East Dunbartonshire Council

Data Protection Assessment Policy 2018

Content

1. Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.

A DPIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

An effective DPIA will allow East Dunbartonshire Council ("the Council") to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

DPIAs are often applied to new projects, because this allows greater scope for influencing how the project will be implemented. A DPIA can also be useful when the Council is planning changes to an existing system. A DPIA can be used to review an existing system, but the Council needs to ensure that there is a realistic opportunity for the DPIA conclusions to implement necessary changes to the system.

2. Data Protection Impact Assessment Policy

This Policy takes the recommendations set out in the Information Commissioner's Privacy Impact Code of Practice and applies them to the Council.

This procedure applies to all employees, and all processes that include a new or changed use of Personal Confidential Data and/or Business sensitive data in any format.

This includes

- introduction of a new paper or electronic information system to collect and hold personal/business sensitive data
- introduction of new service or a change to existing process, which may impact on an existing information system
- update or revision of a key system that might alter the way in which the Council uses, monitors, and reports personal/business sensitive information
- replacement of an existing data system with new software
- changes to an existing system where additional personal/business sensitive data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal/ business sensitive data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements

3. Benefits of a Data Protection Impact Assessment

The Information Commissioners Office promotes DPIAs as a tool which will help organisations to comply with their GDPR obligations, as well as bringing further benefits. Carrying out an effective DPIA will benefit the individual Data Subjects affected by a project and the Council. It is likely to be the most effective way to demonstrate how personal data processing complies with GDPR.

The first benefit to individual Data Subjects will be that they can be reassured that the Council has followed best practice. A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individual Data Subjects is that a DPIA will improve transparency and make it easier for them to understand how and why their information is being used.

The process of conducting the assessment will improve how the Council uses information which impacts on individual privacy. This should in turn reduce the likelihood of the Council failing to meet its legal obligations under GDPR and of a breach of the legislation occurring.

4. The Data Protection Impact Assessment Process

The DPIA process is a flexible one that can be integrated with the Council's existing approach to managing projects. The time and resources dedicated to a DPIA should be scaled to fit the nature of the project.

A DPIA should begin early in the life of a project, and should develop as the project develops. The assessment will incorporate the following steps:-

- Identify the need for a DPIA
    - Answer screening questions to identify a proposal's potential impact on privacy.
    - Begin to think about how project management activity can address privacy issues.
    - Start discussing privacy issues with stakeholders

- Describe the information flows
    - Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
    - This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)

- Identify the privacy and related risks
    - Record the risks to individuals, including possible intrusions on privacy where appropriate.
    - Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust.
    - Conduct a compliance check against GDPR and other relevant legislation.
    - Maintain a record of the identified risks.

- Identify and evaluate the privacy solutions
    - Devise ways to reduce or eliminate privacy risks.
    - Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.

- Refer back to the privacy risk register until satisfied with the overall Data Protection Impact Assessment.

- Sign off and record the DPIA outcomes
  - Obtain appropriate signoff within the Council.
  - Produce a DPIA report, drawing on material produced earlier during the PIA.
  - Consider publishing the report or other relevant information about the process.

- Integrate the outcomes into the project plan
  - Ensure that the steps recommended by the DPIA are implemented.
  - Continue to use the DPIA throughout the project lifecycle when appropriate.

- Consult with internal and external stakeholders as needed throughout the process

5. Conducting a Data Protection Impact Assessment

The Council has put in place a process to manage and review Data Protection Assessments across the Authority.

When considering if a project may require a DPIA the service area will complete and submit to the Council's Information Management Team a completed 'Data Protection Assessment Screening Form (Appendix 1 to this document).

Where the Information Management Team confirms that a DPIA is required, the Service will work with the Information Management Team to complete a DPIA Form (Appendix 2 to this document).

A further form will be completed linking the proposal to the requirements of the principles of GDPR (Appendix 3).

6. Policy Review

The Policy will be reviewed annually to reflect operational improvements and changes to best practice.

Document Control Table	
Prepared by	Stephen Armstrong – Freedom of Information/ Data Protection Officer
Peer Reviewed By	Karen Watt- Information and Records Manager
Authorised by Senior Responsible Person	Signature:- Date:- Print Name _____
Source Location	
Published Location	
Other Documents Referenced	
Related Documents	Information and Records Management Strategy and Information Management Strategic Implementation Programme(IMSIP) EDC Classification Scheme and Retention Schedules Appraisal and Disposition Policy and Procedures Vital Records Policy Confidential Waste Policy Data Protection Policy Data Protection Breach Reporting Policy and Guidance Freedom of Information Policy and Guidance Toolkit Information Security Policy IM – File Housekeeping – Employees Guidance Note (1) 03.08.12 IM – Top Ten Tips for Better Records Management – Employee Guidance Note (2) 03.08. Saving an Email Guidance Naming Electronic Records

Acknowledgements	

Version Control Table			
Version number	**Date issued**	**Author**	**Update information**
V1	August 2017	Freedom of Information/ Data Protection Officer	Privacy Impact Assessment Policy v1 Draft
V1.2	May 2018	Freedom of Information/ Data Protection Officer	Privacy Impact Assessment Policy v1.2

Appendix 1
Data Protection Assessment Screening Form

The following questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops.

Will the project involve the collection of new information about individuals?

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 purpose it is not currently used for, or in a way it is not currently used?

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.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Appendix 2
Data Protection Assessment

Step one: Identify the need for a DPIA
Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions

Step two: Describe the information flows
The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements
Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step three: identify the privacy and related risks	
Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register. Annex three can be used to help identify GDPR related compliance risks	
Privacy issue	

Risk to individuals	
Compliance risk	
Associated organisation / corporate risk	

Step four: Identify privacy solutions	
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).	
Risk	
Solutions	
Result: is the risk eliminated, reduced, or accepted?	
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?	

Step five: Sign off and record the DPIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Step six: Integrate the DPIA outcomes back into the project plan	
Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?	
Action to be taken	
Date for completion of actions	
Responsibility for action	

Contact point for future privacy concerns	

Appendix 3
Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help identify where there is a risk that the project will fail to comply with GDPR or other relevant legislation, for example the Human Rights Act.

1st Principle: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). In particular, shall not be processed unless: a) at least one of the conditions in GDPR Article 6 is met, and b) in the case of special category personal data, at least one of the conditions in GDPR Article 9 is also met.

- Have you identified the purpose of the project?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:
- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

2nd Principle: 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

- Does your project plan cover all of the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

3rd Principle: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- Is the information you are using of good enough quality for the purposes it is used for?
- Which personal data could you not use, without compromising the needs of the project?

4th Principle: 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 ('accuracy');

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5th Principle: 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software which will allow you to delete information in line with your retention periods?

6th Principle: 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 ('integrity and confidentiality').

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?