East Renfrewshire Council

Data Protection Impact Assessment Procedures

1. Introduction

1.1 These procedures establish the steps to be followed to identify the need for a Data Protection Impact Assessment (DPIA) in respect of any proposal that involves new processing of personal data and the mechanism to be used in concluding that assessment.

2. Scope

2.1 These procedures apply in respect of all projects undertaken by the Council which involve the handling of personal data.

3. Responsibilities under these procedures

3.1 **Project Lead –** the Project lead will carry out the screening process to identify whether a DPIA is necessary and will conduct any DPIA required**.**

3.2 **Data Protection Officer (DPO) –** the DPO will provide advice to the Project Lead on various issues associated with the DPIA

3.3 **Head of Service –** the relevant Head of Service will make the final decision to adopt the DPIA conclusion and sign it off

3.4 **Information Security and Digital Risk Officer –** will act as a consultee in the DPIA process

3.5 **Service Data Protection Officer (Service DPO) –** the Service DPO will retain all completed DPIAs for their service and a list of all screening decisions which conclude that there is no need for a DPIA.

4. Timing

4.1 There is no specific timeframe for completion of the DPIA. The assessment must however be concluded prior to the start of the proposed processing and should be commenced in sufficient time so as to permit a full and thorough assessment of the privacy implications of the proposal.

5. Screening

5.1 A DPIA is required where a type of processing is likely to result in a high risk to the rights and freedoms of individuals. The Project lead should undertake a screening assessment to establish the need for a full DPIA.

5.2 A DPIA must be done for the following types of processing :-

- Systematic and extensive profiling with significant effects:
- Large scale use of special category data or of personal data relating to criminal convictions and offences
- Public monitoring (a systematic monitoring of a publicly accessible area on a large scale eg CCTV)
- Processing involving the use of new technologies, or the novel application of existing technologies (including AI).
- Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
- Any profiling of individuals on a large scale.
- Any processing of biometric or genetic data.
- Data matching ie combining, comparing or matching personal data obtained from multiple sources.
- Processing of personal data that has not been obtained direct from the data subject in circumstances where advising them of the processing would prove impossible or involve disproportionate effort.
- Processing which involves tracking an individual's online or offline location or behaviour.
- The use of children's personal data (or that of other vulnerable individuals) for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to them.
- Where the processing is of such a nature that a personal data breach could result in a risk of physical harm.

5.3 A DPIA does not have to be carried out if:-

- a substantially similar DPA has already been carried out,
- the type of processing is on a list produced by the ICO which excuses it from the need for a DPIA; or
- the processing is part of a legal obligation or public task which itself has already been subject to a data protection risk assessment when the legislation became law**.**

5.4 If after screening the Project Officer decides not to complete a DPIA that decision should be documented and passed to the Service DPO for retention.

6 Conducting the assessment

6.1 Who

6.1.1 If the screening process identifies the need for a DPIA, it will generally be progressed by the Project Lead. He/she may however engage a consultant to undertake the task or, if the processing is expected to be undertaken by a data processor, request that they do it.

6.2 How

6.2.1 The Project Lead /consultant/processor shall complete the standard DPIA template (attached as Appendix 1). The assessment will include:-

- a description of the processing
- consideration of the need and outcome of consultation
- assessment of necessity and proportionality
- identification and assessment of risks
- identification of measures to mitigate the risks
- formal sign off of conclusions and recorded outcomes

7 Advice

7.1 The Project Lead should take advice from the DPO in connection with the DPIA process. This advice should be recorded on the template.

7.1.1 In particular, the DPO should provide advice on:

- whether a DPIA is needed;
- how the DPIA should be progressed (including the scope of consultation);
- whether to outsource the DPIA or do it in-house;
- what measures and safeguards could be used to mitigate risks;
- whether the DPIA has been done correctly; and
- the outcome of the DPIA and whether the processing can go ahead

7.1.2 The Project Lead is not obliged to follow the advice of the DPO but requires to record and justify any contrary decision.

7.2 The Project Lead must seek advice from the Information Security and Digital Risk Officer in relation to any proposed processing involving the use of new technology and may seek her views in relation to any other proposal.

7.3 The Project Lead must take advice from any processor involved in the handling of the data in order to establish their activities and identify any associated risks.

7.4 The Project Lead may take advice from Legal Services or any other expert as he/she thinks fit.

8 Sign Off

8.1 At the conclusion of the assessment the Project Lead shall pass their conclusions to the relevant Head of Service for a decision as to sign-off.

8.2 If there remains a degree of high risk in the processing which cannot be mitigated, the concluded DPIA must be sent to the Information Commissioner's Office (ICO) for their views prior to any processing commencing. The document should be e-mailed to the ICO by the Project Lead.

8.3 Any advice received from the ICO should be followed.

8.4 The outcome of the assessment should be integrated into the project plan

8.5 The concluded DPIA should be sent for retention to the relevant Service DPO who should note the date of the assessment and schedule a review in terms of paragraph 9.1.

9 Review of the DPIA

9.1 The DPIA will be subject to review on a 2 yearly basis or sooner if any significant changes are made to how or why the personal data is processed or the amount of data collected changes to a significant degree.

9.2 At the relevant time the Service DPO shall conduct the review. He/she may delegate this responsibility to officers involved in that particular processing activity.

9.3 The DPIA review will consider any new risks identified from the processing. In particular it should consider external changes to the wider context of the processing such as the availability of new technology, identification of new security issues or increased public concern over the type of processing involved.

Appendix 1

Data Protection Impact Assessment

(*Name of project*)

Complete this template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan

1. Need for a DPIA

Broadly outline the aims of the project and what type of processing it involves. Refer or link to other documents, such as a project proposal or CMT/Cabinet/Council report if relevant. Summarise why you identified the need for a DPIA. (Reflect the outcome of the screening process).

2. Description of processing

Describe the nature of the processing:

How will the data be collected, used, stored deleted?

Where does the data come from?

Will it be shared with anyone?

Are any parts of the processing high risk?

You might find it useful to refer to a flow diagram or other way of describing data flows.

3. Describe the scope of the processing:

Describe the scope of the processing: What is the nature of the data? Does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

4. Describe the context of the processing:

Describe the context of the processing:

What is the nature of your relationship with the individuals?

How much control will they have?

Would they expect you to use their data in this way?

Do they include children or other vulnerable groups?

Are there prior concerns over this type of processing or security flaws?

Is it novel in any way?

What is the current state of technology in this area?

Are there any current issues of public concern that should be factored in?

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

5. Describe the purpose of the processing:

Describe the purposes of the processing:

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the processing – for the Council and more broadly?

6. Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Who else do you need to involve within your organisation?

Do you need to ask your processors to assist?

Do you plan to consult information security experts, or any other experts?

7. Necessity and proportionality

Describe compliance and proportionality measures, in particular:

What is your lawful basis for processing?

Does the processing actually achieve your purpose?

Is there another way to achieve the same outcome?

How will you prevent function creep?

How will you ensure data quality and data minimisation?

What information will you give individuals?

How will you help to support their rights?

What measures do you take to ensure processors comply?

How do you safeguard any international transfers? (if relevant)

8. Risk assessment

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

9. Risk Reduction measures

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

10. Outcome

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA