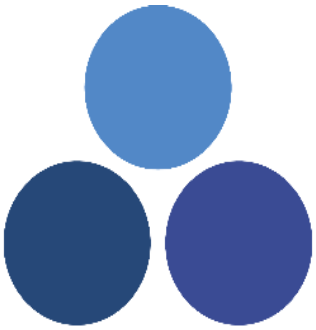
Home Office

NPCC National Police Chiefs' Council



National ANPR Service

Data Protection Impact Assessment (DPIA)

Version 3.1
February 2024

This publication is available at www.gov.uk/government/publications Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk.

Contents

The need for a DPIA

The National ANPR Service (NAS) is operated by police forces and other Law Enforcement Agencies (LEA) the chief officers of which are Joint Controllers within the meaning of Section 58 Data Protection Act 2018. The lead controller Chief Constable Hall is accountable for completion of the DPIA.

A Privacy Impact Assessment (PIA) was completed in 2013 and has remained under review since that time.

This DPIA was published in January 2020 to ensure that all data protection risks have been identified and to review the status of the National ANPR Service (NAS) in the context of recent legislation. The DPIA is now subject review which will be reflected in a revised document, (Version 3.0 May 2022) which has been further reviewed in February 2024.

The DPIA applies to England, Wales, Scotland and Northern Ireland.

The aim of the NAS DPIA is to:

1) Ensure a national data collection system is in place and complies with all relevant legislation.
2) In compliance with the Data Protection Act 2018 a DPIA is required to determine whether Automatic Number Plate Recognition (ANPR) processing is likely to be 'high risk to rights and freedoms of individuals.'
3) Ensure consistency and support throughout the police service in how ANPR data is captured, used, stored and deleted.
4) Ensure consistency and support throughout Law Enforcement Agencies (LEAs).
5) Ensure compliance with Data Protection Act (DPA) 2018 (Part 3).
6) Ensure compliance with Human Rights Act 1998.
7) Take account of European Convention on Human Rights (ECHR)
8) Follow Information Commissioners Office (ICO) guidance.
9) Ensure compliance with relevant parts of the Surveillance Camera Code of Practice. issued under provisions of the Protection of Freedoms Act 2012 taking account that this Code may cease to be applicable on implementation of the Data Protection and Digital Information (No 2) Bill 2023. However, for the purposes of this assessment the principles detailed within the Code are considered to be relevant.
10) The principles of data protection by design have been considered in the design and implementation of the NAS

At present over 18000 ANPR cameras nationally, submit on average over 80 million ANPR ‘read’ records to national ANPR systems daily. ANPR data from each police force is stored together with similar data from other forces for a period of one year.

It is recognised that the NAS is possibly the largest vehicle surveillance system of its type in the world and that it is essential for the police and LEAs to ensure that the collection and use of data is and remains necessary and proportionate for law enforcement purposes.

It is evident that a number of aspects of NAS have the potential to result in high risk to the rights and freedoms of individuals including the large scale of data collection and volume of data stored that has the potential to support systematic monitoring and tracking of individuals.

A detailed assessment is within Step 4 of this document. The risks and mitigations are detailed within steps 5 and 6. All ‘high level risks’ are appropriately mitigated and therefore this DPIA is not required to be submitted to the Information Commissioner for prior consultation (DPA Section 65).

The nature of the processing

Introduction

This DPIA concerns the National ANPR Service (NAS) which is the national system used by the police and other law enforcement agencies (LEA) for law enforcement purposes as defined by Part 3 Data Protection Act 2018. **This DPIA does not relate to consideration of the deployment of ANPR cameras**; it is a requirement that any police force or LEA deploys cameras only in accordance with National ANPR Standards for Policing and Law Enforcement (NASPLE) and are responsible for completion of a DPIA for that deployment. The only read data that enters NAS is that submitted from a police force or LEA the chief officer of which is a joint controller for NAS.

Automatic Number Plate Recognition (ANPR) technology is used by the police and other LEAs, to help detect, deter and disrupt criminality at a local, force, regional and national level, including tackling travelling criminals, Organised Crime Groups and terrorists. ANPR provides lines of enquiry and evidence in the investigation of crime and road traffic offences throughout England, Wales, Scotland and Northern Ireland.

ANPR is also used by private companies and public authorities for a range of purposes including car park management and clean air zones. The use for these purposes by organisations is not part of the NAS and is also not relevant to this DPIA. They manage the cameras and process the data independent of the NAS and therefore this aspect of widespread ANPR use is out of scope of this assessment.

How it works

As a vehicle passes an ANPR camera, its registration number is read and instantly checked against database records of vehicles of interest. Police officers can intercept and stop a vehicle, check it for evidence and, where necessary, make arrests. A record for all vehicles passing by a camera is stored, including those for vehicles that are not known to be of interest at the time of the read that may in appropriate circumstances be accessed for investigative purposes. The use of ANPR in this way has proved to be important in the detection of many offences, including locating stolen vehicles, tackling uninsured vehicle use and solving cases of terrorism, major and organised crime. It also allows officers' attention to be drawn to offending vehicles whilst allowing law abiding drivers to go about their business unhindered.

The NAS is not used for speed enforcement or traffic management and whilst in some cases ANPR cameras submitting data to the NAS may be co located with other cameras the use is separate from other camera used on the national road networks.

The NAS supports policing and LEAs in three key aspects:

- **Operational Response** – A vehicle known to be of interest may be circulated on a list of vehicles of interest (VOI) such that when it passes by an ANPR camera an 'alert' is created and resources may be deployed to stop the vehicle and deal appropriately with the reason for including the vehicle on the VOI list

- **Supporting Investigations** - Searches of ANPR data can confirm whether vehicles associated with a known criminal has been in the area at the time of a crime and can dramatically speed up investigations. Detailed provisions for use for defined law enforcement purposes are within NASPLE Annex C which includes use for investigations at three levels Major Investigations, Serious and Complex Investigations and Priority and Volume investigations which includes traffic offences.

- **Intelligence development** – Research of data stored within NAS can be of significant benefit in supporting assessment of information and intelligence reports particularly for organised crime investigations that may reduce the need for more intrusive surveillance activity and reduce costs.

National ANPR Standards for Policing and Law Enforcement (NASPLE) and National Compliance and Audit Standards for Law Enforcement ANPR (Audit Standards) provide clear rules to control access to ANPR data to ensure that access is for legitimate investigation purposes. Members of staff only have access to ANPR data if it is relevant to their role and the majority of those who have permission may only do so for a maximum period of 90 days from the date it was collected. Some staff are able to access data for up to a year subject to appropriate authorisation. The NASPLE includes detailed criteria for access and controls which provides including the disclosure of data. Personal data is only accessed by staff within police forces and LEAs that are competent authorities within the meaning of Part DPA and subject to the requirements of NASPLE.

It is recognised that the collection and use of personal data has to be lawful and proportionate. This DPIA is used by the Joint controllers to enable this as well as informing the ANPR Standards. Any access to the searching the data collected in the NAS is proportionate to the gravity of the offences being investigated.

The NAS consists of the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, that are the responsibility of police forces, and other LEAs that connect to a single national system. This provides the functionality to enable use by LEAs for operational response, investigation and intelligence purposes and provides for a single national store of data.

The National Police Chiefs' Council (NPCC) ANPR lead, is the lead controller for the purposes of the Data Protection Act 2018 (DPA). Controller responsibilities are set out in the Joint Controller Arrangements (JCA)

The roles and responsibilities for NAS arise in the following circumstances: Police, other LEAs and the Home Office, as a result of the operational use of ANPR by the Border Force and Immigration Enforcement, are joint controllers as defined by the DPA in respect of their operational use and their organisation's management responsibilities in respect of NAS.

The Home Office as a joint controller provides advice and supports the other controllers in respect of policy, management of NAS including procurement of ANPR services, and the management of processors.

How is data collected?

There are many types of ANPR camera from which data can be collected stored within NAS

Source of data is fully detailed in NASPLE Part 2 and includes:

- Static ANPR
- Moveable ANPR
- Multi- Lane ANPR
- CCTV integrated ANPR
- Mobile ANPR
- Covert Systems ANPR

The decisions regarding deployment and installation of cameras are the responsibility of the controller for the police force or LEA that deploys that resource. The standards, NASPLE set out clear criteria for infrastructure development that are supported by clear guidance documents to aid consistency in decisions on deployment. Controllers deploying cameras are accountable for completion of any DPIA for that deployment and as such are outside the scope of this document.

How is data stored?

Storage locations are within NAS and configured to allow primary and secondary capability. All ANPR data is Official – Sensitive. Data stored within NAS is retained for a period of 12 months unless preserved under the provisions of Criminal Procedure and Investigations Act 1996 (CPIA)[1] and equivalent provisions in Scotland. Unless preserved, data is automatically deleted. In accordance with NASPLE data may be held locally for a maximum of 7 days.

In addition, a copy of read data is held locally by the LEA that originally collects the data for a maximum of 7 days from initial capture. If data is received at the Management Server (MS) more than 7 days after being 'read' by a camera, it may be retained for a maximum of 24 hours after being received at the MS and then deleted.

The core NAS functionality does not provide for more advanced analytical requirements to combat terrorism and the most serious crime. The specifications and delivery method for that more advanced capability is to be determined and will be subject to specific DPIA process. In the interim provision has been made for continued use of the legacy National

[1] The CPIA requires investigators to secure relevant material in the context of investigation to ensure it is preserved for a period of time that is determined by reference to the nature of the offence and judicial outcomes.

ANPR Data Centre (NADC) and a separate DPIA has been conducted in relation to the continued use of that capability. The use of NADC is also subject to the provisions of NASPLE.

How is data used?

Data will be used in the interests of:

1. National security and counter terrorism

2. Law enforcement
   - The prevention and detection of crime
   - The apprehension and prosecution of offenders
   - Enforcement of the collection of any tax or duty by police and other agencies - such as DVLA as a tool of last resort when other procedures have failed and not for routine administrative compliance activities.

3. General processing
   - In circumstances of significant public interest and purposes of public safety (for example vulnerable and missing persons)

Who has access to the data?

Approved organisations (Appendix A) which include police forces and some other LEAs have access to the NAS subject to compliance with all the standards within NASPLE. The NASPLE provide for access by staff within approved organisations as necessary and proportionate to their role and subject to any required authorisation taking account of the reason for access and the time that has elapsed since the data entered the NAS. Unless specific criteria as detailed in NASPLE arise data may only be accessed for 'Priority and Volume Investigations' for a period of up to 90 days following entry into the NAS.

The Intelligence Services (IS) will be permitted to make enquiries of the NAS and receive disclosure of information relevant to those enquiries from the NAS, subject to written agreement that in processing data under Part 4 DPA they will comply fully with the requirements of NASPLE.

Who will share the data?

Data may be accessed under Part 3 DPA competent authorities, including approved LEAs (see appendix 1 list) in accordance with the provisions within NASPLE and in addition may include Criminal Justice Systems for law enforcement purposes. Data may be disclosed on application under Schedule 2 (2) DPA or Article 6 of General Data Protection Regulations

(GDPR) or relevant sections of 'UK GDPR' following Brexit . The NASPLE set out clear requirements for access to and the disclosure of data that establish clear safeguards for NAS data. In particular NASPLE includes a requirement that *"*data held within or obtained from the NAS may not be used or disclosed for any purposes except those as authorised within NASPLE*".* Audit Standards are also in place to support compliance.

Are data processors used?

Yes, the following are Data Processors:

Third Party suppliers are processors of the software application and data storage. The processors are responsible for the software application that provides the functionality within NAS and for storage of data. They do not process the data within the system, that processing is carried out by the staff of police and forces and LEA that are authorised to access the NAS and are accountable to their chief officer who is a joint controller.

The current suppliers of the software application are Leonardo MW Ltd and data storage is provided by Redcentric plc. Data storage provisions are not impacted at the time of this DPIA however the position remains under review and a DPIA will be completed to ensure continued appropriate data storage provisions.

What are the retention periods?

Data held on local systems must be deleted within 24 hours after the period 7 days following the time of the read. Data held on mobile ANPR will be transferred within 48 hours from the time of capture. Data may be retained within NAS for 12 months unless provisions of CPIA apply when it may then be preserved for a longer period. The period for retention of read data remains under review to ensure that it remains appropriate and is proportionate.

Vehicle of Interest (VoI) data retention:

The standards within NASPLE require that lists of VoIs are:

a) Kept up to date

b) Deleted when no longer required

c) Auto-deleted after 28 days following the last date of revision.

How will data be deleted?

Requirements for retention and deletion are contained within NASPLE.

Unless preserved, data will be automatically deleted 12 months after initial capture. Data held within local management servers will be deleted after 7 days, unless it is retained following CPIA assessment.

NAS authorised staff are required to amend incorrect records or delete records at the time they are found to be incorrect.

The software application includes the functionality for the automatic deletion of data once prescribed time limits are reached, and processors are required to ensure that this functionality is always in operation.

NASPLE Part 3 makes the following provision:

Where an LEA has established links between the NAS and other computer based systems, for the purposes of monitoring, and the initiation of an operational response to any hit against a list of VoI's or for more advanced research and analysis purposes, in relation to an investigation, the ANPR data must be deleted from those systems within 7 days of entry into those systems of that data. The exceptions are:

a) A review has been conducted of the data that it is proposed to retain which has identified the items of data where a continued policing purpose remains that can only be satisfied by processing of the data within a system external to the NAS. In this case provisions of Management of Police Information (MOPI or similar provisions in Scotland) apply and the relevant items of data may be retained and managed in accordance with those provisions; or

b) A review has been conducted of the data that it is proposed to retain which has confirmed that the items of data are relevant to an investigation. In this case the relevant items of data may be retained, managed and deleted in accordance with the requirements of CPIA.

Data may not be transferred to local systems to facilitate basic user access to ANPR data.

What security measures are in place?

All LEAs that connect to, or have access to, the NAS must have an up to date written policy in place as required by NASPLE and data protection legislation in respect of the access, management and use of ANPR data, including provisions for audit consistent with the Audit and Compliance Standards.

The NAS is hosted in secure data centres with appropriate physical security. The security operating procedures are in place and the NAS is subject to regular accreditation and review. Police forces and LEAs connecting to the NAS are required to comply with detailed security requirements that are overseen by a national accreditor. These include provisions for all aspects of security both physical and technical.

The NAS is protected by technical security controls. Access to NAS is restricted through technical measures such that attempts to access from unauthorised networks are rejected.

Data being transferred to or from the NAS is protected through appropriate cryptographic controls to protect and encrypt data in transit.

The NAS has a range of protective monitoring capabilities to detect and respond to suspicious activity, together with regular security testing and vulnerability management. This ensures that security measures remain appropriate through the life of the system.

Password requirements for access to the NAS are based on National Cyber Security Centre guidelines and is applicable to all roles within LEA, third party contractors and suppliers and staff responsible for NAS management.

Access to ANPR data is restricted through user accounts with Role Based Access Control. This ensures that access is proportionate in relation to the circumstances and taking account of the impact on the fundamental rights and freedoms of individuals.

Staff who are approved to access the NAS as both a user and for administrative purposes must be allocated separate accounts such that these functions cannot be achieved using a single log in account.

Accounts must be suspended or terminated in the following circumstances:

a) Account suspended if not accessed for a period of 90 days, and the need for access reviewed within the subsequent 7 days; the account then reactivated or deleted as appropriate.

b) Account terminated within a maximum of 48 hours of a person leaving an LEA or partner agency. This managed locally by police forces and LEA.

c) Suspicious activity is detected on the account.

Accounts must be reviewed, suspended or terminated if any of the following circumstances apply:

d) Access permissions reviewed within 7 days of a person changing role within the LEA.

e) Suspended if not accessed for a period of 90 days, and the need for access reviewed within the subsequent 7 days. The account then reactivated or deleted as appropriate. Terminated within a maximum of 48 hours of a person leaving an LEA or partner agency.

LEAs have responsibility to ensure individual user privileges are consistent with those necessary for their role and required vetting standards for them to be granted access.

Audit trails and records are maintained which includes successful and failed searches. Users to provide reasons for their access to NAS on each occasion that they initiate an enquiry.

All components of NAS are United Kingdom based. NASPLE Part 2 sets out the requirements for accreditation for police systems. The national accreditor for policing systems sets out the requirements for physical features of all aspects of NAS as provided by third party supplier and data processors and within LEAs.

Are any new technologies in use?

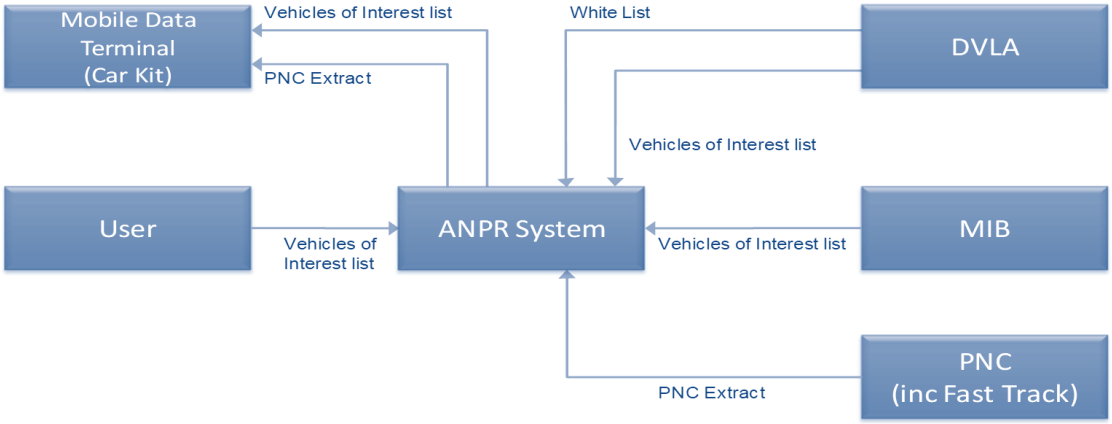
The ANPR does not currently use new technologies, the configurations bring together local systems into a single national service which provides significant benefits in improved data

management and reduced potential for misuse of data. Developments in technology will remain under review and a DPIA will completed as appropriate.

There are no types of novel processing to be considered or used. No screening criteria is flagged as high risk.

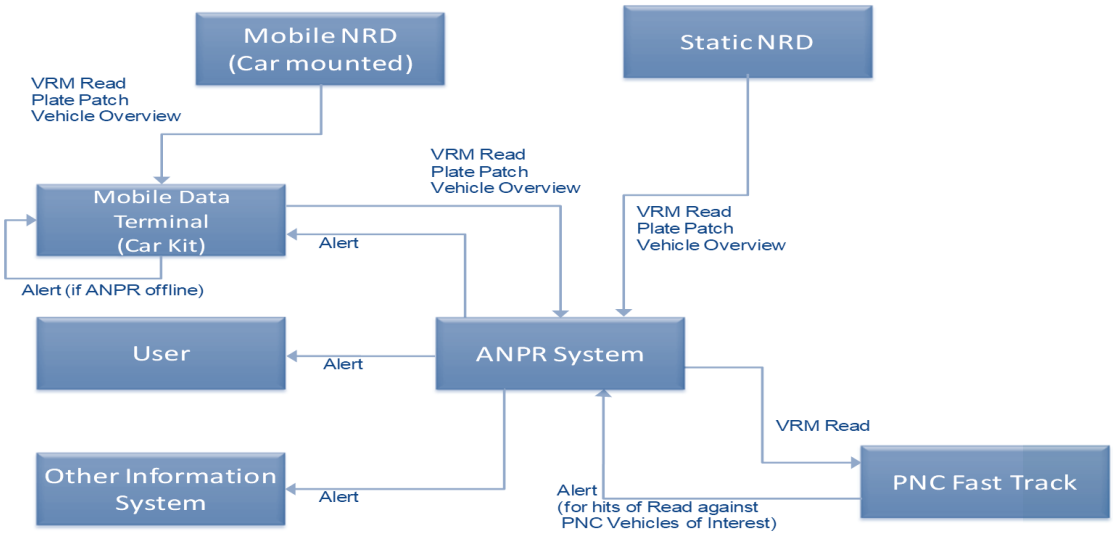
The following diagram shows how:

1. Reference data flows around the system.



The following diagram shows how:

1. Read data is captured and moved around the system.
2. Information objects associated to a hit of a read against a list of vehicles of interest are moved around the system.



The scope of the processing

What is the nature of the data?

The deployment of ANPR cameras enabling the collection of vehicle registration marks (VRM) an associated plate patch, an overview image and associated data detailing the time and location for that read.
A plate patch is an image of the number plate on its own and an overview is an image of the front or rear of the vehicle including the plate. The purpose of images is to assist confirmation of the accuracy of the ANPR read both in terms of the numbers and being displayed on the correct vehicle. The images may show occupants of the vehicles, however the configuration of ANPR cameras is optimized for number plate reading and as a result the quality of images of persons is significantly reduced.
This is retained for 12 months.
An image will generally provide an overview of the front of the vehicle in most cases. Therefore, it is recognised that on occasion images of persons are captured. Safeguarding is considered prior to any cameras being installed and agreed within each individual location.
In addition, Vehicle of Interest (VOI) lists held on NAS may contain personal data relating to persons of interest associated with the vehicle which in some cases may involve sensitive processing.

What is the volume and variety of the data?

ANPR read data recording the VRM and associated images does not include any sensitive or criminal offence data. The lists of VoI's within the NAS may include criminal offence data and sensitive processing.
Each camera records details of a VRM for the location of that camera, and the volume of data collected is variable due to changing traffic flows at that location, however it will be integrated into the NAS where it will be stored with reads from other cameras throughout the United Kingdom.
The volume of reads submitted to the NAS overall can exceed 80 million per day.

What might be the sensitivity of the personal data?

ANPR read data is personal data as defined by the DPA. An overview image of the front of the vehicle is obtained in most cases to support verification of read accuracy which may show the occupants of the vehicle. However, identity of individuals can only be ascertained by reference to secondary data sources.

Vehicle of interest lists may include personal data and, in some cases, sensitive personal data where the information by necessity either directly or indirectly may for example indicate ethnicity, issues of health or political views.

What is the extent and frequency of the processing?

ANPR systems operate at all times across a national infrastructure and processing is therefore continual.
The network of cameras across the United Kingdom are all individually subject to an assessment of the proportionality of their deployment which includes risk assessment.
National Standards include detailed requirements to support a consistent approach to the development of ANPR Infrastructure with oversight by a National Camera Strategy group reporting to the NPCC ANPR lead.
Captured data includes the registration plate, time and location and in most cases an overview image.

What is the duration of the processing?

Duration is continual unless there are exceptions as detailed within NASPLE. The data is retained for 12 months. Continual management is required for VoI lists.
Information extracted will be by Management of Police Information CPIA.
Data untitled in respect of investigation will be subject to CPIA legislation.

What is the number of data subjects involved?

Exact numbers cannot be provided. It is likely due to volume of cameras that all vehicle road users will be involved. At the time of this DPIA readings are in excess of 80 million per day. The system is vehicle based and focused on road users and so otherwise does not discriminate on any section of society.

What is the geographical area covered?

ANPR is deployed throughout the United Kingdom.

The context of the processing

Data is shared by LEAs subject to the provisions of NASPLE Part 3 Data Access and Management Standards.

Infrastructure Development

Following implementation of the NAS the camera infrastructure will be reviewed to:

- Ensure that current deployments are consistent between LEAs.
- Identify any potential duplication of capability arising as a consequence of integrating local systems into a single national system, with proposals for mitigation.
- Identify any gaps in infrastructure provision that may be mitigated by deployment of additional ANPR capability.
- Ensure that support to the consistent development of infrastructure will be established. All camera deployments are subject to a separate DPIA process.
- Identify opportunities for collaboration between LEAs and with other public and private sector operators of ANPR which will be explored to reduce the overall number of cameras that are deployed. This is to reduce the costs of establishing ANPR infrastructure at locations where it is necessary and proportionate to do so. This will contribute to efficiency and take account of privacy concerns by reducing the number of cameras that are deployed at a location.

What is the source of the data?

ANPR cameras are deployed throughout the United Kingdom. The location of cameras is determined in accordance with NASPLE Part 2. Where a vehicle becomes of interest to an LEA for investigation for operational response purpose it may be included in a list of VoI to enable the movements of that vehicle to be identified by ANPR systems.

What is the relationship with the individuals?

Data relating to an individual can only be obtained by reference to another data source. Individuals have no control of the collection of data from a location. The data collected may be linked to the registered keeper of a vehicle or to persons linked with a vehicle in other data storage systems. Whilst registered keeper data will not include persons under 16 years, it is possible that other data systems may include links to persons of any age and vulnerable groups.

The JCA make provision for the consistent management of requests by data subjects in relation to their rights under the DPA and for the provision of consistent information to data subjects by all controllers who are parties to the JCA.

What is the extent that individuals have control over their data?

Individuals have no control but may request access under provisions of the DPA.
The concerns by some members of the public and civil liberty groups in relation to the potential impact on privacy are recognised and acknowledged and these concerns have resulted in the development of the national retention standards that are embedded within NASPLE. This DPIA has taken into account those privacy views to ensure the collection and use of ANPR is proportionate and lawful.

The LEA conforms fully to the requirements of NASPLE which provides for significant safeguards to the granting of user permissions for access with clear criteria to support proportionate access to the data. Provisions for logging and audit are established.

The extent to which individuals are likely to expect the processing?

Information is available on public websites both nationally and those for police forces and LEAs, who also make use of social media to provide information of ANPR use and there is previous experience of this type of processing documented. In some areas there are a road signs and signage on police vehicles.

Any relevant advances in technology or security?

No, although there has been natural progression within configuration of the NAS as a system providing significant improvements.

This is in comparison with previous combination of local ANPR systems and the National ANPR Data Centre (NADC) particularly in relation to user permission, access and management, system security, log in and audit.

Any current issues of public concern?

It is recognised the extent of the UK network is a privacy concern and the scale of that network is likely to remain so for some sections of the community. Some have been

addressed and there should be continued and on-going engagement with civil society and relevant groups as a key priority.

The NPCC ANPR lead has established an Independent Advisory Group (IAG) chaired by the Surveillance Camera Commissioner (SCC), with a broad representation from civil society and other interest groups to ensure appropriate awareness of issues of concern. The office for the Biometrics Commissioner and the Surveillance Camera and Biometrics Commissioner is to be disbanded on implementation of the Data Protection and Digital Information (No2) Bill 2023 and arrangements for a replacement chair of the ANPR IAG are being progressed.

The purpose of the processing

The purpose is to support the response by LEAs in respect of:

1. Law enforcement purposes
   - The prevention, investigation, detection or prosecution of criminal offences
   - The prosecution of criminal offences or the execution of criminal offences
   - The prevention of threats to public security

Whilst NAS is a system operated within the scope of Part 3 DPA some policing purposes may require use under GDPR provisions, or similar provisions within the replacement 'UK GDPR'.

2. General Processing
   - In circumstances of significant public interest and the purposes of public safety (for example vulnerable and missing persons.)

Processing identified as a potential high data protection risk is the collection and use of records for vehicles passing through ANPR cameras. The data collected provides a record of the location of a vehicle at a specific time and when compared with other data has the potential to reveal personal data in relation to persons associated with that vehicle. The integration of that data into a national collection of data presents a capability to establish the movements of a vehicle through the network of ANPR cameras over a given period, and to reveal associations between individuals through analysis of that data.
As a vehicle passes an ANPR camera, its registration number is read and instantly checked against database records of vehicles of interest. Police officers can intercept and stop a vehicle, check it for evidence and, where necessary, make arrests.
A record for all vehicles passing by a camera is stored, including those for vehicles that are not known to be of interest at the time of the read that may in appropriate circumstances be accessed for investigative purposes by approved LEAs.

The intended outcome for individuals.

Improved performance by LEAs and through the use of VoI lists reducing the likelihood of law abiding citizens being stopped.
Improved performance will be reflected in areas such as road safety, improved management of data, reduction in data duplication, reduction in crime and investigation, as a preventative to reduce crime and keep people safe.

The expected benefits for a society as a whole.

Improvement in relation to all the above purposes. Information detailing benefits is collected within a value model and it is intended that information from that source will be published as appropriate.

Consultation process

The following have been consulted throughout the development of NAS.

- Audit professionals with police service
- Data Storage Company
- Data Protection Specialists
- Home Office
- Independent Advisory Group (IAG) chaired by Surveillance Camera and Biometrics Commissioner
- Information Commissioner's Office (ICO)
- LEAs
- NPCC ANPR lead
- NAS Programme team
- National Accreditor for police systems
- National police Information Risk Management Team (NPIRMT)
- Software supplier company
- Surveillance Camera and Biometrics Commissioner (SCBC)
- As an addition published information from national privacy groups has been considered.

We have communicated and sought advice of both the ICO and SCBC in relation to the NAS and this DPIA All relevant parties have been involved. No further assistance required from processors.

Consulting information security experts, or any other experts?

Already consulted- specific aspects have been consulted on and all the following areas considered:
Data Retention, Data Management, Identity and Access Management, and Auditing.
There continues to be on going dialogues through NAS working groups.

Standard Operating Procedures (SOPs) will be confirmed to provide the rules by which NAS must be operated. They will specify to all personnel involved in NAS operations, their individual roles and responsibilities. The SOPs are designed to assist in the efficient operation of NAS and provide for access according to the role of the authorised person.

Consultation that is relevant to this development

There are recorded details of the consultation process and outcomes. It is agreed no further groups need consulting.
There is a continuous and regular consultation process both internal and external with all stakeholders and regulators - LEAs, Data Protection Office, specialist ANPR and Independent Advisory Group (IAG.)
Recorded, documented and escalated with NPCC ANPR lead as lead controller.

Assessment of necessity and proportionality – compliance and proportionality measures

What is the lawful basis for processing?

When consulted, the lawful basis for processing ANPR data has been highlighted by the IAG as an area of specific interest taking account of the large numbers of 'reads' collected and the period that data is retained.

The extensive use of ANPR by the police and LEAs enables observation of vehicle movements to be undertaken quickly efficiently and extensively and in reality, could not be achieved by human observation in the absence of technology. The High Court have recently considered the lawfulness of police use of automatic facial recognition (AFR) technology in the case R (Bridges) v CCSWP and SSHD and the legal principles relevant to that case are considered in the context of the NAS. Any future decisions of the courts in that regard will be kept under review and considered in relation to the NAS.

The NAS is operated for the 'Law enforcement purposes' as defined by S31 DPA and is subject to the provisions of Part 3 of that Act. The NAS is compliant with S35(2)(b) DPA in that processing within NAS is carried out for those purposes by competent authorities, as necessary for the performance of a task. Sensitive processing is only undertaken when strictly necessary in accordance with S35(5) DPA. The joint controllers for NAS are the chief officers of police forces and LEA that are competent authorities within the meaning of Schedule 7 DPA.

It is evident that consideration of Article 8 ECHR is necessary since it has been proposed that the collection of vehicle movement data may impact on that right.

Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The court in the Bridges case observed that when using technology, it is necessary to pause for thought because of its potential to impact upon privacy rights, and cited with approval the Grand Chamber of the Strasbourg Court said in S v. United Kingdom (2009) 48 EHRR 50 at [112]:

[T]he protection afforded by art.8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests … any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.

From examination of the jurisprudence for Article 8 rights it is apparent that the use of ANPR by the police and LEAs to monitor vehicles and to compare vehicle registration marks with lists of vehicles of interest may interfere with those rights.

Registration plate details is not private information in itself. Whilst a registration mark is personal data within the meaning of the DPA since it can be linked to a person, that link does not in itself impact on private life, and even if linked to a particular vehicle and thereby to a particular individual in live time, is simply a hazard of driving a car on the roads. A registration number plate is a deliberately overtly displayed marker which can be seen and is intended to be seen. Every person who drives a car voluntarily accepts that they are likely to be capable of being linked to a particular vehicle. In general, road users have no reasonable expectation of privacy in relation to ANPR being able to determine their presence on the road. Both the Strasbourg Court (in PG v United Kingdom (2008) 46 EHRR 51) and the Supreme Court (in Kinloch v HM Advocate [2013] 2 WLR 141) have expressly accepted that CCTV in public places is a part of everyday life and that the use of CCTV does not of itself give rise to private life considerations. These decisions have relevance to ANPR in that regard and the standards and controls that are required for compliance with NASPLE provide robust governance to support compliance.

The deployment of ANPR cameras for the purpose of monitoring the VRM of vehicles passing through the field of view and comparing them against a list of VOI are unlikely to interfere with Article 8 rights, however the storing and any analysis of those VRM is likely to do so even though the information is publicly available.

Article 8 rights are not absolute rights and any interference with Article 8 rights must therefore be in accordance with the law.

The following elements of common law powers were referenced in the ‘Bridges’ case where the court concluded that the extent of the police’s common law powers has generally been expressed in very broad terms.

The police have a common law duty to prevent and detect crime. In R (Catt) v Association of Chief Police Officers [2015] AC 1065, the Supreme Court considered the lawfulness of collecting and retaining personal information. Lord Sumption JSC held that “At common law the police have the power to obtain and store information for policing purposes, i.e. broadly speaking for the maintenance of public order and the prevention and detection of crime” and in Lord Parker CJ said in Rice v Connolly [1966] 2 QB 414 at 419 B - C:

“[I]t is part of the obligations and duties of a police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal damage. There is no exhaustive definition of the powers and obligations of

the police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice.

The common law provides a sound basis for the use of ANPR however that may be insufficient to meet the Article 8 (2) requirement that interference is in 'accordance with the law'. The courts have confirmed that the principles applicable in this regard are:

a) Here must be some basis in domestic law, and,

b) It must comply with the legal basis must be "accessible" in that it is published and comprehensible and "foreseeable" such that a person can be aware of the consequences of ANPR use.

The legal framework in which the NAS operates comprises of three elements in addition to the Common Law, namely:

a) Primary Legislation – The Data Protection Act 2018 (DPA)

b) Secondary Legislative Instruments – The Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (SCC Code)

c) National Standards and Policy –NASPLE and National Standards for Compliance and Audit of Law Enforcement ANPR (Audit Standards)

Primary Legislation

It is essential to be able to demonstrate compliance with the 6 DPA Data Protection Principles as follows:

Principle 1 – Processing must be lawful and fair

Principle 2 – the purposes must be specified, explicit and legitimate

Principle 3 – the data must be adequate, relevant and not excessive for the purpose for which it is processed

Principle 4 – data must be accurate and kept up to date; inaccurate data should be corrected or erased

Principle 5 – data should be kept for no longer than necessary

Principle 6 – data should be processed in a secure manner.

S29(6) and 33 of the Protection of Freedoms Act 2012 are also relevant.

In addition, the DPA includes a relevant safeguarding measure in that the controller must have an appropriate policy document. In respect of the NAS this is the NASPLE.

The standards detailed within NASPLE set out a comprehensive framework to meet the requirements of the DPA. All police forces and LEA in accessing NAS will ensure the capability to meet those standards. A national audit capability has been established that will oversee local provisions for audit and monitor compliance. The Joint Controller Agreement (JCA) also includes measures to support consistent compliance and the management of subject rights.

Additionally, support to Principle 3 is provided by a 'National ANPR Strategy Group' that provides further oversight of the development and review of infrastructure and has published guidance to aid consistent decision making by the police and LEAs in installation, review and decommissioning of cameras. This is also an area of interest monitored by the IAG.

Principle 5 requires ongoing monitoring and review. At present data is retained for 12 months before deletion unless retained under provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) or following assessment is retained for a continued policing purpose in accordance with the Management of Police Information (MOPI) Code.

It is known that many ANPR reads enter the NAS and are not then subsequently accessed for any purpose until they are automatically deleted after 12 months. The NASPLE provisions provide for users to only be able to access the data as necessary for their role and therefore provide safeguards reducing the risk of inappropriate access to the data, however the retention of data for 12 months requires further consideration to either justify that period or establish an alternative evidence-based retention period to satisfactorily demonstrate compliance with Principle 5.

Secondary Legislative Instruments

The Surveillance Camera Code comprises 12 "guiding principles". These principles concern when and where surveillance cameras should be used; the information to be provided to members of the public when surveillance cameras are used; the extent to which information obtained from surveillance cameras should be retained; the circumstances in which access to such information should be permitted, or use should be made of the information; and the technical standards to be required of any equipment that is used.

National Standards and Policy

The NASPLE and Audit Standards provides a comprehensive framework to support compliance with DPA and the Surveillance Camera Code.

Does the processing (the plans) help to achieve a purpose?

Yes - ANPR is an important technology for law enforcement enabling them to meet their statutory obligations and is indicated in previous sections.

Is there another way to achieve the same outcome?

No, the extensive use of ANPR by the police and LEAs enables observation of vehicle movements to be undertaken quickly efficiently and extensively and, could not be achieved by human observation in the absence of technology.

What are the conditions for undertaking sensitive processing?

Sensitive processing is processed under **Schedule 8 DPA** – Conditions for sensitive processing under Part 3. This may be relevant to some VOI lists and the relevant conditions of schedule 8 including 'Administration of justice' and 'protecting individual's

vital interests' apply. Controllers are accountable for the content of VOI lists managed by their police force or LEA and NASPLE requires that all have relevant policy documents in place. The templates within NASPLE support management of VOI lists and additionally business rules for construction of Police National Computer (PNC) reports to support ANPR require that circulations use a PNC reference number for an individual and that the name of the person is not included within the report, thereby providing a safeguard for the processing of sensitive data.
Bulk VOI lists from the Driver and Vehicle Licensing Agency (DVLA) and the Motor Insurers Bureau (MIB) include details of vehicles that are not compliant with vehicle registration, licensing or Insurance requirements. DVLA and MIB are accountable as controllers for the accuracy of data within the lists that are supplied, however the content and volume of entries within the data for those lists is subject to review to ensure that the information remains relevant and that circulation is proportionate. Staff within 'Approved LEA' are only to be permitted access to that data where relevant to their role and for purposes consistent with NASPLE.

How will you prevent function creep?

The requirements for ANPR is document managed by NAS Programme board. Any changes must be agreed through that process which may require a further DPIA.

How will you ensure data quality?

The VRM as recorded by the cameras and enter NAS are a matter of fact in the interpretation by ANPR system. NASPLE includes provisions requiring the correction of any inaccurate reads by staff identifying that inaccuracy. Information within VRM lists are based on facts and the staff within he police force or LEA that initiate the circulation of the list are accountable for ensuring the accuracy of the information the justifies that circulation and for ensuring that circulations are not based on opinion.
Standards are set within the Audit Standards. It is known that the poor quality of vehicle registration plates can cause poor or inaccurate data within the ANPR systems. With support of the surveillance camera commissioner proposals to improve the regulation of number plate manufacturer and improved vehicle testing is on-going.

Data quality, consistency and retention

Data quality and consistency are important aspects of privacy. A high standard of data quality is important to the successful implementation and the realisation of benefits from NAS.

The primary purpose for the retention of ANPR data is to support investigations. Maximum retention periods for ANPR data have been defined at 12 months and will remain under review.
Whilst other factors may also be relevant this element of assessment requires consideration of the following factors, with appropriate analysis:

- The numbers of people that are or could be affected by the issues identified within the strategic assessment.
- Whether those issues could lead to damage, distress or both and if so the nature and severity of those consequences.
- Any local views on the deployment of ANPR.
- Any wider societal views on the use of ANPR.
- The alternative tactical responses that may be available to meet the challenges that may be less or more intrusive than ANPR.
- How the use of ANPR will assist resolution of the issues identified.
- The scope of privacy intrusion – How many people does this affect? (E.g. traffic volume).

Process in place for faulty cameras

Yes - Requirements for performance and testing as part of the standards.

How do you intend to ensure data quality and minimisation?

Included within NASPLE with requirements for compliance and audit. NASPLE requires police forces and LEA to manage and delete data from NAS within the timescales detailed within the standards and to ensure compliance with CPIA and MOPI in respect of data from NAS that is managed in other systems.

How do you intend to provide privacy information to individuals?

ANPR website and members of public have access in line with DPA requirements to local and national websites. All organisations that are parties to the NAS will provide consistent information for data subjects and a Single Point of Contact (SPoC) will be provided to assist communications.

Privacy feature of NAS

A number of features of NAS provide significant privacy improvements in comparison with the current infrastructure, such that there will be safeguards to ensure that the system is only accessible by authorised, trained users. Users will only be able to access ANPR data as authorised and necessary in the context of their role. All use of the system will be logged and subject to audit. NAS capabilities will be developed with full consideration of privacy and data protection requirements. Business rules will be set for the use of the system, and for the use of any information obtained from it to support compliance with NASPLE. The retention period is 12 months, his has been considered as part of this DPIA review which confirms that 12 months remains currently appropriate however this will remain under review. Deletion functionality and leap years have been considered such that whilst access to data is limited to 12 months, deletion occurs at 367 days.

How will you help implement and support individual's rights?

Access to the relevant information to local and national police websites will be available to provide information to any member of the public. A template for a data protection notice for each police force and LEA will be made available providing information regarding the reasons for deploying ANPR and how data is collected and used. Information regarding data subject rights will be included. In addition, information will be provided on national web sites. Details are included in the documents NASPLE and Audit Standards which have already been published.
All forces have a Senior Responsible Officer with regards to Data Protection and Data Protection Freedoms. All forces have a data protection contact and specifically dedicated data protection staff.

What measures do you take to ensure processors comply?

Data processing contracts are in place and are kept under review. Audit standards set out the requirements for review which are within the responsibility of the national auditor.

How do you safeguard any international transfers?

Data may be transferred with established Schengen procedures which include appropriate safeguards in relation to that data. It is not intended that other international transfers will take place. The National Crime Agency (NCA) manage Schengen enquiries consistent with the provisions of NASPLE regarding disclosure of data. Vehicle movement data is not disclosed otherwise than through those processes.

Safeguarding access to the system

Chief Officers as joint controllers will implement the Government Security Classification (GSC) in respect of ANPR systems.
Privacy is currently assessed on the basis that the system has been accredited as OFFICIAL – SENSITIVE within the GSC. A requirement of the system is that only a limited set of records are accessible at any interface at any one time. Strict controls are in place to control the personal data volumes available at the interfaces.
Technical security risk analysis was conducted to identify the specific controls that are required and the Information Risk Assessment Report (IRAR) has been developed in liaison with the National Accreditor, and in connection to the NAS is in accordance with their requirements and that analysis.

Safeguarding access to the data

NAS will support role-based access such that users will only have access to data that they need for their business role.
NAS functionality and clearly defined business rules will define and limit the access of staff to data.
Standard report templates will be established to meet identified user requirements.
Statistical and performance reports will not include personal data other than relevant details of LEA staff. The number of data items and time parameters for these reports will not be limited.
The full set of business rules, limiting access to data, will be in place prior to the roll-out of NAS.

Auditing Use of NAS

In addition to securing access to the system and to the data within that system, NAS will include auditing capabilities that will deter misuse and, where misuse does happen, help to identify and provide evidence against those involved.
All access to and activity within NAS will have a mandatory logging functionality in accordance with S62 DPA. This will include searches and other data retrieval, what was done and when it occurred.
In addition to identifying misuse of access rights, the audit provisions within NAS will help to identify any unauthorised attempt to access from an external source or attempts to bypass access controls from within LEAs.
The NAS audit log will be used for the purposes of proving the integrity of the system and for monitoring any improper use, including the analysis of patterns of usage over a period of time.
The log will be available to LEAs, National Auditors, and the Information Commissioner's Office if required. Auditors will conduct reactive audits, investigating where misuse is

suspected and proactive audits, sampling activities to check for misuse or complaint, suspected breach or for audit purposes.
The activities of auditors on NAS will be logged and also subject to audit by the National Auditor.

NAS will be seeking feedback from auditors on any problems identified to enable consideration to be given to strengthening controls either through the IT or business processes.

NAS will be seeking feedback from auditors on any problems identified to enable consideration to be given to strengthening controls either through the IT or business processes.

Identification and assessment of risks

	The source of risk and nature of potential impact on individuals.	Likelihood of harm Remote, Possible or probable	Severity of harm Minimal significant or severe	Overall risk Low, medium, high
1	Retention Period of retention is disproportionate and excessive.	Possible	Significant	Medium
2	An LEA may deploy ANPR other than in accordance with the requirements detailed within NASPLE, as a result this may not be proportionate to the risk and purpose of deployment.	Possible	Significant	Medium
3	Quality Data within the NAS may be inaccurate when standards are not followed as a result of external factors such as poor quality number plates.	Probable	Significant	High
4	Responsibility The operation and management of ANPR by LEAs is not consistent with the national strategy and policy.	Possible	Significant	High
5	Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their privacy.	Possible	Minimal	Low
6	Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate, or the VRM may have been faulty. The VRM may be false. This includes the potential for a vehicle to displaying a cloned number plate.	Possible	Significant	Low
7	Inappropriate access to data,	Possible	Significant	Low
8	Inappropriate disclosure of data.	Possible	Significant	Low
9	Excessive data is collected.	Possible	Minimal	Low

10	The information can be damaged or inappropriately deleted	Possible	Significant	Low
11	The information is inaccessible to those who should have access to it	Remote	Significant	Low
12	The information is being used unfairly or without transparency to data subjects	Possible	Significant	Low
13	The information is being used for a purpose incompatible with the reason it was first used	Possible	Significant	Low
14	Duplicate versions of the information exist	Remote	Minimal	Low
15	Vehicle of interest lists may include a large number of vehicles such that they are not proportionate taking account of reason for circulation and the geographic extent of circulation.	Possible	Minimal	Low
16	Data storage arrangements may need to be changed depending on the outcome of Sungard (UK) Ltd Administration	Possible	Significant	Medium
17	Oversight and consultation with civil society groups and others with concerns regarding the use of ANPR by policing and IEAs may be reduced with the removal of the Biometrics and Surveillance Camera Commissioner post who also chairs the IAG	Possible	Minimal	Low

Measures to reduce risk

	Risk	Options to reduce or eliminate risk	Effect on risk Eliminated Reduced Accepted	Residual risk Low Medium High	Measure approved Yes / No
1	Retention	Operational use remains under review and retention subject to further consideration	Reduced	Low	
2	Deployment	National oversight of ANPR infrastructure that will ensure consistency in decision making LEAs and prevent duplication of infrastructure between LEAs.	Reduced	Low	
3	Quality	Mitigated by procedures by LEAs to ensure compliance with NASPLE -compliance and audit standards are met.	Reduced	Low	
4	Responsibility	Provision of oversight by NPCC ANPR lead and monitoring compliance and audit activities by LEA.	Reduced	Low	
5	Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their privacy.	Transparency in regard to ANPR with provision of information concerning why it is needed, how it is used, provided via internet sites, written communication and through NPCC.	Reduced	Low	
6	Action taken as a result of ANPR hits from a camera may be seen as disproportionate or the VRM may have been	Management controls in place to ensure use in accordance with NASPLE. Robust process for managing lists of vehicles of interest to ensure that data for the circulated	Reduced	Low	

	faulty. The VRM may be false.	vehicles remains accurate and relevant.			
8	Inappropriate access to data	NASPLE sets out clear rules for data access. NAS functionality is designed to limit access to that appropriate for the role of the user. Audit provisions in place,	Reduced	Low	
7	Inappropriate disclosure of data.	Data is only shared and accessed in accordance with NASPLE. Provisions for monitoring and audit of data access and use in place.	Reduced	Low	
9	Excessive data is collected	ANPR is only deployed where a pressing need has been identified for law enforcement purposes and that deployment is proportionate. Retention and disposal of data is in accordance with NASPLE.	Reduced	Low	
10	The information can be damaged or inappropriately deleted	Users are not able to delete data in NAS but can alter reads which is essential for correction of any misreads. All transactions are logged, and audit provisions are in place	Reduced	Low	
11	The information is inaccessible to those who should have access to it	Users have access to data according to permissions. Local management servers provide a capability should the NAS become unavailable	Reduced	Low	
12	The information is being used unfairly or without transparency to data subjects	Subject rights notices published nationally and by police and LEAs	Reduced	Low	
13	The information is being used for a purpose incompatible with the reason it was first used	Approved use is fully documented in NASPLE. Approved use is included within training. Audit requirements are in place.	Reduced	Low	

14	Duplicate versions of the information exist	Local copies of read data are retained for 7 days subject to detailed requirements of NASPLE If received at a management server more than 7 days after the time of the read it may be retained for a maximum of 24 hours.	Reduced	Low	
15	Vehicle of interest lists may include a large number of vehicles such that they are not proportionate taking account of reason for circulation and the geographic extent of circulation	NASPLE requires that VOI lists are proportionate to the circumstances relevant to each list and that access permissions are limited as appropriate. Guidance on the management and use of VOI lists to be provided by the lead controller.	Reduced	Low	
16	Data storage arrangements may need to be changed depending on the outcome of Sungard (UK) Ltd Administration	Continued monitoring of the situation and a DPIA will be completed as required. Plans developed for security of data should change be needed. Redcentric plc now appointed in place of Sunguard	Eliminated	Low	
17	Oversight and consultation with civil society groups and others with concerns regarding the use of ANPR by policing and IEAs may be reduced with the removal of the Biometrics and Surveillance Camera Commissioner post who also chairs the IAG	Appointment of a new chair of the IAG	Reduced	Low	

Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Chief Constable Charlie Hall Hertfordshire Police Welwyn Garden City AL8 6XF	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Chief Constable Charlie Hall Hertfordshire Police Welwyn Garden City AL8 6XF	If accepting any residual high risk, consult the ICO before going ahead
Data Protection Officer advice provided:	Jack Chimes Director of Information & SIRO Bedfordshire, Cambridgeshire and Hertfordshire Police Collaboration – NPCC ANPR Data Lead	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: *I have been fully involved in the development of this DPIA and the appropriate consultation. I am satisfied that the processing is proportionate and lawful. All relevant risks are identified and mitigated having consulted with interest groups and regulators. The processing replaces legacy national and local ANPR systems and is therefore ongoing. It is appropriate that this should continue. This DPIA should be subject to ongoing review by the ANPR Standards and Security Group and approved by the lead controller at least annually.* *The DPIA has been reviewed and updated. All relevant risks have been identified and mitigated. It is appropriate that the processing continues and remains subject to annual review.*		
DPO advice accepted or overruled by:	Accepted C Hall	If overruled, you must explain your reasons
Comments:		

Consultation responses reviewed by:	K Sharpe	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by: Jack Chimes – NPCC ANPR Data Lead	A review should be carried out on each release of functionality	The DPO should also review ongoing compliance with DPIA

Appendix 1 List of Approved Organisations

Avon and Somerset Constabulary
Bedfordshire Police
Border Force
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Department for Work and Pensions (DWP)
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Licensing Agency (DVLA)
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Environment Agency
Essex Police
Food Standards Agency
Gangmasters and Labour Abuse Authority
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
HM Revenue and Customs (HMRC)
Humberside Police
Immigration Enforcement
Intelligence Services
Kent Police
Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Medicine and Health care products regulatory agency (MHRA)
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police

National Crime Agency (NCA)
NAFN Data and Intelligence Services (facilitating Local Authority Trading Standards investigations)
National Vehicle Crime Intelligence Services (NaVCIS)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Scotland
Police Service of Northern Ireland (PSNI)
Royal Air Force Police
Royal Military Police
Royal Navy Police
Scottish Environment Protection Agency
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Thurrock National Investigation Service
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police
Wiltshire Police