Procedure for Undertaking a Data Protection Impact Assessment

Contents

Version	Amended by	Date	Summary
1.0		May 2018	
2.0	HIAG	January 2023	

1. Introduction

1.1 Under previous legislation, the carrying out of a Privacy Impact Assessment was considered to be good practice. Both the UK General Data Protection Regulation ("UK GDPR"] and the Data Protection Act 2018 ["DPA"] requires that carrying out a Data Protection Impact Assessment (DPIA) is mandatory in certain circumstances. This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

1.2 A DPIA is a process to help identify and minimise the data protection risks of a particular project when the processing of personal data is likely to result in a high risk to individuals interests. A high risk might arise if the Council is intending to process data that:

1.2.1 involves the use of sensitive or highly personal data;
1.2.2 concerns vulnerable adults or children;
1.2.3 involves preventing people from using a service or exercising a right;
1.2.4 includes processing data on a large scale.

1.3 If you are in any doubt as to whether you need to complete a DPIA, you should consult with the Council's Statutory Data Protection Officer (DPO) who is Glen Egan, Acting Head of Legal Services and Monitoring Officer. His contact details are:
Email: GEgan2@Hillingdon.Gov.UK Telephone number: 01895 277602

1.4 If a high risk is identified and you cannot mitigate that risk, you must consult with the Council's DPO, who will determine whether to liaise with the Information Commissioner's Office (ICO) before starting the processing. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases. In appropriate cases, the ICO has the power to issue a formal warning not to process the data, or to ban the processing altogether.

2. When should a DPIA be undertaken?

2.1 A DPIA is a process to systematically analyse the Council's processing and help it to minimise data protection risks. It is not intended to be a one-of exercise and should be seen as an ongoing process. It should be monitored and reviewed as necessary. A DPIA must:

2.1.1 describe the processing and its purposes;
2.1.2 assess necessity and proportionality;
2.1.3 identify and assess risks to individuals; and
2.1.4 identify any measures to mitigate those risks and protect the data.

2.2 The UK GDPR states that the Council must carry out a DPIA if it plans to:

2.2.1 systematically monitor a public place on a large scale by for example, installing CCTV cameras;
2.2.2 process special category personal data or criminal offence data on a large scale;
2.2.3 use systematic and extensive profiling with significant effects;

2.2.4 2.2.4. use new technologies, process biometric data (eg fingerprints, facial recognition, retinal scans) and geometric data (an individual's gene sequence);
2.2.5 profile children or target services at them;
2.2.6 match data or combine data sets from different sources;
2.2.7 process personal data without providing a privacy notice directly to an individual;
2.2.8 process personal data that might endanger an individual's health or safety in the event of a security breach.

2.3 The UK GDPR also provides that the Council must, where appropriate, seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

The following checklist will assist you in terms of determining whether a DPIA must be carried out.

		DPIA questions	**Yes/No**
1.	Identity	Will the project involve collecting information about individuals for the first time?	
2.	Identity	Will your project compel individuals to provide information about themselves?	
3.	Sharing Information	Will any information about individuals be disclosed to any other organisations?	
4.	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5.	Data	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 or CCTV cameras.	
6.	Data	Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	
7.	Data	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.	
8.	Data	Will the project require you to contact individuals in ways that they may find intrusive?	

If you have answered YES to ANY of the questions in the checklist, you will need to consult with the DPO.

3. What should a DPIA contain?

3.1 Section 64 of the DPA 2018 prescribes that a DPIA must contain as a minimum:

3.1.1 A systematic description of the proposed processing and its purpose;
3.1.2 An assessment of the risks to the rights and freedoms of data subjects;
3.1.3 The measures proposed to address those risks;
3.1.4 Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Council's Data Protection Policies and Procedures.

4. The following Data Protection Impact Assessment Template should be used when carrying out a DPIA.

1. Describe the project - new service or change to service	**Title of project:**	
	What is the project?	
	What is the purpose of the project?	
	Head of Service (insert name):	
2. Risk Assessment	**Is there a high risk to personal data?** **Please give details, refer to checklist**	
2. What personal a sensitive personal data will be collected?	**What Personal Data will be collected (list all fields)**	
	What special category personal data will be collected *(list all)*	
3. Data Protection principles	**What is the legal basis for processing the data?**	
	Is the data you will collect the minimum necessary to achieve the purpose of the project? *(please explain)*	
4. Data Protection principles	**How will the accuracy of the data be checked?**	
	How long will you retain the data collected for? **(The retention period may be defined by law, if not you should only retain data as long as is necessary)**	
	What measures are in place to ensure the data is held securely?	

5. Contracts	**[issues that might arise if service is under contract]**
	
	• **Tender process**
	• **Contractual controls**
	• **Contract Term**
	• **Supplier(s) & Accreditation**
	• **Training**
	• **Organisational Policies**
	• **Technical Controls**
	  o **Access**
	  o **Security at rest**
	  o **Security in transit**	

6. Risk management	**What controls are in place to manage or mitigate any risks and have you considered whether there is a need to consult with data subjects?** **Note: If the risks to personal data cannot be mitigated, the Data Protection Officer will need to consult the Information Commissioner's Office before your project can proceed.**	
7. Attachments	**Please attach the following as appropriate:** • **Privacy Notice** • **Consent Form** • **Business Case** • **PID/Specification** • **High and low level design documents, network diagrams** • **Procurement evaluations, contracts agreements**	
8. Reviews		
9. Approvals	**Head of Service Signature:** **Date:** **DPO Signature:** **Date:**	