Data Protection Impact Assessment

This template is a method by which you can record your Data Protection Impact Assessment (DPIA) process and outcome. It follows the process set out in the ICO DPIA guidance, and you should read it alongside that guidance Data protection impact assessments | ICO. It provides the Criteria for an acceptable DPIA set out in European guidelines on DPIAs (S28 Working Party).

This assessment is a statutory requirement under Part 3 Data Protection Act 2018 (DPA).

Before commencing, check the ICO guidance screening checklist in appendix A to see if you need to complete a DPIA. It is anticipated that a DPIA will be required for the majority of police processing.

If you decide not to carry out a DPIA, document your reasons in the box below. Refer to the numbers in the checklist to evidence your decision and submit a copy to the Data Protection Officer for advice. Please keep this form with the project documents as evidence of the DPIA consideration having been made.

Not applicable

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes of the DPIA into the project plan. You may find that you are able to fill out parts of the assessment in a manner other than in strict chronological order and occasionally have to revisit some steps as your project develops. The Data Protection Officer (DPA2018 S71(1)(b)) and/or the Information Assurance Coordinator are able to provide advice and assistance with this assessment.

Version control

Revision number	Date	Update/Status	Author
1	03/08/2023	Newly revisited DPIA following	ACE & Faculty **S40(2)** / **S40(2)** / **S40(2)**
2	23/11/2023	Updated DPC flow diagram, comments from David Angell	**S40(2)**

Step 1: Identify the need for a DPIA

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. Also insert the numbers from the Appendix A checklist which assisted your decision to complete a DPIA

Background and Context:
At present, policing data analytics capabilities tend to be either commercial products designed for analysts or a mix of tradecraft and office automation tools such as Excel. A gap therefore remains in the system, whereby simple tools to aid the more effective and efficient operational use of data is not available to front-line investigators.

To address this, the Home Office Police and Public Protection Technology Insights Centre (PPPT IC) has developed a prototype 'Find and Profile (F&P)' **S31(1)**

The tool was developed in collaboration with the Home Office's Accelerated Capability Environment (ACE), using live operational data, and was **S31(1)**

Following the success of this prototype in demonstrating the value of AI and data analytics to police operations, a project to deliver an expanded trial to additional ROCUs has been commissioned to prove the value of the tool in other ROCUs, identify areas of tool development and make the tool widely available. The Home Office Capability Reforms Unit and the NPCC Centre for Data and Analytics (CDAP) is leading this piece of work. Alongside testing the value of the tool, the strategic aim is to deploy the tool and make it nationally available through Police Digital Services (PDS) platform. **S31(1)**

The trial forms part of the Home Secretary's £20m initiative to disrupt the County Lines model, specifically: *Investment in technology to disrupt county lines operations.*

S31(1)

S31(1)

[redacted]This is the only way to identify the patterns of interest in a way which will inform the analytics and subsequently used operationally for targeted enforcement.

The purpose is consistent with the original law enforcement purpose for which the personal data was collected, and the processing is not intended to have any effect on individuals whose personal data is held within the ANPR records.

The tool can only be used within a ROCU by NAS trained users and so the use of the ANPR data is already lawfully justified.

This DPIA covers the use of the tool on a nationally hosted platform (PDS) for the **S31(1)**

A DPIA is appropriate for the following reasons from Appendix A:

4. Use new technologies.
9. Process personal data without providing a privacy notice directly to the individual.
20. Innovative technological or organisational solutions.

This DPIA references:

1. The NAS DPIA: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/858735/ANPR__DPIA.pdf
2. The National ANPR Standards for Policing and Law Enforcement (NASPLE):
3. PLACEHOLDER: PDS Risk Assurance Arrangement

Step 2: Describe the processing

2a-Describe the nature of the processing

Step 2: Describe the processing

2a-Describe the nature of the processing:

a) How will you collect, use, store and delete data?
b) What is the source of the data?
c) Will you be sharing data with anyone? If so who?
d) You might find it useful to refer to a flow diagram or another way of describing data flows.
e) What types of processing identified as likely high risk are involved?

The following assumptions underpin this DPIA:

1. Processing will be in line with the NAS DPIA
2. **S31(1)**
3. **S31(1)**
   S31(1)
4. **S31(1)**

5. The PDS platform has sufficient logging to support the DPA.
6. The PDS platform provides a mechanism for 2FA (two factor authentication) to be used on the tool. This requires the user to have a work mobile phone.
7. The platform has been security accredited

A - How will you collect, use, store and delete data?

The following diagram sets the context of the end-to-end processing of the data:

S31(1)

S31(1)

The following diagram shows a process flow which will utilise the environment shown above.

The use of the data is to improve the ability to prevent, detect and disrupt serious and organised drugs trafficking, aka county lines. This may be achieved in 2 ways. Firstly by identifying evidence or new lines of enquiry in ROCU investigations and secondly, by informing policing investigative processes.

S31(1)

S31(1)

Collection

S31(1)

Storage

S31(1)

Users will do some analysis on the raw data and their targeted and analysed output will be exported from the tool onto their local computer. ROCUs need to confirm the terms of use of this filtered and targeted data to ensure they only hold it while it is justified and proportionate in line with the Management of Police Information (MOPI).

All data is encrypted at rest and in transit.

3. Access

Users should be able to access the tool using a URL on their own machine.
Users will need to authenticate to use the tool with a username and password.
Authenticated users can upload **S31(1)** data into the tool from their local machine.
Users will only be able to see their own data that's been uploaded.

4. Combination/Alteration

S31(1)

5. Deletion

As per the NASPLE, although data is required to be reviewed every 7 days and deleted if no longer needed, within this trial all data will be deleted at the end of the day on a schedule. Data of continued relevance to ROCU investigations may also be retained by them under provisions of the Criminal Procedure and Investigations Act (CPIA) or the Management of Police Information (MOPI) principles as appropriate.

B - What is the source of the data?

S31(1)

C - Will you be sharing data with anyone? If so, who? (Step 6 on the diagram)

S31(1)

Filtered and targeted output data from the tool can be exported for use to provide to local police to action the intelligence. ROCUs need to confirm the terms of use of this filtered and targeted data to ensure they only hold it while it is justified and proportionate in line with the Management of Police Information (MOPI).

E - What types of processing identified as likely high risk are involved?

One of the aims of the project is to understand the use of AI and data analytics of this nature in policing, in conjunction with human decision making. Any investigative leads generated by the project will be reviewed by the appropriate police investigators and should be treated as an indicative source.

2b-Describe the scope of the processing

2b-Describe the scope of the processing:

a) what is the nature of the data?
b) Does it include special category or criminal offence data?
c) How much data will you be collecting and using?
d) How often?
e) How long will you keep it?
f) How many individuals are affected?
g) What geographical area does it cover?

A - what is the nature of the data

S31(1)

S31(1)

B - Does it include special category or criminal offence data?

This will not contain any special category data. The basic premise is that vehicles of interest are involved in county lines drugs trafficking.

C - How much data will you be collecting and using?

For the duration of the trial the following data will be collected.

S31(1)

Filtered and targeted ANPR data

S31(1)

D - How often?

The data will be collected daily by ROCU users based on their intelligence picture for the duration of the trial. After this, users will no longer have access to the tool **S31(1)**

E - How long will you keep it?

Raw NAS ANPR data

Once users upload data into the tool it is temporarily stored in a database, the data will be deleted on a schedule from the database daily at night.

Filtered and targeted ANPR data

Once users export the data it is temporarily stored in a database, the data will be deleted from the database daily at night on a schedule.

Once the data is exported it is up to the ROCUs to follow the NAS DPIA and terms of use and only hold the report while it is justified and appropriate for their investigations.

The VRM is classed as personal data as it can be linked back to an individual via the DVLA registered keeper database, but only NAS trained users will be using the tool and they already have a lawful basis for access.

When looking at ANPR data covering large geographical areas it is possible that millions of VRMs will be collected.

At the end of the trial all data from the database will be deleted and this will be confirmed. Users will no longer have access to the tool and so will not be able to generate new data.

G - What geographical area does it cover?

S31(1)

2c-Describe the context of the processing

2c-Describe the context of the processing:
What is the nature of your relationship with the individuals?

a) How much control will they have?
b) Would they expect you to use their data in this way?
c) Do they include children or other vulnerable groups?
d) Are there prior concerns over this type of processing or security flaws?
e) Is it novel in any way?
f) What is the current state of technology in this area?
g) Are there any current issues of public concern that you should factor in?
h) Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

S31(1)

As stated in the NAS DPIA, information is available to the public about NAS and ANPR. The processing in this project is an extension of the analysis done in relation to serious and organised crime. The project aims to test the technical possibilities which will inform decision making about investment in further capability development and inform the ethical decision about the use of this technology.

The data does not include children or any vulnerable groups.

The use of current technologies with VRM data, accredited AWS based environments, and advanced analytics and rule-based analysis have been proven in many scenarios within the Home Office and Law Enforcement.

S31(1)

The project will engage with the Home Office Data Ethics Advisory Group and Biometrics and Forensics Ethics Group(BFEG) to ensure compliance is maintained throughout.

The project will conform to the following standards, codes of practice or guidelines:

- National ANPR Standards for Policing and Law Enforcement (NASPLE)
- GDS Data Ethics Framework
- ICO guidance on AI and data protection – via the online toolkit
- GDS/Office for AI – A guide to using artificial intelligence in the public sector

2d-Describe the purposes of the processing

2d-Describe the purposes of the processing:

a) What do you want to achieve?
b) What is the intended effect on individuals?
c) What are the benefits of the processing for you, and more broadly?

The purpose of the processing is to improve the ability for law enforcement to prevent and detect serious and organised drug trafficking in the form of county lines.

The threat landscape for County Lines is complex and multi-faceted, but the focus of this project is criminal's use of vehicles and the road network, with the core dataset of interest being the national ANPR dataset and force specific county lines data to identify known vehicles and routes of county lines activities. One of the goals of the project is to establish whether advanced analytics including machine learning hosted on a national platform eventually, but in this case PDS, can identify additional lines of enquiry based on operational tradecraft and patterns identified in known county lines vehicles.

In the case that investigative leads are identified these will be followed up by the police investigation teams. Any written or recorded outputs for the project will be retained by each ROCU under MOPI and any material used by the Home Office will not include VRMs (or any other personally identifiable information).

If this project leads to improved capability to disrupt county lines, individuals will benefit from reduced crime specific to county lines but also increased efficiency of the police. Automated analytics will reduce the risk of human error or insufficient training leading to incorrect identification of vehicles of interest.

The broader benefits of the specific project are that any decisions to further use the technologies tested will have an evidence-base, including the effectiveness and any ethical considerations.

Step 3: Consultation process

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

a) Describe when and how you will seek individuals' views or justify why it's not appropriate to do so.
b) Who else do you need to involve within your organisation?
c) Do you need to ask your processors to assist?
d) Do you plan to consult information security experts, or any other experts?

The following will be consulted:

CC Charlie Hall, ANPR NPCC lead will be providing approval for the work to be carried out as the Data Controller for NAS.

Each participating ROCU and their associated data protection officer.

Police Digital Service (PDS), in particular the platform team and cyber assurance team.

Different DPA related artefacts are required for the NAS and CL data and the following roles have been proposed at a high level, and the details are being produced in parallel.

Diagram for editing can be found here

S31(1)

Step 4: Assess necessity and proportionality

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

a) What is your lawful basis for processing?
b) Does the processing actually achieve your purpose?
c) Is there another way to achieve the same outcome?
d) How will you prevent 'function creep' *(the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, esp when this leads to potential invasion of privacy)*?
e) How will you ensure data quality and data minimisation?
f) What information will you give individuals?
g) How will you help to support their rights?
h) What measures do you take to ensure processors comply?
i) How do you safeguard any international transfers?

The processing is necessary for the prevention and detection of serious and organised drug trafficking and will be conducted under Part 3 (Law Enforcement Processing) of the Data Protection Act. The NAS DPIA considers the ECHR Article 8 right to a private life.

S31(1)

The trial is focussed on the county lines mission and is time limited to 8 weeks per ROCU. At that point an evaluation of the accessibility of the technology at a national scale, success of the technology and the ability to integrate into policing operations and the ethics will be made prior to further rollout. Any change of scope may require a new DPIA.

S31(1)

There will be no transfers of data or information outside of the EEA.

Step 5 ICT Security Arrangements

Step 5 ICT Security Arrangements.

If necessary, liaise with ICT staff about this section especially if there is an IT Project Manager. This will be mutually beneficial because it could avoid a duplication of effort by the person(s) completing this assessment and the IT personnel. This is particularly the case if data is to be subject to 'Cloud' storage because IT may have already assessed this against the 16 Cloud principles and can provide more comprehensive information for this assessment.

a) How will you gather the data?
b) By which method(s) do you intend to share the data with third parties?
c) What are the Government Security Classifications for the data? (See policy)
d) On which system do you intend to store the data gathered?
e) Where will the data be stored?
f) What safeguards are in place to protect the data?
g) What standards of security are met?
h) Is there an external data processor involved?
i) Do you have a data processing agreement in place with any external processor?

NOTE: This is an addition to the standard ICO DPIA template

S31(1)

The project team are working with PDS on the platform requirements. It is expected that the PDS platform has the following characteristics:

- The platform will be security accredited to PDS standards and is hosted in the Azure UK Region.
- Users will access the tool with URL using reverse proxy.
- Users will not have direct access to the platform only to specified tools
- Admins on the system will have access to the database that temporarily holds the ANPR data but they have no need to look at the data
    - Any access to the data will be logged

Further details of the design are available. The diagram below illustrates the High-Level Design.

S31(1)

Step 6: Identify and assess risks

S31(1)

Step 7: Identify measures to reduce risk

S31(1)

Sign off and record outcomes – National ANPR Service

Step 8: Sign off and record outcomes		
	Name/Role/Date	**Notes**
Measures approved by Project lead?	YES/NO and comments and date	
Residual risks approved by Project lead	YES/NO and comments and date	If accepting any residual high risk, consult the ICO before going ahead. This must be done via the DPO as ICO SPOC.
DPO advice provided:	Mandatory	DPO should advise on compliance, steps 5 and 6 measures and whether processing should proceed
Summary of DPO advice: ***Subject to security accreditation of the platform by PDS, I am content for this data processing to proceed as detailed for the 14 week period outlined. This DPIA is consistent with previous DPIA iterations presented to me, and demonstrates the natural progression and review of this work over time.***		
DPO to register the DPIA and provide a reference No. here > **2023-08-31 Find and Profile**.		
DPO to identify existing or nominate new Information Asset Owners (IAO). **CC Charlie Hall**		
List Systems and IAO involved		
DPO to decide; Must the ICO be consulted in respect of this assessment (DPA 2018 S65)? – YES/**NO** – If YES the DPO as Force SPOC must make the referral to the ICO.		
DPO advice accepted or overruled by relevant Information Asset Owner(s)	YES/NO and comments and date	If overruled, you must explain your reasons in the comments area below.
IAO Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	**S40(2)** – Director of Information for BCH – NAS Data Protection Lead.	The DPO should also review ongoing compliance with DPIA

APPENDIX ‘A’

ICO guidance ‘At a glance’

- A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for certain listed types of processing, or any other processing that is **likely to result in a high risk** to individuals’ interests. You can use our screening checklist to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Checklists

DPIA screening checklist

Always carry out a DPIA if we plan to:

1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
2. Process special category data or criminal offence data on a large scale.
3. Systematically monitor a publicly accessible place on a large scale.
4. Use new technologies.
5. Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit.
6. Carry out profiling on a large scale.
7. Process biometric or genetic data.
8. Combine, compare or match data from multiple sources.
9. Process personal data without providing a privacy notice directly to the individual.
10. Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
11. Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
12. Process personal data which could result in a risk of physical harm in the event of a security breach.
13. Consider carrying out a DPIA if you plan to carry out any other:
14. Evaluation or scoring.
15. Automated decision-making with significant effects.
16. Systematic monitoring.
17. Processing of sensitive data or data of a highly personal nature.
18. Processing on a large scale.
19. Processing of data concerning vulnerable data subjects.
20. Innovative technological or organisational solutions.
21. Processing involving preventing data subjects from exercising a right or using a service or contract.
22. If you decide not to carry out a DPIA, document your reasons.
23. Consider carrying out a DPIA in any major project involving the use of personal data.
24. We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.