Conducting a Data Protection Impact Assessment (DPIA)

Introduction

The term PIA (Privacy Impact Assessment) has been used for some time to describe an assessment of data protection and other privacy risks associated with the design, development and implementation of a new system, process or other project. The concept of the DPIA is introduced within the General Data Protection Regulation (GDPR) – essentially this is the same concept as a PIA, but it is primarily focussed on the data protection element of privacy risks.

Purpose

DPIAs are an important part of the 'privacy by design' culture which is central to the GDPR and seeks to ensure that privacy issues are considered at the outset of a project rather than being an afterthought (or ignored altogether), when it may be too late to address all the concerns, at least without significant cost implications

Understanding of the data protection risks associated with a project will help to improve its design and enhance communication about data privacy risks with relevant stakeholders. Some of the benefits of conducting a DPIA are:

- ✓ Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks
- ✓ Early understanding of the major risks should reduce the likelihood of the project failing
- ✓ Reducing operation costs by optimising flows within a project and eliminating unnecessary data collection and processing.
- ✓ Improving service and operation processes
- ✓ Improving decision-making regarding data protection
- ✓ Raising privacy awareness within the organisation
- ✓ Improving the feasibility of a project
- ✓ Strengthening confidence of users, members of the public and, employees in the way which personal data are processed and privacy is respected

When to undertake a DPIA

It should be started early on in the project, ideally integrated into the wider project plan and within broader risk assessment and risk management plans. Results can then be built into project design and implementation. A DPIA will evolve along with the project and is an ongoing process during the project lifecycle.

If a project is already underway, a DPIA can still be undertaken, on the basis that it is better to carry out some assessment than ignore data protection risks altogether!

The GDPR gives some examples of where PIAs will be required (e.g. processing on a large scale of special categories of data, in the event of a systematic monitoring of a publicly accessible area or in the context of profiling on which decisions are based that produce legal effects), but the PIA process may be used to help determine whether or not this is the case. DPIAs are an effective way of demonstrating accountability. It is likely that organisations will choose to use them more widely than expressly required under the GDPR.

Examples given by the ICO of when it might be advisable to undertake a DPIA

- embark on a new project involving the use of personal data;
- introduce new IT systems for storing and accessing personal information;
- participate in a new data-sharing initiative with other organisations;
- initiates actions based on a policy of identifying particular demographics;
- use existing data for a “new and unexpected or more intrusive purpose”.

If the processing is likely to result in a greater risk to data subjects and these cannot be mitigated, or the volumes of processing are high, there might be a requirement to consult with the ICO before going ahead.

The DPIA Process

Appendix A contains a template for undertaking some initial screening questions to help in determining whether a DPIA is required.

Appendix B contains a DPIA flow chart

Please discuss any requirements with the DPO, Michele Sarginson, email: michele.sarginson@peakdistrict.gov.uk, 01629 816278.

Appendix A:
The aim of the initial assessment is to gain a high level understanding of the proposed project and the potential privacy risks in order to decide whether a formal DPIA is required.

The following questionnaire should help with this process. The final column can be used to note any initial comments on the relevant issues and impacts, for example, areas of the project in which the issue arises, the individuals who may be affected; the predicted level of risk and whether further details or analysis is needed.

Issue	Questions	*Examples*	Yes/No	Initial Comments on issue and privacy impacts
Purpose for data and how collected	Does the project: • Involve a new purpose for which the data are to be used • Involve processing personal data in a new way	*Profiling, data analytics, marketing*		*Note: GDPR requires a DPIA to be carried out where there is **systematic** and **extensive** evaluation of personal data relating to individuals based on **automated processing** including profiling, and on which **decisions** about individuals are based*
Individuals	Will the project: • Affect an increased number or	*Expanding existing customer base*		

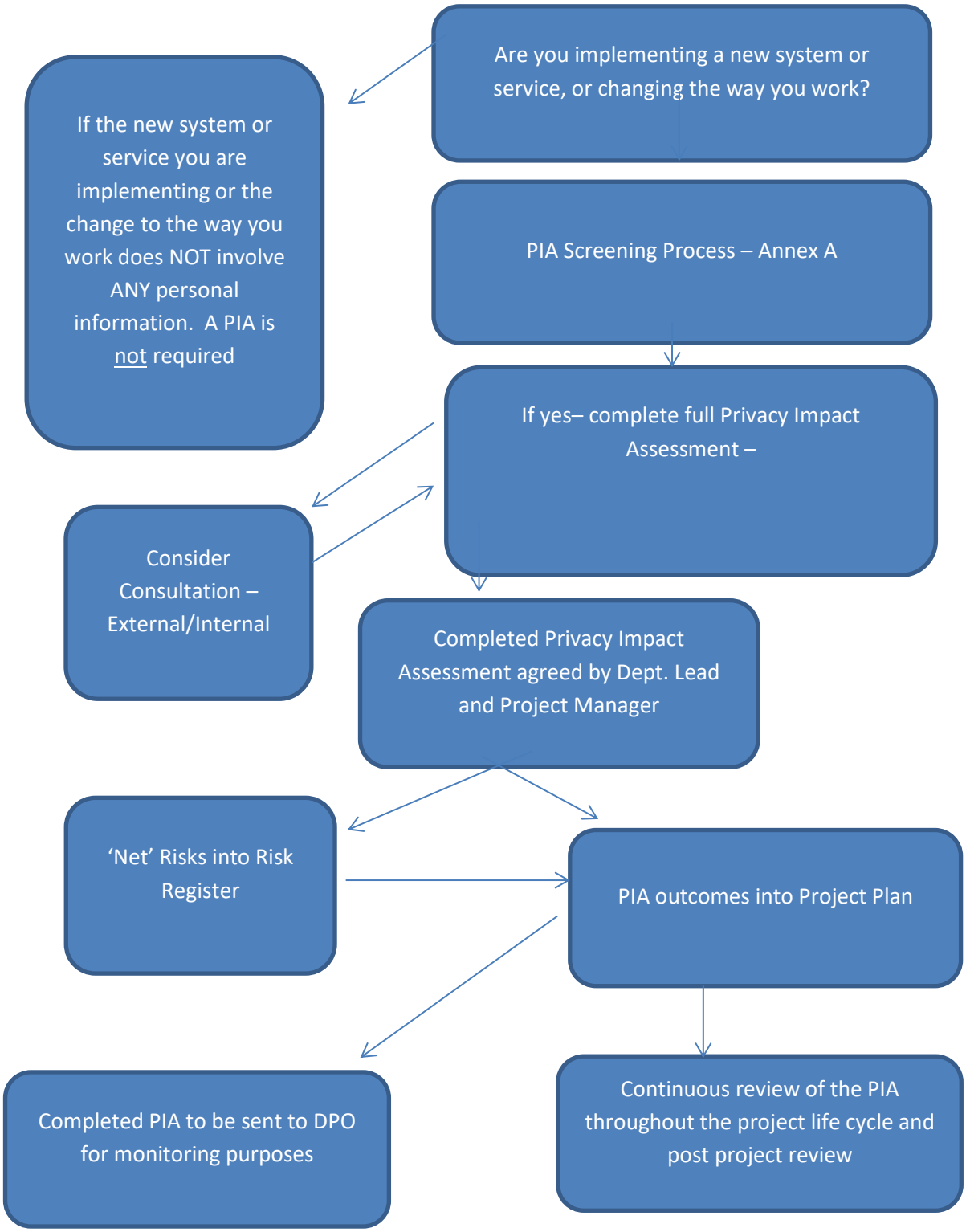
Issue	Questions	*Examples*	Yes/No	Initial Comments on issue and privacy impacts
	a new group or demographic of individuals • Involve a change in the way in which they are contacted, or are given access to services or data • Affect particularly vulnerable individuals • Present risks that individuals may not know or understand about how their data is used	*Technology that may be used by individuals* *Hidden or complex uses of data* *Children's data*		
Issue	Questions	Examples	Yes/No	Initial Comments on issue and privacy impacts
Parties	Does the project involve: • The disclosure of personal data to new parties • Working with and sharing data with third/multiple parties	*Outsourced service providers* *Funding partners* *Joint ventures*		
Data categories	Does the project involve: • The collection, creation or use of new types of data • Use of sensitive or data that could be considered an intrusion into privacy	*Sensitive personal data* *Biometric or genetic data* *Criminal offences*		*Note: GDPR requires a DPIA to be carried out where there is processing on a **large scale** of **sensitive data** or data relating to **criminal convictions and***

Issue	Questions	*Examples*	Yes/No	Initial Comments on issue and privacy impacts
	• New identifiers, or consolidation or matching of data from multiple sources	*Financial data* *Health or social data* *Data analytics*		***offences***
Technology	Does the project involve • new technology that could be privacy-intrusive	*Locator or surveillance technologies/CCTV/Body cameras* *Facial recognition*		*Note: GDPR requires a DPIA to be carried out where **new technology** is involved and especially where a **high risk** is likely.*
Data quality, scale and storage	Does the project involve: • changes to data quality, format, security or retention • processing data on an unusually large scale	*New technology*		
Monitoring, personal intrusion	Does the project involve: • monitoring or tracking of individuals or activities in which individuals are involved • any intrusion of the person •	*Surveillance, GPS tracking* *Bodily testing, searching*		

Issue	Questions	*Examples*	Yes/No	Initial Comments on issue and privacy impacts
Issue	Questions	*Examples*	Yes/No	Initial comments on issues and privacy impacts
Management of privacy	Does the project involve: • Review of existing internal policies and governance to ensure that they are adequate for the needs of the project	*Existing policies and procedures, roles and expertise*		
Compliance	Does the project involve: • Consideration of data protection and privacy laws – statutes, industry regulation • Are there other laws which may apply and have an impact on privacy	*GDPR, PECR, PCI, FOI, Human Rights Act*		
Data Transfers	Does the project involve: • Transfer of data to or activities within a country which has inadequate or significantly different data protection and privacy laws	*Countries outside of EEA*		*Note: Consider the **Privacy Shield** if transfer to **US*** *Use of **Binding Corporate Rules or Model Clauses**.*

Appendix B

DPIA PROCESS CHART




PEAK
DISTRICT
NATIONAL
PARK