



OFFICIAL-SENSITIVE
(When complete)

Data Protection Impact Assessment (DPIA) – Stage 1

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material available before completing the form.

Data Protection Impact Assessment (DPIA)	
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.	
Section 1 - Governance	
Project Proposal Name:	National Data Analytical Solution (NDAS)
Information Asset Owner:	Chief Constable
Information Custodian:	Superintendent
DPIA Coordinator:	
Date on which processing will commence:	18/11/2019
Date submitted to DPO:	24/10/2019
Note: DPO will give an initial response within 10 working days of receiving the completed form.	
DPO Assessment	
DPO Use Only	
A. DPIA is not mandatory.	<input type="checkbox"/>
B. DPIA is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	<input type="checkbox"/>
C. DPIA is mandatory.	<input checked="" type="checkbox"/>



OFFICIAL-SENSITIVE

(When complete)

Section 2 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

The proposal of the National Data Analytics Solution (NDAS) is to develop a data analytics capability for use by UK law enforcement which will support officer decision-making to reduce crime and create efficiencies. NDAS collates existing local police force data onto a secure, cloud-based web platform and derives operational and strategic insight from this data through the application of algorithms (known as 'use cases').

NDAS is a national programme funded by the Home Office and implementation is led by West Midlands Police (WMP) in collaboration with [REDACTED]. There are currently seven further partner forces in the programme, alongside the [REDACTED].

Use cases are developed according to partner force priorities (e.g. modern slavery, sexual offences) and in collaboration with the Home Office. In the development of a use case, NDAS receives a wide ranging and large amount of data which is already held within a police forces' computer systems. This includes all categories of personal data and will include some special category data. This data is processed and stored on a secure cloud platform. All of the data processed on the harmonised layer has been gathered and retained in the first instance by a police force for a policing purpose.

NDAS applies advanced analytics and machine learning techniques to the data to provide insights for the police force(s) that have provided their data. Using these techniques, and through presentation of data in an online dashboard, NDAS is able to reveal insights from data which may otherwise have remained unseen or taken a significant amount of time and resource to uncover. This information can be used by officers to support operational and strategic decision making and will assist them in their mission to protect the public and reduce crime.

NDAS will process data from multiple disparate systems not normally performed in traditional operational methods, and therefore creates opportunity for previously unavailable insight to be presented.

The data is processed using a range of statistical techniques to gain insights. The use of data range in complexity from basic counts, sums and averages on individual data items to advanced machine learning derived techniques that identify complex correlations and interactions between multiple data items in the dataset. The outputs of this process are a deeper understanding of the data with the potential to discover previously unidentified relationships.



OFFICIAL-SENSITIVE

(When complete)

The necessity to process the data by the NDAS project is three fold:

1. To meet demand due to the significant increase in the volume and complexity of digital data held by UK Law Enforcement Agencies (LEA).
2. To provide efficiency opportunities, this coupled with a continuous increase in demand on Police and LEA required the need to develop new and more efficient data solutions.
3. To provide increased focus on prevention of crime with greater emphasis on anticipating potential harm before it occurs, identifying vulnerable individuals in need of safeguarding and targeting interventions towards the high risk persistent and prolific offenders.

The processing of individuals personal data by NDAS is considered proportionate as it will be used to assist in the prevention and detection of serious offences which include: serious sexual offences, firearms offence, serious violence offence and offences relating to modern slavery which may not have been identified using conventional policing methods.

NDAS is fully funded until March 2022 and has already built several proofs of concept and it has also started to operationalise use cases, launching a Controlled Pilot Go-Live of a modern slavery use case in March 2021 with [REDACTED]. Over the coming financial year NDAS will look to operationalise further use cases on modern slavery, sexual offences, firearms, organised exploitation, and organised crime communications. NDAS will work closely with partners to ensure it continues to develop capability in priority areas, shares knowledge and builds capacity across the policing sector.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

NDAS will be using a broad variety of data from various Police data sets. As such all categories of personal data will be used in the processing they will include Names, Date of births, Addresses, Communication data: Telephone numbers, emails, and Criminal records.

NDAS receives structured and tabular data from key policing systems, such as Crime, Intelligence and Custody, these may contain some personal data from some of the special categories, where these have been recorded by that Force when required. NDAS will not be processing special category data on its own to produce any insight, however textual information will exist (mainly in free text description fields) within the data provided related to special category data.

NDAS data will not contain data in multi-media format, such as photos or fingerprint images.

No Genetic or Biometric data will be processed.



OFFICIAL-SENSITIVE

(When complete)

2.3 Will special category data be used in the proposal? (Select all that apply)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Race | <input type="checkbox"/> Trade union membership |
| <input checked="" type="checkbox"/> Ethnic origin | <input type="checkbox"/> Genetic Data |
| <input checked="" type="checkbox"/> Political opinions | <input type="checkbox"/> Biometric Data |
| <input checked="" type="checkbox"/> Sex life | <input checked="" type="checkbox"/> Sexual orientation |
| <input checked="" type="checkbox"/> Religion | <input type="checkbox"/> Health |
| <input type="checkbox"/> Philosophical beliefs | <input type="checkbox"/> None |

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in the WMP's possession, from a different force.

NDAS will obtain the data for processing from established data sets already held by Police Forces or LEA. The data obtained will have been lawfully collected by the originating Police Force or LEA and be held for a policing purpose. NDAS will not be collecting any new data.

The data will be securely transferred to NDAS by established security accredited methods preventing the risk of any breaches of the Data Protection Act.

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

Data will be processed by the application of advanced data analytics across the data sets provided based on the requirements of the specific use case. Each partaking force will provide relevant data sets for respective use cases to the NDAS platform.

Data will be stored on the NDAS platform in a secure 123 cloud environment, in-line with relevant government grading requirements. The data sets provided by a Police Force or LEA will be kept segregated and not directly shared with any other partner force or outside agency.

Once the data is on the NDAS platform, it will be used to form and deploy analytical use cases specific to policing priorities. Insight from the analytical use cases will be provided to a small number of specific end users, with the relevant training to assist in their decision making for the detection and prevention of crime based on the specific use case.

New data will be ingested in full every week from Police Forces or LEA this will replace the previous processed data. Since previous data will be replaced with the new data, any deleted data in the source system will no longer be available in the NDAS live environment in line with the Review, Retention and Deletion (RRD) policy.

NDAS will archive previous processed data in a cold storage which will not be available in the live environment to end users. It will only be accessible by security cleared NDAS development team. All archived data will be deleted after 12 months based on data lifecycle policies and once deleted will not be able to be retrieved. This archived data can be retrieved within 3-12 hours and can be made available if the correct authorisation is obtained.

2.6 How many individuals will the processing affect? (Please specify one answer below)



OFFICIAL-SENSITIVE

(When complete)

- Fewer than 100 data subjects
- 100 to 1000 data subjects
- 1000 to 5000 data subjects
- More than 5000 data subjects

2.7 What categories of data subject are involved? (Please select all applicable categories below)

- Persons suspected of having committed or being about to commit a criminal offence
- Persons convicted of a criminal offence
- Persons who are or may be victims of a criminal offence
- Witnesses or other persons with information about offences
- Children or vulnerable individuals
- WMP staff (current and former)
- Other

If other then please provide further details below: **N/A**

2.8 Will it involve the collection of new information about individuals? Will WMP collect data that it has not previously collected or had access to?

- Yes
- No

2.9 Data Sharing

Does the processing involve:

Select one option

2.10.1	Data being shared with third parties external to WMP or recipients that have not previously had routine access to the information?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.10.2	Transferring data outside the UK but within the EU?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
2.10.3	Transferring data outside the EU?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
2.10.4	Storing data using a cloud service provider?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.10.5	Is there an ISA, contract, or other sharing agreement in place with all parties with whom data will be shared?	<input checked="" type="checkbox"/> Yes – agreements in place <input type="checkbox"/> Not yet – agreements required <input type="checkbox"/> No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?

For example, can the aim be achieved by using less data or different types of data?



OFFICIAL-SENSITIVE

(When complete)

Are all categories of data necessary to achieve the aim?

Conventional methods for the prevention and detection of offences for which NDAS supports will still continue by the respective Police Force or LEA.

The necessity for NDAS to process personal data is to provide new and efficient additional support to already established policing methods for high priority policing issues and operational requirements in a use case. This is based on the need to efficiently process high volumes of digital data held by Police and LEA, reducing the demand placed on Police and LEA resources to provide a greater focus for the prevention and management of serious crime.

All the data is used is necessary to give the most accurate and informed insight. By using less data would hinder the effectiveness of the project and provide less informative insight.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal.

Weigh the advantages of achieving your purpose against disadvantages to data subjects.

The use of personal data is proportionate to the aim of NDAS to develop a data analytics capability for use by UK law enforcement which will support officer decision-making to prevent and detect serious crime and create efficiencies. Without the use of the personal data then this would not be possible because personal data forms the basis of data used to form insights based on the use case.

All the personal data used is currently held by Police Forces or LEA for a lawful policing purpose and will already be processed by the owning Police Force by conventional policing methods for the prevention and detection of crime. NDAS will seek to make this processing more efficient by the use of data science which is suitable for the desired outcome.

The data subjects will not be disadvantaged as the data is still be used for the policing purpose it was acquired.

The data will be processed lawfully, fairly and in a transparent manner in relation to the data subject and not used for any other purpose.

Section 3 – Lawful Basis

3.1 Lawful Basis

To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Necessary for a law enforcement purpose

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes): **N/A**

Choose an item.

3.2 Further Special Category Lawful Basis

If processing special category data (section 2.3) you must have identified a further lawful condition

Operational Data:

The processing is strictly necessary (please tick to confirm)



OFFICIAL-SENSITIVE
(When complete)

AND

One of the following conditions applies (select from the list):

Statutory Purpose

Administrative Data: N/A

It is necessary for one of the following conditions (select from the list):

Choose an item.

OR

It is in the substantial public interest (tick to confirm)

AND for the following purpose:

Choose an item.

Section 4 – Review, Retention and Disposal

4.1 Does the proposal have a review, retention and disposal process that complies with WMP Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within the WMP IM document suite.

Yes

No



OFFICIAL-SENSITIVE

(When complete)

Section 5 – ICO: Additional Factors

The Information Commissioner’s Office have published a number of factors that present a ‘high risk’ when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.

Does the processing involve:		Please check either Yes or No	If ‘Yes’ then please provide further details
5.1	<p>Systematic, extensive and large scale profiling and automated decision-making about people? <i>"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"</i></p> <p>Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual’s performance.</p> <p>Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<p>NDAS will be processing personal data to identify specific outcomes based on specific use cases. This processing will be performing a number of data analysis techniques to provide respective outcomes that can be used by a small number of trained Police Officers and Police Staff to assist them in their roles.</p> <p>It’s important to understand that this processing will not replace any existing procedures. Officers and Staff will always make the final decision based upon their own assessment, meaning there will be no automated decision making.</p>
5.2	<p>Large scale use of special category data or criminal offence data? <i>"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"</i></p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<p>NDAS will be processing criminal offence data due to the nature of the chosen use cases, as well as a small segment on Special Category data.</p> <p>Please see Sections 2.2 and 2.3 for confirmation of datasets to be processed.</p>
5.3	<p>Public monitoring?</p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	



OFFICIAL-SENSITIVE

(When complete)

	<i>"Systematic monitoring of a publicly accessible area on a large scale"</i>		
5.4	<p>New technologies or techniques? <i>"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"</i></p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<p>The processing performed by NDAS involves the novel application advanced analytical techniques to Police Force and LEA datasets, to derive insights.</p> <p>As per 5.1 above, it is important to understand that this processing will not replace any existing procedures within the Force. Force Officers and Staff will always make the final decision based upon their own assessment, meaning there will be no automated decision making.</p>
5.5	<p>Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? <i>"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"</i></p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
5.6	<p>Biometrics/genetic data? <i>"Any processing of biometric data" and/or "any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject" Biometric data can include Facial Recognition technology, fingerprints and is defined as</i></p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
5.7	<p>Data matching? <i>"Combining, comparing or matching personal data obtained from multiple sources"</i></p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Data matching could take place across data sets to assist with analysis, and provide more informed insight
5.8	<p>Invisible processing? <i>"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove</i></p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	As per 5.1 and 5.2 crime data is to be processed, and it is understood that elements of those datasets may have been collected through means which



OFFICIAL-SENSITIVE

(When complete)

	<p><i>impossible or involve disproportionate effort"</i></p> <p>For example, when gathering data, without the knowledge of the data subject, in the course of a Police investigation.</p>		<p>the Data Subject was not privy too. This would still be in line with normal Policing investigative procedures.</p>
5.9	<p>Tracking? <i>"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"</i></p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
5.10	<p>Targeting of children or other vulnerable individuals? <i>"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children"</i></p> <p>For example, the use of personal data relating to children for the purposes of marketing their online safety products.</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<p>Children and/or vulnerable individual's datasets are not specifically being "targeted" however it is accepted that due to use cases of NDAS that there will be data processed respective to children and/or vulnerable individuals.</p>
5.11	<p>Risk of physical harm? <i>"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals"</i></p> <p>For example, if data relating to CSAE, HUMINT or protected persons data was compromised then it could jeopardise the safety of individuals.</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<p>In theory yes there is risk of physical harm, however this is extremely low probability and could only occur in the event of a very sophisticated data breach. That said, with the controls in place the breach would have to bypass controls and measures in place by both █████ and █████, as well as being able to decrypt the datasets to which West Midlands Police will ultimately hold the encryption keys. There are a lot of variables in place to which each and everyone one them would have to be impacted to get anywhere near the raw data itself.</p> <p>NDAS has added security measure to ensure that any data which is deemed sensitive and may hold a risk if a breach</p>



OFFICIAL-SENSITIVE

(When complete)

			occurred is not being processed and will not be ingested.
5.12	<p>Evaluation or scoring? <i>"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of a recruitment process.</i></p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
5.13	<p>Data processed on a large scale. <i>Considerations include:</i></p> <ul style="list-style-type: none"> • <i>The number of data subjects concerned</i> • <i>Volume of data and/or range of data items</i> • <i>Duration, or permanence, of the data processing</i> • <i>Geographical extent of data processing</i> 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Please see 5.1
5.14	<p>Preventing data subjects from exercising a right? <i>The rights are:</i></p> <ul style="list-style-type: none"> • <i>The right to be informed</i> • <i>The right to access data</i> • <i>The right to rectification</i> • <i>The right to erasure</i> • <i>The right to restrict processing</i> • <i>The right to object</i> • <i>The right to portability</i> • <i>Rights relating to automated processing</i> 	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

Please forward the completed form the WMP DPO.