p>

	<p>this Council DPIA which specifies clear and limited purpose for processing activity.</p>
<p>Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')</p>	<p><i>You should collect only the minimum data required for the intended processing activity. On the other hand, the amount of data needs to be sufficient to ensure that it can support effective decision making.</i></p> <p>Data is limited to Name, address, email address, dob telephone number for contacting target age group where we have failed to make contact. However, there is a risk that by the Council providing all variations of address and telephone number we have on record to the NHS we are not fully meeting data minimisation requirements.</p>
<p>Retention. The data must be held for no longer than required for this purpose.</p> <p>How long should this data be held?</p> <p>How will it be securely disposed or/permanently deleted?</p>	<p><i>Where there are concerns about the appropriate retention of data, this section will be reviewed by the Information Governance Team.</i></p> <p><a href="#"><u>Islington Retention Schedule</u></a></p> <p>Retention will be aligned with the end of the COPI notice. All data previously shared under this notice must be deleted when the COPI notice comes to an end so the approach taken will be to include these data too. This reduces the risk of some data flows being missed.</p>
<p>Are there measures in place to deal with data subjects' rights?</p> <p>Data subjects have the right to ask for a copy of their data – this must be provided within 30 days.</p> <p>Data subjects have the right to have incorrect data corrected</p> <p>Data subjects may ask the council to 'cease processing.' This could involve deleted data there is no legal reason to hold, or to desist from contacting them.</p>	<p><i>Where LBI (Camden) controls the data, data subjects' rights will be managed using existing Islington processes. However, where data is processed by a third party please detail the measures which are in place. If new technology is being introduced, consider how the technology helps us meet our obligations.</i></p> <p><a href="#"><u>(ICO Guidance on Data Subject Rights)</u></a></p> <p>The Council's Privacy notice <a href="http://www.camden.gov.uk/data-protection-privacy-and-cookies#yedw"><u>www.camden.gov.uk/data-protection-privacy-and-cookies#yedw</u></a> covers covid relating sharing states that "In this current pandemic we may share your information with other public authorities, emergency services, and other stakeholders as necessary and where it is proportionate to do so."</p> <p><b>Subject access requests</b> SARs will be managed by each Controller and Partner to the NLP Data Sharing Agreement.</p> <p>Very little in the HealthRecord and HealthRegistries applications is unique information, and any information is only kept in the platform whilst a patient is resident in the population or registered with an NLP GP Practice. Queries are run through the respective application via:</p> <ul style="list-style-type: none"> <li>• Web Portal or Millennium Mpages (route through to the Web) – the Cerner Sentinel audit tool are available for pulling subject access requests</li> <li>• EMIS Portal SDK (patient in context) – The EMIS audit tools, available within EMIS Web are available for pulling subject access requests when HealthRecord and HealthRegistries applications are accessed via this the EMIS web application (integrated route)</li> </ul>
<p>Data must not be transferred outside the EEA without appropriate provisions.</p> <p>Please confirm where the data will be stored, sent and where it will be accessed from.</p>	<p><i>EEA (European Economic Area) consists of EU member states and three European Free Trade Association (EFTA) states (Iceland, Liechtenstein, and Norway). Due to Britain leaving the EU, our current requirement is that Servers should be UK based.</i></p> <p>The HealthIntent solution will be hosted in a Cerner Data Centres in the UK:</p> <p>Equinix LD5, Slough Trading Estate, 8 Buckingham Ave, Slough, SL1 4AX</p>

<p>If a third party hosts or accesses the data you will need to confirm the location of the data in a written contract.</p>	<p>Disaster Recovery and backup is to be covered in Cerner's Pop Health/HeIntent SLSP (further referred to as the "Cerner SLSP"). Action confirmed by Cerner HoIG</p> <p>Cerner have a cold site Disaster Recover service* – back-ups of all platform data is held off site and will be deployed into back-up datacentre infrastructure in the event of a disaster.</p> <p>A cold-start DR service will require a long recovery period (over 24 hours probaly).</p> <p>Cerner Limited (UK) will not transfer data outside the EEA. However, access will be provided to Cerner US in the eventuality of a Hel system outage.</p> <p>Information re. Cerner data centres added to the Cerner SLSP as follows: Patient data will be stored and managed at Cerner UK Data Centres with a back-up incident management team available from the Cerner Corporation's (US) "Immediate Response Centre". Their access to data is in the eventuality of a system outage. Troubleshooting a system outage may lead to access to patient identifiable data.</p>
---	---

Risk Management

**3.7.1 Identify and assess risks**

All contributors to the DPIA should consider risks associated with the project and record any identified risks here:

Please attach a completed version of the DPIA Risk Register when you submit this form.



DPIA Risk Register\_  
HealthIntent Vaccina

### 3.8 Privacy Impact assessment: COMMENTARY

This section is to be completed by the Information Governance team

#### 3.8.1 DP Lead Comments

##### **Secondary use of proposed data sets:**

I shall be applying a standard test to help determine whether the proposed use of each dataset is within tolerance. Further processing is allowed in circumstances where:

1. the new purpose is compatible with the original purpose; we need to consider
  - any link between our original purpose and the new purpose;
  - the context in which we originally collected the personal data – in particular, our relationship with the individual and what they would reasonably expect;
  - the nature of the personal data – eg is it particularly sensitive;
  - the possible consequences for individuals of the new processing; and
  - whether there are appropriate safeguards - eg encryption or pseudonymisation.
2. we obtain the individual's specific consent for the new purpose; or
3. we can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

Council Tax, Open Electoral Register, ASC and Housing data has already been approved through the original Covid-19 HealthIntent for use and are already being shared with the NHS for Covid purposes.

Parking and My e-account data cannot be said to contain any logical link between their original purpose and the new purpose. In addition data subjects would have no reasonable expectation that their data collected for these original purposes may be repurposed in this way. This is offset by the following factors:

- a) data is not sensitive,
- b) processing is for the health benefits of the data subjects
- c) possible consequences for the data subject are negligible,
- d) HealthIntent is a secure system which rigorous IG and security standards and is the approved STP population health management system for NCL,
- e) While data is being transferred outside the Council the recipients are health professionals who adhere to NHS standards of Information Governance,
- f) We are relying on our statutory powers under the Health and Social Care Act in order to provide a lawful basis for the new processing activity.

On balance, I believe the further processing may be justified under the circumstances.

**Transparency**

These factors need to be considered in the context of our transparency obligations. For the purposes of this DPIA I shall be taking into account that the Council's website has had a specific COVID-19 privacy notice in place which details sharing and the conditions under which it may take place.

I am satisfied that this provides a fairly broad platform upon which the Council has explained its position with regards to further processing of Council datasets. I recommend that the Privacy notice for Covid is reviewed to ensure it accurately reflects our current position particularly if the pilot is extended to other age groups and other councils.

**Does the COPI notice apply to the datasets?**

There is an argument to be made that because the ultimate purpose for data sharing etc is for a health and social care that the COPI notice should apply to all data used to this end. However, in my opinion this would be a very liberal interpretation of the notice and the very definition of Confidential Patient Information limits the application to personal data relating just to those receiving social care and for the data to be descriptive of their care or treatment. So while ASC care records may fall in scope, other council datasets would not. For this reason, and following discussions with Steve Durbin, we have decided not to rely on the COPI notice and instead are relying on the Health and Social Care Act 2012 Section 12 3C.

Proposed Review Date:

30<sup>th</sup> September 2021



## 4 RISK ASSESSMENT: AUTHORISATION FOR LINKED DATASETS

Use this section in cases where the project will be using or combining data from other directorates and therefore requires additional authorisation from the directorates responsible for the source data.

### 4.1 Service Area IGWG representative ([guidance](#))

Name	Not applicable
Job Title	
Telephone	
Signature	
Date	

### 4.2 Islington Digital Services authorisation (where applicable)

Name	Not applicable
Job Title	
Telephone	
Signature	
Date	
IDS Risk Assessment	<i>Please attach a copy of the Risk Assessment if one was carried out on this project.</i>

### 4.3 Linked Data Information Asset Owner / Risk Owner

Name	Mahnaz Shaukat
Job Title	Head of Health and Care Intelligence
Telephone	020 7527 3860
Comments	

Signature	
Date	


As the overall risk owner for the project, I agree with this risk assessment and accept the risks as described in this document. I confirm that I have read the "Islington ICT Security Policy Framework" and assert that nothing in this risk assessment is in conflict with this overarching framework.

I am aware that the council needs to adhere to the Data Protection Act (2018) and in particular Section 56 that all organisations commit to: "Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part."

I am also aware that we must comply with the terms of the General Data Protection Regulations and any revised UK Data Protection legislation.

I confirm that while accepting the risks stated in this risk assessment, that I have not breached any of the above legislative requirements.

#### 4.4 Data Protection Officer comments

Name	Andrew Maughan
Job Title	Data Protection Officer
Comments	Agreed
Signature	
Date	11 <sup>th</sup> May 2021

## 5 APPENDIX 1: GUIDANCE NOTES

### 5.1 Legal requirement to conduct a DPIA

Conducting a DPIA is a legal requirement of the GDPR in certain circumstances where there is a high risk to privacy. A DPIA will be mandatory where the council plans 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 new technologies.

- 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.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- 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 which could result in a risk of physical harm in the event of a security breach

\*Large Scale - the GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing.

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.
- Individual professionals processing patient or client data are not processing on a large scale.

Examples of where a DPIA would be appropriate

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications
- The collection of new data on an existing system

[Back to Screening Questions](#)

## 5.2 Controllers and Processors

When answering this question, please consider that suppliers, software providers etc will count as other organisations as well as partner agencies.

**'Controller'** means alone or jointly with others, the name of the organisation that determines the purposes and means of the processing of personal data

**'Processor'** means the organisation that is processing personal data under the instruction of a Controller and does not determine the purposes and means of the processing

**'Joint Controller'** means two or more Controllers who decide the purposes and means of processing together – they have the same or shared purposes. Controllers will not be Joint Controllers if they are processing the same data for different purposes. (Article 26 (1), GDPR).

## 6 APPENDIX 2: LINKED DATA DPIA PROCESS

