POLICE & CRIME COMMISSIONER
for Leicester, Leicestershire & Rutland
Your Communities - Your Commissioner

OPCC Policy and Procedure for Data Protection Impact Assessments (DPIAs)

Version v.1 July 23
Review Date: July 2025

Policy Owner:	Chief Executive Officer
Role Responsible:	Policy and Compliance Officer
Senior Manager Review:	Director of Governance and Performance
Protective Marking:	Official
Date of next review:	Jul 2025

Review log

Date	Minor / Major / No change	Section	Author
3/7/23	v.0.1 – First draft – combining previously drafted policy and procedure for DPIAs	All	8520 Forman (IM)and 7491 N Padhiar
7/9/23	Final Version	All	SMT – CEO Andrew Champness

Contents

1. Statement

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018, this document outlines the policy and procedure for the undertaking of Data Protection Impact Assessments (DPIAs) by the Leicestershire Office of the Police and Crime Commissioner (OPCC). This should be read in conjunction with the OPCC Data Protection Policy.

A DPIA is mandatory under the UK GDPR for any processing that poses a high risk to the rights and freedoms of individuals. This is essentially a tool which helps an organisation systematically and comprehensively assess the privacy risks to data subjects in relation to the processing of personal data[1] for a project[2]. The DPIA requires the organisation to identify and implement the appropriate mitigations in order to reduce the risk to the individual's privacy

The introduction of the General Data Protection Regulation (GDPR) EU 2016/679 placed increased emphasis on accountability and data protection by design and default. This means that data protection considerations and data subject's rights should be at the forefront of an organisation's planning, thinking, decision-making and design. The Leicestershire OPCC is committed to being accountable and protecting the rights of individuals with regard to the processing of their personal data. This policy and procedure is intended to embed a 'data protection by design and default' approach to OPCC activities by mandating the use of DPIAs at appropriate points in the OPCC's operational planning, project management, procurement and commissioning workflows.

The use of a DPIA has more wide-reaching benefits than just complying with the data protection legislation. A thorough DPIA allows the OPCC to obtain a clear direction for the project's use of data from the outset, as well as enabling them to work more efficiently by only collecting and using the data that is needed. A good DPIA will also help to protect the public, staff and other individuals against any unlawful infringements of their rights, whilst avoiding the need to redesign all or major parts of the project at a later stage. Overall this should help to minimise the cost of retrospectively incorporating data protection safeguards by building them into the project at an early stage. The process of completing a Screening Sheet, and where necessary a DPIA, helps to make certain that the OPCC meets its requirements in terms of UK GDPR for ensuring data protection by design and default, and the implementation of the appropriate technical and organisational measures to protect the data. Ultimately this is an integral part of compliance with the data protection legislation and will help to ensure that the Leicestershire OPCC

[1] Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[2] For ease of reference this term is used, but it should be taken to mean a new process, technology, way of working, service etc. – this may relate to operational planning, project management, commissioning or procurements for the OPCC

avoid costly sanctions from the Information Commissioner's Office (ICO), as well as any potential damage to their reputation.

2. Aims

This Policy and Procedure aims to:

- Set out the expectations of the PCC with regard to DPIAs including Screening Sheets[3] – what the process is for determining if one is required, when they should be completed and whom should complete them;

- Ensure that there are clear, consistent processes and structures to provide all staff with guidance for identifying and reducing data protection risks when embarking upon new projects; and

- Build and maintain public confidence by ensuring that DPIAs are completed as required and that data is processed fairly and lawfully.

3. Scope

This Policy and Procedure is applicable to all employees of the PCC for Leicestershire, as well as the Police and Crime Commissioner, Assistant Police and Crime Commissioners, volunteers, consultants, contractors and partner organisations. This document supports the OPCC Publication Scheme and its plans and strategies – it is designed to provide clarity and consistency in how and when DPIAs should be completed by the OPCC.

4. Responsibilities

Any persons looking to commence a new project, system, or process must ensure that the procedure outlined in this document is adhered to. The PCC will ensure that all persons working for the OPCC understand the importance of DPIAs, when they should be completed and by whom. The OPCC will liaise with the Leicestershire Police Information Sharing Advisors, Information Security, the OPCC DPO and any other relevant persons to ensure that the DPIA is completed to an appropriate standard.

[3] The Screening Sheet is a short, scoping question set which helps to determine whether or not a full DPIA is required, and what areas of processing are likely to be deemed as high risk

5. Policy

The following circumstances are instances in which a DPIA is likely to be required or need to be reviewed:

- The PCC are introducing a new project that involves the processing of personal data or operationally sensitive data;
- The PCC are commissioning for a new project; and/or
- The PCC are making material changes to an existing project.

Based on the ICO guidance, the Leicestershire OPCC will always carry out a DPIA for projects that:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Process special category data on a large scale;
- Systematically monitor a publicly accessible place on a large scale;
- Use new technologies;
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
- Carry out profiling on a large scale;
- Combine, compare or match data from multiple sources
- Process personal data without providing a privacy notice directly to the individual
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them; and/or
- Process personal data which could result in a risk of physical harm in the event of a security breach.

In accordance with the ICO guidance, the Leicestershire OPCC will also consider carrying out a DPIA for projects that include

- Evaluation or scoring;
- Automated decision-making with significant effects;
- Systematic processing of sensitive data or data of a highly personal nature;
- Processing on a large scale;
- Processing of data concerning vulnerable data subjects, including children;
- Innovative technological or organisational solutions; and/or
- Processing involving preventing data subjects from exercising a right or using a service or contract.

6. Procedure

The process for a DPIA will commence prior to any proposed changes, and before any processing of personal data takes place, in order that the data protection

implications can be fully understood and mitigated against. In practical terms, this means that initial the DPIA work should be undertaken prior to going to tender (i.e. at project initiation phase or its equivalent, or the business case stage – certainly before decisions are made about the project). It may be appropriate to insert the DPIA Screening Sheet (see **Appendix A**) within a relevant contract.

A Screening Sheet will be completed at the inception of a new project – this will be retained by the OPCC for reference, to facilitate timely reviews, and also in compliance with the accountability requirements of the UK GDPR. The Leicestershire Police ('the Force') Information Management Section will also keep a copy as they are providing support around data protection matters to the OPCC.

Where the Screening Sheet indicates a DPIA is required, this will be completed by the project lead or relevant expert in the proposed project or processing. The OPCC project lead will identify the most appropriate individual and delegate the work accordingly. This must be undertaken by an individual who understands the processing thoroughly and who has a clear idea of what the OPCC are trying to achieve. Where the OPCC decides not to carry out a DPIA, this must be documented with the rationale for this on the DPIA Screening Sheet. The project lead must then liaise with the Operations and Compliance Manager who will review the Screening Sheet and rationale, and send to the Data Protection Officer (DPO).

All DPIAs completed by the OPCC will:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess any risks to the individual; and
- Identify any additional measures to mitigate those risks.

A DPIA may cover a single processing operation or a group of similar operations, and joint controllers can do a joint DPIA. For example, it is likely that the OPCC and Leicestershire Police will need to work collaboratively on some DPIAs, where there is a joint means and purpose for the processing. It is important that DPIAs are not seen as a one-off exercise and that they are instead viewed as an ongoing process, and as such are embedded into the OPCC organisational processes.

In order to assess the level of risk, the OPCC will consider the likelihood and severity of any impact to individuals. Clearly where a project carries a high probability of harm to an individual or group of people, it will be considered as high-risk. The Leicestershire Police Information Management Section and the DPO can be consulted throughout the DPIA process for feedback and guidance, and an ad-hoc meeting can be arranged where necessary to discuss the processing. Once the project lead has reviewed and signed off the DPIA, this will be sent to the Operations and Compliance Manager who will review and send the document for risk assessment by the DPO.

The completed DPIA will be reviewed by the DPO who will objectively assess the project and determine if the residual risk is low, medium or high. Where necessary, the DPO will liaise with the OPCC (and if necessary the ICO) to further examine the risks involved and identify any further mitigations. DPIAs with a high residual risk will be sent to the ICO for their consideration and advice – no processing of personal data will take place until a decision has been made and returned to the PCC from the ICO. Only when the DPO is satisfied that the risks have been reduced to an acceptable level will the DPO approve the project for the next stage of sign-off.

The OPCC have determined that the DPIAs will be sent to the Policy and Compliance Officer who will liaise with the Director of Governance and Performance and Chief Executive as deemed necessary, with regard to the risks related to DPIAs. Whilst the sign-off of DPIAs has been delegated to the Director of Governance and Performance, it is recognised that the Chief Executive **remains the overall risk-owner for the OPCC. This responsibility cannot be delegated.**

The DPIA will then be registered with the Policy and Compliance Officer who will maintain an up-to-date list of current OPCC DPIAs. The final DPIA (subject to exemptions) will be submitted to a publically available register in line with the guidelines from the ICO.

Any mitigations identified in the DPIA **must** be integrated back into the project delivery plan, and should be kept under review to ensure they are working effectively to minimise the risks. The recommendations of the DPO (and for high-risk processing, the ICO) must be implemented in full. Where a decision is made to go against the advice issued by the DPO, this must be recorded with the rationale.

The DPIA will be a living document, and as such will be subject to periodic review. Any personal data processing, whose conditions of implementation (the scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since prior checking by the supervisory authority (the ICO) or the DPO, and which are likely to result in a high risk, will be subject to a comprehensive DPIA review. In summary, any material changes to the processing for a project must prompt an immediate review of the Screening Sheet and/or DPIA.

OPCC Commissioning

One of the key roles of the OPCC is to commission services; these services may, or may not, involve the processing of data held by the Force, and could include all categories of personal data and/or operationally sensitive data. Where the OPCC are commissioning a service, it is agreed that the OPCC will carry out the initial Screening Sheet for the intended processing of such services at the start of the commissioning. The OPCC will be assisted with this by the Force Information

Management Section at meetings held on at least a 4-weekly basis. This is to ensure that this process is commenced at the earliest possible opportunity.

Where Force data is to be processed as part of the service commissioned by the OPCC, an appropriate Force Lead or Single Point of Contact (SPoC) must be identified at the very earliest opportunity within the relevant business-area of the Force, this is to ensure that the DPIA (where required) and any other necessary data protection related work is completed prior to the commencement of the processing. Whilst this will ultimately be the responsibility of the Force (on behalf of the Chief Constable as the Data Controller), this is likely to be a collaborative piece of work between the OPCC and the Force, with both organisations working together to ensure that the document is completed appropriately, and in a timely manner.

Where Force data is not required for the processing, the Screening Sheet will be used by the OPCC to identify the potential high-risk areas of processing, and to ensure that those who are processing personal data as part of the commissioned service (e.g. partners such as Local Authorities) carry out a DPIA where this is appropriate.

Although the OPCC are generally not the Data Controller for the information being processed for commissioned services, the completion of a Screening Sheet offers the following benefits to the organisation:

- Forms part of the OPCC's due diligence;
- Ensures that the process in which services are commissioned by the OPCC facilitates, encourages and elicits data protection by design and default by the relevant partners – a requirement under UK GDPR;
- Protects the reputation of the OPCC – reduces the risk of data protection issues or security breaches linked to services commissioned by the OPCC;
- Permits early engagement and co-operation (if appropriate) by the Force and partners' Information Management Sections – identifies high-risk services at an early stage;
- Promotes more effective partnership working between the OPCC and the Force, particularly where the commissioning phase 'dovetails' into a service involving the processing of Force-held data;
- Avoids costly mistakes being made in the commissioning phase – changes to the envisaged services after commissioning can impact on the timely delivery of such work streams, and can have a significant financial and reputational impact;
- Enables the OPCC to ensure that the contracts agreed are appropriate and that the processing required to fulfil them is lawful; and
- Helps to ensure the accountability and integrity of the commissioned services, and also improves the transparency to the public.

See **Appendix B** – Table to summarise OPCC and Force actions for DPIAs

7. Legal Basis

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

8. Monitoring

This Policy and Procedure will be monitored to ensure effective compliance. Monitoring will be the responsibility of the document owner, who will be responsible for developing and reviewing accordingly.

- Active monitoring will be undertaken by supervisors deployed into all relevant business areas.
- Where this document is being managed through a project, the project lead will review at regular times with the project managed through the project plan reviews.

This monitoring will:

- Ensure this document has been put into practice;
- Check that all the elements are operating properly and the information is up-to-date;
- Verify that any published policies and procedures are being applied and complied with;
- Ensure the aims of this document are being achieved.

Staff engaged within business areas will also be expected to undertake personal responsibility to ensure the Policy and Procedure is adhered to.

Associated Documents:

OPCC Data Protection Policy.

Appendices

Appendix A

DPIA Screening Sheet

Project name:

Please complete the DPIA Screening Sheet, this will help to determine whether any of the processing[4] may be considered a "high-risk" type of processing and therefore whether a full DPIA is required to assess this.

	If you answer "yes" to any of the following questions, a DPIA is mandatory:	**Yes / No/Maybe**
1	**Does the project use systematic and extensive profiling or automated decision-making to make significant decisions about people?**	
	Systematic – occurs according to a system, is pre-arranged, organised or methodical, takes place as part of a general plan for data collection, or is carried out as part of a strategy. **Extensive** – implies that the processing covers a large area, involves a wide range of data or affects a large number of individuals. **Profiling** – the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people, e.g. work, economic situation, health, location, movement, behaviour.	
2	**Does the project process special category data or criminal offence data on a large scale?**	
	Special category data – broadly similar to sensitive personal data (under what was DPA 1998). Refers to information which requires more protection due to the increased risk of discrimination, e.g. ethnic origin, religion, political beliefs, trade union membership, health, sexual orientation, sex life, biometrics and genetics. **Criminal offence data** – personal data relating to criminal convictions and offences or related security measures. **Large scale** – consider the number of individuals concerned, the volume of data, the variety of data, the duration of the processing, the geographical extent of the processing.	
3	**Does the project systematically monitor publically accessible places on a large scale?**	

[4] Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [Article 4(2), UK GDPR, 2016/679]

4	**Does the project use new technologies?** **New technologies** – this concerns new developments to the state of technological knowledge in the world at large, or the novel application of existing technologies (including AI), rather than technology that is new to you. A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software where this is likely to be used by different data controllers to carry out different processing operations.	
5	**Does the project use profiling, automated decision-making or special category data to help make decisions on someone's access to a product, service, opportunity or benefit?**	
6	**Does the project carry out profiling on a large scale?**	
7	**Does the project process biometric or genetic data?** **Genetic data** – personal data relating to the inherited or acquired genetic characteristics of a data subject, which gives unique information about the physiology or the health of that individual and which in particular, from analysis of a biological sample from the individual in question – such as DNA. **Biometric data** – personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristic of a natural person, which allow or confirm the unique identification of that natural person – such as facial images or fingerprints.	
8	**Does the project combine, compare or match data from multiple sources?** For example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.	
9	**Does the project process personal data without providing a privacy notice directly to the individual?**	
10	**Does the project process personal data in a way which involves tracking individuals online or offline location or behaviour?**	
11	**Does the project process vulnerable person's personal data (including children) for profiling or automated decision-making, or for marketing purposes, or offer online services directly to them?** **Vulnerable persons** – may include children, employees, mentally ill patients, asylum seekers, the elderly, mentally ill persons etc. – such individuals may not be able to easily consent to, or oppose, the processing of their data, or exercise their rights.	
12	**Does the project process personal data which could result in a risk of physical harm in the event of a security breach?**	
13	**Does the project involve invisible processing?** **Invisible processing** – processing of personal data that has not been obtained directly from the data subject without providing the data subject with the information explaining the processing.	

14	**Does the project involve preventing data subjects from exercising a right, or using a service or contract?**	
15	**Does the project involve processing which involves tracking an individual's geolocation or behaviour including, but not limited to, the online environment?**	
If you answer "yes" to any of the following questions, a DPIA must be considered:		
16	**Does the project involve evaluation or scoring?** This includes profiling and predicting from aspects concerning the data subject's performance at work, economic situation, health, personal preference or interests, reliability or behaviour, location or movements.	
17	**Does the project involved automated decision-making with legal or other similar significant effects?** **Significant effects** – has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way. **Legal effect** – something that affects a person's legal status or legal rights.	
18	**Does the project involve systematic monitoring?** Systematic monitoring – processing used to observe, monitor or control data subjects, including data collected through networks or a systematically monitoring of a public area. In these circumstances data subjects may not be aware of who is collecting their data and how it will be used, additionally it may be impossible for individuals to avoid being subject to such processing.	
19	**Does the project involve the processing of sensitive or data of a highly personal nature?**	
20	**Does the project involve processing on a large scale?**	
21	**Does the project involve the processing of data concerning vulnerable data subjects (including children)?**	
22	**Does the project involve innovative technological or organisational solutions?** This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individual's rights and freedoms – for example, use of facial recognition or fingerprint for authentication.	

If, having completed the above assessment, you decide not to carry out a DPIA you **must** document your reasons for this decision below:

Name:	Date:

The Screening Sheet must be dated and signed above, then submitted to the Information Management Section for their consideration – The Data Protection Officer (DPO) may be consulted where necessary.
Following this consultation, if the decision remains not to carry out a DPIA, the views of the DPO must be recorded below:

Name:	Date:

Appendix B

Table to summarise OPCC and Force actions for DPIAs

Project type	OPCC actions	Force actions
Project based in the OPCC involving only data under the Controllership of the PCC Services commissioned by the OPCC involving only OPCC data	• Screening Sheet completed by OPCC at the inception of the project / commissioning • DPIA completed by OPCC if required • Outcome of Screening Sheet (and DPIA if required) used by OPCC to shape project – Data Protection by design and default	• IM advise on and support process
Service commissioned by the OPCC involving Force data under the Controllership of the Chief Constable	• Screening sheet completed jointly by the OPCC and Force at the inception of the project • Outcome of Screening Sheet used to shape project commissioning – Data Protection by design and default • Force lead identified and Force IAO involved at inception • Completed Screening Sheet and responsibility for the DPIA handed over to Force lead to complete	• IM to advise on and support process • Force to take responsibility for the DPIA (linking in with the OPCC where necessary and appropriate
Service commissioned by the OPCC not involving Force or OPCC data	• Screening Sheet at the inception of the project • Outcome of Screening Sheet used to shape project commissioning – Data Protection by design and default • DPIA to be completed by the partners who will be processing personal data	• IM to advise on and support process