PRIVACY IMPACT ASSESSMENTS ("PIA"): GUIDANCE

Introduction

A PIA is merely a process that helps the Council to identify and minimise the privacy risks of new projects or policies or when planning changes to an existing system or process. It is designed to help the Council assess whether what it proposes to do is necessary and proportionate. It isn't always possible to remove risk completely, but a good PIA will enable the Council to reduce privacy risks to an acceptable level while allowing the Council to meet its objectives.

Carrying out a PIA will assist the Council to meet its legal obligations – for example, under the General Data Protection Regulations 2016 ("GDPR"), the Data Protection Act 2018 and the Human Rights Act 2000. A PIA will help the Council both to comply with its GDPR obligations and also to demonstrate that compliance.

A template has been produced to guide you through the PIA process and you should have regard to this guidance when completing it. A copy of the template is attached to this guidance and an electronic version is available in the data protection section of the Council's Hyntranet.

When should I carry out a PIA ?

In certain circumstances, the Council is required by law to undertake a PIA before it starts to collect or use personal information. In other circumstances it may be good practice to carry out a PIA even if this isn't a legal requirement.

A PIA **must** be carried out in the following circumstances:

- any processing (in particular using new technologies) likely to result in a high risk to the rights and freedoms of individuals, taking into account the nature, scope, context and purposes of the processing; or
- a systematic monitoring of a publicly accessible area on a large scale (such as CCTV); or
- processing on a large scale of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or a person's sex life or sexual orientation, genetic or biometric data or criminal convictions ; or
- systematic and extensive evaluation of information about individuals (including profiling) by automated processing and leading to decisions which have legal effects on individuals

Article 35 GDPR

A PIA **would be good prac**tice in the following circumstances:

- the introduction of new technology that could be intrusive; or
- when sharing personal information with third parties, such as contractors or other local authorities; or
- when proposing to collect personal information of a type which is likely to cause privacy concerns, such as medical records or criminal convictions; or
- when you wish to contact people in a way they may find intrusive, such as "cold calling" or unsolicited texts
- when you want to use personal information you already have in a new and potentially more intrusive way

When deciding whether you should undertake a PIA either as a legal requirement or as a matter of good practice, it may help to consider the following:

- ✓ will you be using or holding sensitive or highly personal information about people ?
- ✓ will you be using or holding information about vulnerable people ?
- ✓ will you be using or processing personal information on a large scale ?
- ✓ will you be involved in systematic monitoring or assessment of personal information ?
- ✓ will you be using innovative technology ?

 you probably need a PIA (and you should seek legal advice or consult the Data Protection Officer if you are unsure).

Undertaking a PIA : tips on completing the PIA template

Section of the PIA	Comments
purpose	You should describe what you plan to do and explain why. You should explain what end result you wish to achieve. What legal power or duty are you replying on to carry out your proposal ?
processing	You need to understand exactly what personal information you will be collecting and using in order to identify the privacy risks. You must: • identify each type of personal information you will be collecting or using – e.g. names, health data, conviction details, CCTV images etc • indicate the scope or volume of personal information you will be collecting or using – e.g will you collect data on a few people or hundreds of people ? You also need to understand exactly what you will be doing with the personal information in order to identify the privacy risks. You must:

	• give a detailed description of what you plan to do with the data at each stage – including collection, storage, use, data sharing, retention period and disposal; • (if you will be sharing the information with others) explain who will receive it, why the sharing is taking place and how it will take place; • Explain the form the information will take – e.g. will it be in a paper format or will it be held electronically (and if the latter, you should say what hardware, software and networks will you be using) • Explain how you will comply with any applicable codes of conduct – e.g the Home Office's "Surveillance Camera Code of Practice"
justification	You must explain why what you propose is necessary and proportionate. You should consider: • whether you have to use personal information at all to achieve your objective • have you limited your use of personal information to what is necessary and relevant to achieve your objectives • whether the risks to privacy are reasonable and proportionate to what you aim to achieve or whether your proposal is it too intrusive You should include details of the measures you have taken to ensure that your proposal is proportionate and necessary. For example: • have you consulted • what information will be given to the individuals concerned about use of their data • how will you give effect to individual's rights of access to their data or their rights to rectify or erase it • have ensured you will not keep the information for longer than is necessary
consultation	The type and amount of consultation required depends on the scale of the project and the level of risk involved, and this need not be an onerous requirement. If you decide not to consult then you must give good reasons for your decision. For example, if you conclude that it is disproportionate or impractical to consult then you must explain why. Consultation can be internal, as well as external – e.g. you may need advice from Legal to ensure you meet statutory

	requirements, and with IT (or your IT supplier) to consider measures to mitigate risk. In addition, you **must** consult the Council's Data Protection Officer when carrying out a PIA. The DPO is the Executive Director (Legal & Democratic Services).
risks	These should be considered and identified at an early stage in your project planning to give you time to consult and explore your options to minimise privacy risks. You should consider the origin of each risk, its nature, likelihood and likely severity. You don't need to eliminate risks entirely, you just have to reduce them to an acceptable level. Risks can be: - to individuals rights and freedoms (e.g. undue intrusion, inappropriate data sharing, data loss or unwanted data modification); and - to the Council (damage to reputation, loss of customer trust); and - compliance risks (enforcement action, and fines and compensation payable for a breach of the law)
Mitigation of risk	There are many things you could consider to minimise privacy risks. For example, consider: - arrangements and procedures for secure storage, use and destruction of the personal information - possible technological security measures - staff training on privacy risks and information sharing - scope for password protection,anonymization or encryption of personal data - data sharing agreements with agents, contractors and partner bodies - building privacy measures and criteria into specifications and the contractor selection process - using appropriate privacy clauses in contracts - ensuring information is not retained longer than necessary - ensuring individuals are aware of how their personal data will be used - considering if access to the personal data can be restricted - consider what back-up arrangements you will need in the event of the information being lost, damaged, stolen or compromised

PRIVACY IMPACT ASSESSMENT ("PIA")

Please refer to the Council's PIA Guidance before completing this form. The Guidance can be found in the Data Protection section of the Hyntranet and Council website.

Purpose

What personal information do you intend to collect or use and why ? e.g what is the aim of the project or the reason for the data processing ? e.g what sort of personal information will it be (such as names, addresses, CCTV footage, criminal convictions, information about age, religion or ethnicity) ?

Processing

What do you propose to do with the personal information ? e.g how will you collect the information, where will you keep it, how will you use it, who might you share it with, how and when will you delete it ?

Justification

Why is what you propose a necessary and proportionate thing to do ? e.g is the impact on privacy proportionate to the aims of the project ?

Consultation

Have you consulted the people who may be affected by what you propose ? Please give details of the consultation – who did you consult, how did you consult them, what did they say and has this led you to change your proposal in any way ? If you do not intend to consult, please explain why.

Privacy Risks

What are the privacy risks ?

How will you reduce the risks ?		
privacy risk	**mitigation measure(s)** **(*use a continuation sheet if you need to)***	**risk reduced or eliminated ?**

You are required to consult the DPO

Comments of Data Protection Officer	
Signed:	Date:

Privacy Impact Assessment re ……

Continuation sheet:

How will you reduce the risks ?		
risk	**mitigation measure(s)** **(*use a continuation sheet if you need to)***	**risk reduced or eliminated ?**