Council Address: The Town Hall, Heath Road, Petersfield, GU31 4EA
Email Address: clerk@petersfield-tc.gov.uk
Telephone numbers: 01730 264182

Privacy Impact Assessment (PIA)

Introduction

Privacy impact assessments were launched in the UK by the Information Commissioner in December 2007, and mandated by the cabinet office for Information Communications Technology (ICT) projects following the Data Handling review in June 2008.

Purpose;

The purpose of this document is to set out the process for completing Privacy Impact Assessments to identify any impact on privacy where a new service or system is introduced.

Scope:

This procedure is to be followed in the following circumstances:

- Introduction of a new information system to collect and hold personal data (consultation is seen as one of these purposes)
- Update or revision of a system that might alter the way in which the Council uses, monitors and reports personal information.
- Changes to an existing system where additional personal data will be collected, a proposal to collect personal data from a new source or for a new activity.
- Plans to outsource business processes involving storing and processing personal data.
- Plans to transfer services form one provider to another that include the transfer of information assets
- Any change to or introduction of new data sharing agreements
- Data sharing initiative where two or more organisations seek to pool or link sets of personal data
- Any change to access of an information asset that involves an external organisation
- Changes in legislation, policy or strategies which will impact on privacy through the collection of or use of information, or through surveillance or other monitoring.

Responsibility

Any person who is responsible for introducing a new or revised service or changes to an existing service, process or information asset is responsible for ensuring the completion of a PIA and therefore must be effectively informed of these procedures.

PIA Process

A PIA should incorporate the following steps (ICO, 2016):

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related tasks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

Privacy Impact Assessment Form

Step 1: The Initial Screen Questions to identify the need for a PIA

This section is to be completed by the Controller responsible for delivering the proposed change/system. The purpose of this section is to assess whether a more complete assessment is required.

If response to any if the questions in the screening question is "Yes" then an initial Privacy Impact Statement must be completed.

Please ensure that answers to all questions in each stage of this form are evidenced by providing detailed remarks, and are not simply Yes/No.

SN	Screening Questions	Yes/No	Explanation
1.1	Will the project involve the collection of new information about individuals?		
1.2	Will the project compel individuals to provide information about themselves?		
1.3	Will information about individuals be disclosed to or shared with organisations or people who have not previously had routine access to the information?		
1.4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?		
1.5	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?		
1.6	Does the project include new software, apps or any other new form of information asset hat use personnel identifiable information in any way?		
1.7	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?		
1.8	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 are likely to consider as private? [NB: if health information is in any way involved, the answer to this question is always "Yes".]		
1.9	Will the project require you to contact individuals in ways which they may find intrusive?		

Answering "Yes" to any of the questions represent a potential Information Governance risk that needs to be further analysed to ensure those risks are identified, assessed and mitigated. If any of the answers for the questions above is "Yes" complete Stage 2

Stage 2: Initial Privacy Impact Assessment

SN	Questions		Explanation
2.1	Is this new or changed use of personal information that is already collected?	New /Changed	
2.2	**What Data will be collected?** Name Date of birth Age Gender Passport Number Address Telephone number Email Address Location data Online identifier Any other unique identifier Other type of data type (please state) Special Category Data: Racial or ethnic origin Sexual life Political opinion Religious belief Trade Union Membership Physical Health or mental health or condition Biometric Data or Genetic Data **Criminal Record:** Commission or alleged commission of an offence Proceedings for any offence committed or alleged **Details and description of other data collected:**		
2.3	Can the same outcome be achieved without processing any of the above dataset?		Yes/No
2.4	Is the processing fair, lawful and transparent?		Yes/No
2.5	What is the lawful processing basis for this dataset being processed?		

2.6	If interest is being used has the means test been completed?	Yes/No/NA
2.7	If consent is the Lawful processing basis, is the consent and context it was provided recorded?	Yes/No/NA
2.8	Is the information being used for a different purpose than it was originally collected for?	Yes/No
	If yes, please list the new purpose (s)	
2.9	If being used for a new purpose, is the new purpose compatible with the original purpose?	Yes/No/NA
2.10	Are other organisations involved in processing (including receipt) of the collected data?	Yes/No *If yes, list below:*

Name of Organisation	Contact Person	Assurance (i.e.) ISO Certificate, Cyber Essential

2.11	Has the data flow mapping exercise been undertaken?	Yes/No
	Can you please provide a copy of the document or complete section 3.0	
2.12	Does the work involve employing external third party contractors accessing system/data?	Yes/No
	If yes, please provide a copy of the agreement/contract.	
2.13	Will the information be collected electronically, on paper or both?	
2.14	Where will the information be stored?	
2.15	Who will have access to the system/data?	
2.16	Is there an ability to audit access to the information?	Yes/No
	If yes, who will have access to audit logs?	

2.18	Does the system involve new links with personnel data held in other systems or have existing links been significantly changed?	Yes/No
	If yes, please list the systems	
2.19	How will the information be kept up to date and checked for accuracy and completeness (data quality)?	
2.20	What security and audit measures have been implemented to secure access to and limit use of personal identifiable information? User name and password Encryption Smart card Secure token Restricted access to file servers Locked Physically secure location Any other……..	

2.21	Will any information be sent (transferred) offsite i.e. outside of the organisation and its computer network?	Yes/No
	If yes, within the organisation is a standalone system Outside of the organisation Outside the Uk Outside the European Economic Area	
2.22	If being sent outside the European Economic Area, what safeguards will be in place to ensure the fair and lawfulness of data. i.e. Binding Contract Rules, Standing Contract Clause EU-US Privacy Shield	
2.23	Please state the method the data will be transferred Non secure email Secure email Website Access External portable Devices File transfer Service (FTP) Post Fax Other……	

2.24	Is a system level security policy in place for the proposed system? If yes, please provide a copy	Yes/No/NA
	If no, when will the policy be in place?	
2.25	Is staff training for the new system in place? Data Collection System usage Collecting Consent Secure processing	 Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA
2.26	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/NA
2.27	How will individuals be informed of the proposed uses of their personal data? E.g. Privacy notice. If yes, please provide a copy of the information	
2.28	Are arrangements in place for the following: 1) Access to data (SAR) 2) Right to rectification 3) Right to be forgotten 4) Right to data Portability 5) Right to Notification 6) Right to Object	 Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA
2.29	Have you had the data retention policy defined for the collected dataset?	Yes/No/NA
2.30	How would you ensure the secure disposal of data at the end of the retention period?	

3.0 Data Flow details and Mapping

SN	Questions	Details
3.1	How has the data been gathered?(source of Data)	
3.2	Who has access to data and what is the process for gaining access?	
3.3	Is there an audit trail showing the access and type of access?	
3.4	How is data stored and who is responsible for data?	
3.5	Who will the data be shared with? Justification for sharing	
3.6	How the data will be shared/moved?	

Please provide a data flow map, which is a flow chart/graphical representation of data flow.

This should include:
Incoming and outgoing data
Organisations and/or people sending/receiving data
Storage of data and method of transfer

Please provide comments relating to your project that demonstrate how it is compliant with the Data Protection Act or which legislation provides the basis for this activity or why Data Protection Act requirements may be set aside. We have provided references to previous questions whose answers would likely contain the information you need.

Please provide comments relating to your project that demonstrate how it is compliant with the Data Protection Act or which legislation provides the basis for this activity or why Data Protection Act requirements may be set aside. We have provided references to previous questions whose answers would likely contain the information you need.

Principals	Ref Sec	Comment
Principal 1 (processed lawfully, fairly and transparent manner in relation to data subject)	2.1 2.5 2.6 2.7	
Principal 2 (personal data shall be collected for specified, explicit and legitimate purpose)	2.8 2.9 2.18	
Principal 3 (personal data shall be adequate, relevant and not excessive in relation to the purpose	2.2 2.3	

or purposes for which they are processed)		
Principal 4 (personal data shall be accurate and, where necessary, kept up to date.)	2.19	
Principal 5 (personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.)	2.24 2.30 2.31	
Principal 6 (Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	2.10 2.11 2.12 2.13 2.14 2.15 2.16 2.17 2.20 2.23 2.24 2.25	
Individual Rights Obligation	2.11 2.27 2.28	
Transfer to Third Countries Obligation	2.21 2.22 2.23	