STANDARD OPERATING PROCEDURES:
OFFICE OF THE BEDFORDSHIRE POLICE AND CRIME COMMISSIONER

Title	Data Protection Impact Assessment Policy and Guidance
Area of Compliance	Compliance
Version No.	1.0
Senior Lead	Chief Executive
Author	Compliance
Authorised by PCC	24/05/2018

Revision History

Date	Revision	Change	Section	Review Date
23.05.2018	1.0			23.05.2019
20.09.2019	2.0	DPIA		20.09.2020

Introduction

This policy and procedure ensures compliance with the requirement under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) to conduct data protection impact assessments.

This policy ensures there are clear, consistent processes and structures to provide all staff with guidance on the process of identifying and reducing data protection risks when embarking on new projects and initiatives, adopting new police systems, information sharing or in other areas where personal data will be processed.

Applicability

This policy and guidance applies to all staff within the Bedfordshire Office of the Police and Crime Commissioner OPCC).

Compliance with this policy and procedure is mandatory.

What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

Privacy risk is the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or not kept securely.

Understanding privacy risk in this context does though require an understanding of the relationship between an individual and an organisation. Factors that can have a bearing on this include:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people.

Procedure Detail

The DPIA (previously known as a privacy impact assessment or PIA) is an assessment to identify and mitigate data protection risks. A DPIA is effective in ensuring compliance with data protection legislation including meeting individuals' expectations of privacy. The DPIA process identifies how the OPCC intend to collect, use and store personal data, ensuring the processing is lawful, fair and proportionate and that any risks to individual's personal data have been considered and mitigated.

A DPIA is a mandatory requirement under the Data Protection Act where the processing of personal data may present a high risk to the rights and freedoms of individuals. The risks must be identified and mitigated before the processing of the personal data starts. If any residual risks are high, consultation with the ICO is mandatory prior to processing.

The GDPR requires the OPCC to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. The accountability principle requires data

controllers to evidence this and the effective use of DPIAs is essential in order to demonstrate appropriate measures have been taken to ensure compliance.

DPIAs are particularly relevant when a new data process system or technology is being introduced. They should be completed at the beginning of a project to ensure they are integrated into the project design in order to:

- Build and maintain public confidence by ensuring that data is processed lawfully;
- Work more efficiently by only collecting and using the information needed, enabling BCH to confidently and proactively exploit data;
- Obtain clear direction for the project's use of data from the outset;
- Protect the public, staff and other individuals against the unlawful infringement of their rights;
- Avoid the need to redesign all or major parts of the project at a later stage;
- Minimise the cost of retrospectively incorporating data protection safeguards by building them into the project at an early stage;
- Avoid sanctions by the ICO such as fines of up to 20 million Euros.

Advice and guidance is sought from the DPO and from the Information management Unit for BCH.

The requirement to carry out DPIAs (and undertake prior consultation with the ICO in some cases) derives the GDPR Articles 35 & 36 and the GDPR Recitals 75, 84, 89 to 96 (where personal data is processed for any other purposes).

Roles and Responsibilities

Information Asset Owner

The DPIA process must be led by someone able to influence the design of a project. This may be the Information Asset Owner (IAO) of the information concerned or a designated OPCC single point of contact (SPOC).

The IAO or designated Force SPOC is responsible for:

- Ensuring that this policy and procedure is complied with;
- Considering advice provided by the Information Rights DPIA Advisor (Force) and others;
- Ensuring relevant IAO's are consulted;
- Ensuring that a DPIA Stage 1 Form (Force Form) is completed for their project and likewise for the DPIA Stage 2 Form (Force Form) where one is required
- Ensuring that information risks and appropriate mitigations are identified and implemented;

- Determining what residual risks are acceptable;
- Ensuring records of their project are created and maintained;
- Determining on an ongoing basis if and how the project should proceed;
- Ensuring the process is reviewed to check risk mitigations have been successful and identify whether any new risks have emerged that require an updated DPIA.

DPIA Advisor

A DPIA Advisor will be assigned from the Information Rights Unit.

The BCH DPIA Advisors are responsible for:

- Providing or signposting to advice, guidance and assistance to the project to improve project understanding of the law and this policy and procedure;
- Providing or signposting to advice, guidance and assistance to the project to enable data protection risks to be identified and possible mitigations determined;
- Determining if a DPIA Stage 2 Form needs to be completed;
- Ensuring that the completed DPIA meets the requirements of data protection legislation;
- Consulting with the Data Protection Officer (DPO);
- Determining if the ICO needs to be consulted before the project can be implemented and advising accordingly;
- Managing the consultation process with the ICO where it is necessary;
- Maintaining records of the DPIA process in case of future audit, complaint, investigation or enforcement action;
- Alerting relevant Information Asset Owners (and the Senior Information Risk Owner where appropriate) of any significant unacceptable data protection or information risks not mitigated by the project.

DPIA Advisors are **not** responsible for determining if and how the project should proceed – that is the responsibility of the IAO/OPCC SPOC. This will be in consultation with the Senior Information Risk Owner (SIRO) and the Data Protection Officer where there are any high risks.

Two Stage Process

Bedfordshire OPCC along with Bedfordshire Police have a two stage DPIA process.

The first stage is a screening stage to identify whether the project is likely to represent a high risk to individual's personal data. The second stage is a full risk assessment of the processing in order to identify and mitigate risks and ensure lawful processing. In some cases there will be no need to carry out the second stage.

The DPIA process must be seen as an ongoing activity so where changes to a process or element are identified the DPIA needs to be reviewed.

DPIA Stage 1

A DPIA Stage 1 Form (Force Form) must be completed at the beginning of a project involving personal data.

A project could include the introduction of new systems, processes, tools, techniques, services or contracts, as well as changes made to an existing system, including using existing personal data for new and unexpected or more intrusive purposes.

A DPIA Stage 1 Form (Force Form) must be completed at the initial stage of the project's lifecycle and before any significant decisions are made about the collection or use of personal data. This will ensure that any risks are identified and that safeguards are built into the design.

The completed DPIA Stage 1 will be assigned to a DPIA Advisor within Information Rights (Bedfordshire Police) who will review and provide one of the following assessments:

a) DPIA Stage 2 is not mandatory;
b) DPIA Stage 2 is not required as long as remedial actions listed are carried out.
c) DPIA Stage 2 is required.

Completion guidance for the DPIA Stage 1 Form can be found on the Intranet – Policies and Forms - Labelled - DPIA Fact Sheet 2 – Stage 1 Form.

DPIA Stage 2

If a DPIA Stage 2 is required the DPIA Stage 2 Form (Force Form) must be completed. A DPIA Stage 2 is likely to be required if the intention is to:

- Process criminal data on a large scale;
- Process data that could result in physical harm in the event of a security breach;
- Monitor a public place or places on a large scale;
- Use new technologies or techniques;
- Process biometric or genetic data;
- Combine, compare or match data from different sources;
- Conduct systematic, extensive, or large scale profiling;
- Process data relating to vulnerable people such as children;
- Process special categories of data on a large scale, such as health data;
- Collect data without a privacy notice;
- Conduct large scale processing; consider the number of individuals involved, the volume and/or range of data and duration of the activity;
- Allow non-police employees access to police systems.

Completion guidance for the DPIA Stage 2 Form (Force form) can be found on the Intranet – Policies and Forms - Labelled - DPIA Fact Sheet 3 – Stage 2 Form. The SPOC can also use the DPIA Fact Sheet 4 – Assessing DPIA Risks.

Once completed the DPIA Stage 2 Form should be submitted to the Information Rights Unit. The DPIA Advisor will review and support the Force SPOC in finalising the data protection risks and mitigations.

If there are no high residual risks the IAO can approve and sign off the DPIA.

If there are any residual high risks after mitigations the IAO will need to report to the SIRO, the DPO will be alerted and the DPIA must be submitted to the ICO for consultation prior to processing.

Information Rights will submit the DPIA by email to the ICO at dpiaconsultation@ico.org.uk.

The ICO will provide a written response advising whether the risks are acceptable, or whether we will need to take further action. They may advise us not to carry out processing because it would be in breach of the GDPR and they can if appropriate issue a formal warning or take action to ban the processing.