Information Governance Support

Nottinghamshire County Council
in partnership with
Essex County Council

PRIVACY IMPACT ASSESSMENT - GUIDANCE

Approved by	Miss Jane Avison (Chair of Governors)
Date Approved	Summer 2023
Version	4
Review Date	Summer 2026

Contents

Guidance

The Proposal

Identify the project by a title and provide a summary description of what it to be implemented; focussing on the data to be processed.

DPIA Risk Assessment

Does the processing meet the criteria below? (Further guidance awaited from the ICO)

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.
    - systematic and extensive processing activities, including profiling
    - and where decisions that have legal effects – or similarly significant effects – on individuals.
    - large scale processing of special categories of data or personal data relation to criminal convictions or offences.
- This includes:
    - processing a considerable amount of personal data at regional, national or supranational level;
    - that affects a large number of individuals; and
    - involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
    - large scale, systematic monitoring of public areas (CCTV).

The Data

Describe the Data

Identify all the relevant data that will be processed. Where the project is for a new system which stores data in data fields, then the field titles would be required here. Classify each item according to its sensitivity in line with HM Government Security Classification Policy

Format(s) in which the Data will be Processed

Clarify the format in which the data will be held remembering that a data item may be held in more than one format. Select as many that apply.

Special Categories

Clarify whether any of the data to be processed falls within the special categories.

Categories of Data Subject

Specify whose data will be processed. The common categories processed by the organisation should already be identified on the record under the Register of Data Controllers.

Data Risk Profile

Refer to the Risk Treatment Process to identify the overall risk profile for the proposed project

The Principles

Processed lawfully, fairly and in a transparent manner

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals (Article 5(1)(a))

(Article 5, Recital 39) (Guidance)

i. Legal basis for Processing

Conditions for processing

Select however many conditions are applicable ensuring that if the data being processed is both personal data and a special category, then a relevant condition is chosen from both categories

Personal Data:

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 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
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Special Categories:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- 9(2)(i) – 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 healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Legal Gateway

List the relevant legislation which specifically permits the processing of personal data in the way intended

Consent management

We are encouraged to not rely on consent. If it is used however, the following should be in place:

- The capability to produce, on request, documented (and standalone) evidence that an individual data subject has consented to the processing
- Processes in place to manage the withdrawal of consent
- Capability to distinguish and appropriately manage data processed pre- and post-withdrawal of consent
- Consent is freely given (the data subject has a genuine choice whether to provide consent or not), well-informed and clearly expressed
- Data will not be obtained from data subjects under 13 years old, OR if it will, processes for obtaining parental consent/ authorisation are in place

ii. Rights

a) To be informed

Privacy Notices must:

- Be concise, transparent, intelligible and easily accessible?
- Be written in clear and plain language, particularly if addressed to a child?
- Be free of charge?
- Contain:
    - Identity and contact details of the DC, DP (if applicable) & DPO
    - Purpose of processing & legal basis for the processing
    - Legitimate Interests of the DC or 3rd Party (where applicable)
    - Any recipient (or categories of recipients) of the data
    - Any transfers to 3rd country and details of the adequate safeguards
    - Retention period (or criteria used to determine one)
    - Existence of each of DS's rights
    - DS's right to withdraw consent at any time (where relevant)
    - DS's right to lodge a complaint with the ICO
    - Any automated decision making/ profiling and information about:
        - How decisions are made,
        - Significance and consequences.
    - (Where data is obtained directly from the DS):
        - The statutory/ contractual requirement/ obligation
        - The consequences of not providing personal data
    - Where data is not obtained directly from the data subject:
        - Source of the data and whether from publicly accessible sources
        - Categories of personal data
- Be provided:
    - At the time data is obtained (if direct from DS)
    - Before 1st communication takes place (if not obtained from DS and if data is to be used to communicate with DS)

- Before data is disclosed/ within one month of obtaining (if not obtained from DS and is to be disclosed to a third party)

(Articles 12,13 & 14, Recitals 58-62) (Guidance)

b) Access

In order to support the right of access, the activity must:

- Be able to confirm that a DS's personal data is being processed
- Be able to provide that data in hard-copy and electronic formats (and ideally though self-service means)
- Be supported by an accurate privacy notice which was current at the time the data was obtained

(Articles 12, 15, Recital 63) (Guidance)

c) Rectification

In order to support the right to ensure accuracy:

- Is the activity supported by adequate processes to safeguard the individual's right to have personal data rectified if it is inaccurate or incomplete?
- Can this be achieved within 1 month (2 if complex) of receiving a request?
- Does the service have processes in place to ensure that requests can be effectively denied if they disagree with valid professional opinion and look to accommodate adding the DS's objections rather than delete data?

(Articles 12,16 & 19) (Guidance)

d) Erasure

In order to assist with the right to erasure:

- If the legal circumstances are applicable, can the activity support the right to erasure (the 'right to be forgotten') by us and any 3rd parties with whom the data has been shared?

(Articles 17 & 19, Recital 65 & 66)(Guidance)

e) Restrict Processing

In order to assist with the right to restrict processing:

- If the legal circumstances are applicable, can the activity support the right to restrict processing, i.e. when processing is restricted, you are permitted to store the personal data, but not further process it? You can retain just enough information about the individual to ensure that the restriction is respected in future.

(Articles 18 & 19, Recital 67)(Guidance)

f) Data Portability

In order to support the right to data portability:

- If the legal circumstances are applicable, can the activity support the transfer of personal data to a 3rd party?
- The right to data portability only applies:
  - to personal data an individual has provided to a controller;
  - where the processing is based on the individual's consent or for the performance of a contract; and
  - when processing is carried out by automated means

(Articles 12 & 20, Recital 68)(Guidance)

g) Object

In order to support the right to object:

- If the legal circumstances are applicable, can the change support the right to object and to stop processing by us and any 3rd parties with whom the data has been shared?

(Articles 12 & 21, Recitals 69-70)(Guidance)

h) Automated Decision-making and Profiling:

In order to support the right to challenge automated decision making and profiling:

- Where the legal circumstances are applicable, are there processes in place for the activity to support the DS's rights to:
  - Obtain human intervention
  - Express their point of view
  - Obtain an explanation of the decision and
  - Challenge the decision

(Articles 4, 9 & 22, Recitals 71-72) (Guidance)

iii. Data Subject consultation

Note any consultation undertaken with Data Subjects to ascertain their views on the appropriateness of processing their personal data in the manner proposed

Collected for specified, explicit and legitimate purposes

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

(Article 5(1)(b))

- List the purposes which justify the intended processing
- List any intended further processing and assess whether this is compatible with the stated purposes
- Ensure all intended processing is captured in the privacy notice

Adequate, Relevant and Limited

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

(Article 5(1)(c))

- Assess whether the personal data being processed is:
    a. sufficient for the stated purposes
    b. entirely relevant to the purposes
    c. limited so as not to be excessive for the purposes
- Note any consideration of anonymization or pseudonymisation being proposed in order to prevent personal data being processed unnecessarily
- How will the 'Ano/Pseudo' process work, and in particular, at what stage will the process take place?

Accurate and, where necessary, kept up to date

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(Article 5(1)(d))

- Establish:
    a. How the service will be managed to ensure data accuracy is maintained
    b. How DSs are made aware of the need to advise of changes to personal data or able to access facilities to amend it themselves

Kept for no longer than is necessary

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(Article 5(1)(e))

- There is a clear understanding of when in the lifecycle of delivering the service a need to process the data will end
- This is derived from the our Retention Schedule
- List the retention periods
- At the end of the retention period there is a facility which allows a user (with sufficient rights) to delay deletion in the event of complaints/ statutory information requests/ enquiries and investigations
- A deletion process meets the requirements of Principle 5(1)(f)
- Where personal data is processed beyond a retention period it is in line with the accepted purposes above and appropriate safeguards are in place

Appropriate Security

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(Article 5(1)(f))

i. Organisational Controls

    a) Procurement

The Tender Process

The risk rating determined in Section 3 confirms the level of assurance required from the prospective suppliers and the preferred bidder. Stage 1 means the suppliers need only need to supply self-assessment assurance statements. Stage 1 & 2 means that the supplier needs to undertake Stage 1, and then if successful, needs to supply evidence to support their statements under Stage 2.

Contractual Control

Confirm that the contract provided to the winning supplier contains our standard Information Handling schedule. Or if the contract does not contain the standard clauses, why, what is in place instead, and how does this represent an acceptable equivalent control?

Contract Term

Enter the formal commencement and end date for the contract and if the contract includes a facility to extend beyond the end date for a further period, what is that extension period?

The Selected Supplier

Up to 25th May 2018, the ICO required Data Controllers to notify them of the categories of personal data processed by them. In some cases suppliers may not meet the criteria for needing to notify. If the winning bidder has notified, record their details from the online register. If they state that they do not need to notify, confirm their written statement that supports this.

There is scope in this section to record more than one supplier. This is in the event that the contract is a framework, where we may decide to have a number of successful bidders to whom we can offer work in a competitive bidding scenario.

b) Training

Confirm that employees will be effectively trained in a system and/or supporting processes, and also that they will sufficient reference material to access when they need ongoing support.

c) Policy

Record here any instance where the consideration of the processing in this assessment has highlighted an issue with our policies where a current policy may be

too restrictive or there is an absence of a policy statement in an area. Identify the issue and ensure it is referred to the employee responsible for Policy Reviews.

ii. Technical Security Controls

a) Access Controls

This section confirms that an assessment has been made of the access controls. To be accepted, the proposed controls need to make sure that a system owner can control which users have what rights to access and amend the data. This includes (if applicable) how the system will identify that the user attempting to access the data will be validated as having the right credentials.

b) Security at Rest

This section confirms that an assessment has been made of the security of the system where the data is going to be stored. This requires an analysis of:

- Where the data will be held?
- Business continuity and disaster recovery provisions?
- The location of the store?
- What level of access is provided to support staff?
- From what global locations can support staff access the data from?

c) Security in Transit

This section confirms that an assessment has been made of the security of the data when it is being transferred from one location to another either over the internet, secure network, on email or via a type of media storage which is then physically transported.

Records of Processing Activity

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

(Article 5(2))

Ensure that any change to the Record of Processing Activity (new, amended or deleted Information Assets or Flows) is recorded on the ROPA system

Transfer Outside the EEA

If it anticipated that there will be occasions where it is necessary to transfer data outside the EEA (to Third Countries or International Organisations), the following must be in place:

- Is the country (or territory/ processing sector) or organisation approved by the EU/ICO as having an adequate level of protection? (A41)
- Are there appropriate safeguards in place in a legal contract/ agreement? (A42/43)
- If there is no Adequacy decision or appropriate safeguards, do any of the following apply in order to establish validity? (A44)
    - (a) Consent has been given
    - (b) Performance of a Contract
    - (c) Conclusion/ Performance of a Contract
    - (d) Public Interest
    - (e) Establishment, exercise or defence of legal claims
    - (f) Vital interests of the DS
    - (g) Public Register
    - (h) Legitimate interests

Risk

- Identify the main risks introduced by the proposal and link them to the corporate risk register.
- Explain why this risk is relevant
- What is the proposed method of reducing or eliminating the risk?
- With the mitigation in place, what is the predicted impact and likelihood of the risk occurring and the final risk score?

Attachments

- Embed any relevant documents to ensure this assessment is a complete record of what will be approved.
- Briefly describe the purpose of each document
- Identify any sensitive data to withhold for publication on a published version of the document

Reviews

- Identify whether or not a review is required during the lifetime of the proposal
- Record the outcome of any reviews undertaken

Approvals

- Evidence the approvals obtained for the proposal
- Each assessment has a mandatory minimum of 3 stages of approval.
- Where processing meets the criteria of a DPIA, the DPO will need to approve

- Where risks cannot be managed within the organisation's risk tolerance, the proposal can be escalated to the SIRO if the SIRO is willing to accept the risk of the processing.