**Data Protection Impact Assessment Questionnaire**

**Version 4**

Information Governance Team

**Document revision history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Revision | Comment | Author / Editor |
| May 2019 | 3 | Final | Merged the previous 2 documents (threshold assessment and DPAI) into 1 document.  Replacing current LBTH version to align with those used by NHS partners. | Head of Information Security |
| Aug | 4 | Final | Updated version | Head of Information Security, Head of Information Governance & The Data Protection Officer |

**Document approval**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Revision | Role of approver | Approver |
| May 2019 | 3 | Final |  | Information Governance Group |
| Aug 2019 | 4 | Final |  | Information Governance Group |

# Do I Need to Complete a Data Protection Impact Assessment questionnaire?

No need to conduct a full Data Protection Impact Assessment questionnaire. Complete the screening questions (up to page 6 of this document) and note why a full DPIA is not required.

Yes

Document in the business case and/or project documentation

Are you about to start a new project, implement a new system, service, or change the way you work?

No

Yes

No

Does this project involve the collection, recording, storing or processing of personal-confidential data?

Complete a Data Protection Impact Assessment questionnaire.

Send completed Data Protection Assessment to the Council DPO. You may be asked to provide supporting information e.g. contract, system specification, consent forms etc.

When deciding whether a DPIA questionnaire is required, if the first answer is ‘yes’, but the second response is ‘unsure’, please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: DPO@towerhamlets.gov.uk.

It is a requirement of the General Data Protection Regulation that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the DPO and Head of Information Security, and you will be notified of the recommendation from the questionnaire. This could be either:

* + 1. A more detailed response is required where the new process or change of use of Personal data requires more thorough investigation.
    2. The DPIA questionnaire will be signed off by the DPO and Head of Information Security.

**Basic Information**

|  |  |
| --- | --- |
| Project/Service Lead contact details | |
| Your Name |  |
| Job Title |  |
| Your location |  |
| Your telephone number |  |
| Your email address |  |
| Your team |  |
| Your directorate |  |
| Information Asset Owner  (if different from above) |  |

|  |  |
| --- | --- |
| Purpose of the Project/Service | |
| Project/Service Name |  |
| In brief, what is the purpose of the project/service and how is the processing of information necessary to that work?  Please include expected outcomes. |  |
| Does the project require a service provider?  If so, has the contract been awarded?  Please specify the name of the service provider |  |

|  |  |
| --- | --- |
| Timeframe for the Project/Service | |
| When is the Project/Service due to begin? If it’s time limited, please note the expected end/review date. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nature of Information | | | | |
|  | | | | |
| Will all of the information be truly anonymised information[[1]](#footnote-1)?  Anonymised data must meet [the ICO code of practice](https://icosearch.ico.org.uk/s/redirect?collection=ico-meta&url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1061%2Fanonymisation-code.pdf&index_url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1061%2Fanonymisation-code.pdf&auth=mDAlWp%2BBK%2B03Se03OnHpRQ&profile=_default&rank=3&query=anonymisation). | Yes |  | No – some of the information will relate to an identified or an identifiable person (either directly or indirectly) |  |
| Will the information be new information as opposed to using existing information in different ways? | | | . | |

|  |  |
| --- | --- |
| **Key Contacts** | |
| Key Stakeholder Names & Roles: |  |
| Date: |  |

| **Screening Questions** | **YES or NO** |
| --- | --- |
| Will the project involve the collection of information about individuals? |  |
| Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business? |  |
| Will the project compel individuals to provide information about themselves? |  |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |  |
| Are you using information about individuals for a new purpose or in a new way that is different from any existing use? |  |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make a decision about care that’s automated. |  |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on them? E.g. service planning, commissioning of new services |  |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of a particular service being provided?.  **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is “**No**”. |  |
| Will the project require you to contact individuals in ways which they may find intrusive? |  |
| Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners? |  |
| Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual in a database? |  |
| Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources? |  |

If any of the screening questions have been answered “YES”, then please continue with the full Data Protection Impact Assessment Questionnaire (below).

If all questions are “NO”, please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment. Please email the completed screening to [DPO@towerhamlets.gov.uk](mailto:nelcsu.Information-Governance@nhs.net)

**Controller/s[[2]](#footnote-2) and Processors[[3]](#footnote-3)**

|  |  |  |
| --- | --- | --- |
| **Are multiple organisations involved in processing the data?** *If yes, list below* | | Yes/No |
|  |
| Name of Organisation | Controller or Processor? |  |
| Yes/No |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Has a data flow mapping exercise been undertaken?**  *If yes, please provide a copy, if no, please ensure this is completed – see Appendix 2, Note 4 for guidance* | | Yes/No |
|  |

**Personal data[[4]](#footnote-4)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Use of personal information** | | | | |
| Why is personal data required for this project/system/process |  | | | |
| Please confirm that you will be using only the minimum amount of personal data that is necessary. |  | | | |
| Would it be possible for the Controller/s to use pseudonymised[[5]](#footnote-5) data for any element of the processing? | Yes |  | No |  |
| If Yes, please describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals. |  | | | |

|  |
| --- |
| **Description of data: National and local data flows containing personal and identifiable personal information.** What are the required personal data items? |

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Personal Data** | **Please tick all that apply** |  | **Please tick all that apply** |
| Name |  | Racial / ethnic origin |  |
| Address (home or business) |  | Political opinions |  |
| Postcode |  | Religious beliefs |  |
| NHS No |  | Trade union membership |  |
| Email address |  | Physical or mental health |  |
| Date of birth |  | Sexual life |  |
| Payroll number |  | Criminal offences |  |
| Driving Licence [shows date of birth and first part of surname] |  | Biometrics; DNA profile, fingerprints |  |
| Please supply a dummy sample, e.g. blank forms or an itemised list of the data items. | | Bank, financial or credit card details |  |
| Mother’s maiden name |  |
| National Insurance number |  |
| Tax, benefit or pension Records |  |
| Health, adoption, employment, school, Social Services, housing records |  |
| Child Protection |  |
| Safeguarding Adults |  |
| Additional data types (if relevant) | |  | |

**You will also need to identify the lawful basis using the GDPR article 6 (for personal data) and article 9 (for special category data) conditions met, as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.**

**If you are processing personal and special category data for the purposes of law enforcement purposes, please select the appropriate box below.**

**The Data Protection Officer can assist you identifying the lawful basis for processing data**

|  |  |
| --- | --- |
| **Lawful basis for processing personal data under Article 6 of the GDPR** | |
| **Personal data** (eg: Name, address, D.O.B, NI number etc) | |
| **Consent** – The individual has given clear consent for you to process their personal data |  |
| **Contract** – The processing is necessary for a contract you have with the individual, or they have asked you to take specific steps before entering into a contract |  |
| **Legal Obligation** – The processing is necessary for you to comply with the law |  |
| **Vital interests** – The processing is necessary to protect someone’s life |  |
| **Public Task** – The processing is necessary to perform a task in the public interest or for your official functions or and the task function has a clear basis in law |  |

|  |  |
| --- | --- |
| Lawful basis for processing personal data law enforcement purposes under Part 3 of the Data Protection Act 2018 | |
|  | |
| Law Enforcement Purposes – processing is necessary for the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. - |  |

|  |  |
| --- | --- |
| Lawful basis for processing special category data under Article 9 of the GDPR or for lawful enforcement purposes under Schedule 8 of the Data Protection Act 2018 | |
| Special category data (eg: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. | |
| Explicit consent - the data subject has given explicit consent to the processing of those personal data (not required for processing for lawful enforcement purposes) |  |
| Employment, Social Security or Social Protection Law - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller under employment, social security or social protection law |  |
| Vital Interest –to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent |  |
| Not for profit body - processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body |  |
| Information in the public domain - processing relates to personal data which are manifestly made public by the data subject |  |
| Legal claim - processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |  |
| Public Interest - processing is necessary for reasons of substantial public interest (eg: detection or prevention of unlawful acts, prevention of fraud, Safeguarding of children and/or individuals at risk, Counselling etc.) [NB: The Data Protection Officer can assist in identifying whether there is a substantial public interest involved] |  |
| Medical, Health or Social Care – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services |  |
| Public Health - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices |  |
| Archiving, scientific or research - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |  |

|  |  |
| --- | --- |
| **Describe the information flows**  The collection, use and deletion of personal data must be documented. | |
| Please explain how the data is collected and then processed.  Please include a data flow map if available |  |
| Please describe all media used to collect process and store the data?  (e.g. Case/data management system, email, fax, post, courier, secure electronic means [e.g. Egress], other – please specify all that will be used) |  |

| **Answer all the questions below for the processing of Personal Identifiable Data** | |
| --- | --- |
| Briefly explain why you have selected the above lawful basis for processing personal data?  If relying on consent, please include a copy of your consent form when you submit this DPIA |  |
| Where and how will this data be stored?  If the data will be hosted by an external supplier in the cloud, please ask the supplier to complete the NCSC Cloud Security Principles. |  |
| Who will be able to access the identifiable personal data being collected, processed and stored? |  |
| How will you ensure the personal data has been accurately processed (including their rectification or erasure upen request from the data subject where necessary)? |  |
| How will you monitor and maintain the quality of the personal data being collected and processed? |  |
| Will the data be linked with any other data collections, systems, projects or processes?  If so, please specify the other data collections |  |
| How will this linkage of this data to other systems be achieved? |  |
| Is there a lawful basis for these linkages? i.e. is the Controller/s responsible for the data expected to co-operate/link data to carry out their legal obligations. |  |
| If the data will be or is being collected by the Council or on behalf of the Council, explain how the privacy notice will be brought to the attention of the data subjects |  |
| Please provide a link or insert a document of the privacy notice |  |
| What security measures will be used when the data is being collected and processed? |  |
| What confidentiality and security measures will be used to store the data? |  |
| How long will the data be retained in personal identifiable form? And how will it be de-identified? Or destroyed? |  |
| Are there any plans to allow the data to be used elsewhere either in the Council, or by a third party? |  |
| What procedures and policies are in place to oversee the confidentiality, security and appropriate use of the data disclosure to third parties where appropriate? |  |
| Are procedures in place to provide access to records under the subject access provisions of the DPA?  Is there functionality to respect objections/ withdrawals of consent, if consent was a lawful basis |  |
|  |  |
|  |  |

**Access and reporting**

|  |  |  |
| --- | --- | --- |
| What access controls will you have in place to ensure there is only authorised access? Please include your procedure for enabling, monitoring access and identifying any inappropriate access. | | |
|  | | |
| **Are there any new or additional reporting requirements for this project/service?** | | Yes/No |
|  |
| What roles will be able to run reports? | | |
|  | | |
| What roles will receive the report or where will it be published? | | |
|  | | |
| Will the reports be in person-identifiable, pseudonymised or anonymised format? | | |
|  | | |
| Will the reports contain personal identifiable data or will they be redacted in anyway | | |
|  | | |
| If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of? | Yes/No | |
|  | |
| What plans are in place in relation to the internal reporting of a personal data breach?  (NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.) | | |
|  | | |
| What plans are in place in relation to the notification of data subjects should there be a personal data breach?  (NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.) | | |
|  | | |

**Business continuity planning**

|  |  |
| --- | --- |
| How will the personal data be restored in a timely manner in the event of a physical or technical incident? |  |

**Direct marketing[[6]](#footnote-6)**

|  |  |  |
| --- | --- | --- |
| Will any personal data be processed for direct marketing purposes? | Yes/No |  |
| If Yes, please describe how the proposed direct marketing will take place: |  | |

**Automated processing**

|  |  |  |
| --- | --- | --- |
| Will the processing result in a decision being made about the data subject solely because of automated processing[[7]](#footnote-7) (including profiling[[8]](#footnote-8))? | Yes/No |  |
| If Yes, is the decision:   * necessary for entering into, or performance of, a contract between the data subject and a data controller * authorised by law * based on the data subject’s explicit consent? |  | |
| Please describe the logic involved in any automated decision-making. |  | |

**Risk Management**

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA. Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the Council’s Data Protection Officer for review and approval. Any DPIA risks that score as high risk will only have the processing of the data approved once the risk has either mitigated to reduce the risk to medium as a minimum or where this is not possible, a high risk score will require escalation to the Council’s (Senior Information Risk Owner) SIRO. The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible.

|  |  |
| --- | --- |
|  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Risks**  List any identified risks to Data Protection and personal information of which the project is currently aware.  Risks should also be included on the project risk register. | | | | | | |
| **Risk Description**  **(to individuals, to the LBTH or to wider compliance)** | **Current Impact** | **Current Likelihood** | **Risk Score (I x L)** | **Proposed Risk solution (Mitigation)** | **Is the risk reduced, transferred, or accepted? Please specify.** | **Evaluation: is the final**  **impact on individuals**  **after implementing each**  **solution a justified,**  **compliant and**  **proportionate response**  **to the aims of the project?** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Approval by IG Team/Information Security | | | |
| Risk Description | Approved solution | Approved by | Date of approval |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Actions to be taken** | | |
| **Action to be taken** | **Date of Completion** | **Action Owner** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Consultation requirements**  Part of any project is consultation with stakeholders and other parties. In addition to those indicated “Key information, above”, please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information.  It is the project/service lead’s responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations. |
|  |
| **Further information/Attachments**  Please provide any further information that will help in determining Data Protection impact.  See Appendix 2, note 5 for examples |
|  |

|  |
| --- |
| **Data Protection Officer comments:** |
|  |

|  |
| --- |
| **Head of Information Security comments:** |
|  |

Following review of this DPIA by the Information Governance Team, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. No action is required by IG excepting the logging of the Screening Questions for recording purposes.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.

**It is the intention that IG will advise and guide those projects that require IG compliance but at all times will endeavour to ensure that the project moves forward and that IG is not a barrier unless significant risks come to light which cannot be addressed as part of the project/service development and will need to be escalated to the Council’s Senior Information Risk Owner- SIRO for approval.**

**The DPIA Process**

The DPIA process can be displayed as the process diagram below. All stages of the process must be followed in order to ensure compliance.

Any processing that, once risk assessed, is identified as high-risk processing will require the review of the Data Protection Officer and Head of Information Security. If the risk cannot be reduced, then the approval of the SIRO and if necessary the ICO is required before processing can commence.

Complete DPIA Questionnaire

Obtain IG review

Add to DPIA Log

Project/New Process Start

Implement any necessary actions in agreed timescales.

You may be asked

to provide supporting information e.g. contract, system specification, consent forms etc.

You must document and may be asked to provide

assurance that the agreed IG actions have been implemented and are effective on privacy

You may be required

to include recommendations from the DPO or Head of Information Security.

Post implementation reviews for subsequent changes and conduct a new DPIA if required.

Request IAO/ approval

Please email entire completed document to [DPO@towerhamlets.gov.uk](mailto:DPO@towerhamlets.gov.uk)

**Information Security review**

**IG staff name**:

**Signature:**

**Date:**

**Information Asset Owner (IAO) approval**

**IAO name:**

**Signature:**

**Date:**

**Data Protection Officer (DPO) approval**

**DPO name:**

**Signature:**

**Date:**

**Appendix 1-** **The conditions (the lawful basis) for processing Personal Data under the Data Protection Legislation**

The conditions for processing Personal Data and Sensitive Personal Data the Data Protection Legislation, Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation.

**Definition of Personal Data and Sensitive Personal Data**

**Data:**

* The Data Protection Act defines data as:
  + Information which is being processed automatically in response to instruction
  + Information recorded as part of a highly structured filing system (e.g. an individual with limited knowledge of the filing structure could logically retrieve relevant information)
  + Recorded information held by a public authority
  + Information that forms part of an accessible record (health, educational, public record)

**Personal Data:**

* Personal data means data which relates to a living person who can be identified from that set of data or who could be identified if that data was combined with other information either available or likely to become available.
* This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
* **Special Category Data**
* The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Special Categories of personal dataE+W+S+N.I. includes Information relating to the data subjects’:

* racial or ethnic origin,
* political opinions,
* religious beliefs or other beliefs of a similar nature,
* trade union membership,
* physical or mental health or condition,
* sexual life,
* the commission or alleged commission by him of any offence, or
* any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act (DPA) outlines 6 principles for handling Personal Confidential Data (PCD), with 2 additional safeguards:

1. Data must be processed fairly and lawfully
2. Data must be obtained and processed only for one or more specified, explicit and lawful purposes
3. Date must be adequate, relevant and not excessive in relation to the purpose
4. Data must be accurate and kept up to date
5. Data must not be kept for longer than is necessary
6. Appropriate technical and organisational security measures for the data must be in place

Safeguards:

1. Data must be processed in accordance with the rights of data subjects
2. Sensitive Data must only be processed with legal compliance to the Act, referenced to a current policy. e.g. Can only be processed in a country or territory outside the United Kingdom unless adequate levels of protection are in place, within statutory functions.

**Lawfulness of processing**

What follows is copied directly from the Data Protection Act 2018.

*Data Protection Act 2018 (c.* ***12****)*

*Part 2 — General processing*

*Chapter 2 — The GDPR*

**8 Lawfulness of processing: public interest etc**

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller’s official authority includes processing of personal data that is necessary for—

(a) the administration of justice,

(b) the exercise of a function of either House of Parliament,

(c) the exercise of a function conferred on a person by an enactment or rule of law,

(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or

(e) an activity that supports or promotes democratic engagement.

*Special categories of personal data*

**10 Special categories of personal data and criminal convictions etc data**

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health);

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

(i) by adding or varying conditions or safeguards, and

(ii) by omitting conditions or safeguards added by regulations under this section, and

(b) consequentially amend this section.

(7) Regulations under this section are subject to the affirmative resolution procedure.

**11 Special categories of personal data etc: supplementary**

(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the responsibility of a health professional or a social work professional, or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—

(a) the alleged commission of offences by the data subject, or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

**Appendix 2**

|  |  |
| --- | --- |
| **Supporting Guidance for Completion of the Data Protection Impact Assessment** | |
|  | **Information Asset**  **E.g. Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, devices/equipment, records and information (extensive list).** |
|  | **New use of information could include: - consistent with DPIA Introduction** |
| Setting up of a new service.  The Commissioning of a new service Data Extracts  Setting up a database or independent Patient System  Reports |
| **Examples of changes to use of information could include:** |
| Moving paper files to electronic systems  Collecting more data than before  Using Data Extracts for a different purpose  Additional organisations involved in information process  Revisions to systems, databases (including merges) or spread sheet reports |
|  | **Data Flow Mapping** |
| A Data Flow Map is a graphical representation of the data flow. This should include:   * Incoming and outgoing data * Organisations and/or people sending/receiving information * Storage for the ‘Data at Rest’ i.e. system, filing cabinet * Methods of transfer |
|  | **Examples of additional documentation which may be required** *(copies)***:** |
| * Contracts * Confidentiality Agreements * Project Specification * System Specifications (including Access Controls) * Local Access Controls Applications * Information provided to patients * Consent forms |

1. anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable [↑](#footnote-ref-1)
2. 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function [↑](#footnote-ref-2)
3. ‘Processor’ means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data [↑](#footnote-ref-3)
4. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [↑](#footnote-ref-4)
5. 'pseudonymised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [↑](#footnote-ref-5)
6. direct marketing is “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals” - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations [↑](#footnote-ref-6)
7. examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention [↑](#footnote-ref-7)
8. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [↑](#footnote-ref-8)