Home Office

NPCC National Police Chiefs' Council

Law Enforcement Data Service

Data Protection Impact Assessment (DPIA)

Date: October 2020

Version: 1.0

This publication is available at www.gov.uk/government/publications.

Any enquiries regarding this publication should be sent to us at LEDS@homeoffice.gov.uk.

Contents

The need for a DPIA

The Law Enforcement Data Service (LEDS) will provide police forces and other law enforcement agencies with the latest, on-demand and joined-up information at the point of need. This will help to prevent crime and better safeguard the public.

The chief constable (or commissioner) of each police force is a registered data controller ('a controller'). Through their nominated National Police Chiefs' Council (NPCC) leads, they will be the joint controllers for all police data (law enforcement data) held in LEDS. The NPCC, as established under section 22a of the Police Act 1996, will determine the purpose for processing the data and the means. They are jointly accountable for the completion of this DPIA.

The Home Office are responsible for the development and management of LEDS infrastructure, which will be hosted using the skills and expertise of a main system data processor ('a processor'). LEDS will be hosted on a cloud-based platform, which will enable LEDS to facilitate requests for data by authorised users of the service. Authorised users process the data in LEDS under a lawful bases or a lawful purpose.

LEDS involves multiple system and services, each providing access to separately owned datasets. It is the responsibility of the controller to determine how that data will be processed. The Home Office will manage the data within LEDS, as directed, by the various controllers. The Home Office, as owners of some data, will also be a controller. LEDS will have multiple controllers and data flow processors, acting on behalf of the Controller. Each role will be legally determined and enforced using joint-controller agreements, data processing contracts and where necessary, memorandums of understanding.

A LEDS Privacy Impact Assessment (PIA) was completed and published in July 2018 and has remained under review since that time.

As set out in the Data Protection Act 2018 a DPIA is required if "processing is likely to result in a high risk to rights and freedoms of individuals.'

The specific aims of the LEDS DPIA are:

1) To ensure that all data protection risks have been identified and to review the status of the Law Enforcement Data Service (LEDS) in the context of recent legislation and case law.
2) To ensure consistency and support throughout the police service and wider law enforcement in how data is captured, used, stored and deleted.
3) To ensure consistency and support throughout other law enforcement agencies with access to the data in LEDS.

4) To ensure compliance with Data Protection Act (DPA) 2018
5) To ensure compliance with the General Data Protection Regulation (GDPR)
6) To ensure compliance with Human Rights Act 1998.
7) To take account of European Convention on Human Rights (ECHR)
8) To follow guidance from the Information Commissioner's Office (ICO)
9) To ensure the principles of data protection by design have been considered in the design and implementation of the LEDS.

Law enforcement agencies in the United Kingdom currently make use of a wide variety of information systems at a local level. They collect and process data in connection with their law enforcement and policing purposes. It has also been recognised that there is great value in being able to share relevant information across law enforcement agencies in a timely and effective fashion. The two national systems under consideration here are:

- **The Police National Computer** (PNC), was introduced in 1974 and holds personal data and other information relating to individuals, including arrests, charges, summons & court disposals (including convictions), warnings and whether a person is wanted or missing. There is also other information about vehicles and stolen property. Some of the data available on PNC has been migrated from other systems.
- **The Police National Database** (PND), was introduced in 2009 and receives intelligence data, predominantly uploaded by police forces, concerning crimes, intelligence and public protection. This also includes custody information and custody images.

Both are owned and managed by the Home Office. LEDS will relocate both onto a single technology platform, enabled by a cloud commodity provider. This relationship will be managed using a Data Processing Contract as required under s.59(5)-(7) DPA.

It is clear that the integration of data, alongside increased search functionalities presents the potential for significant data protection risks. It is essential for the police service and authorised law enforcement organisations to ensure that the collection and use of data is and remains specific, explicit and legitimate for policing and law enforcement purposes. Further access to this data must be compatible with the purpose for which is was collected as required under Part 3 s.36(3)(b) GDPR.

The risks posed to processing personal data and their mitigations are detailed below in the Identification and assessment of risks section. Article 35 of the GDPR details the conditions for completing a DPIA. Section 64 DPA will also apply in relation to law enforcement processing. This states that where processing of data is likely to result in high risks to the rights of individuals a DPIA must be produced.

The high-level risks associated with processing data in LEDS have been appropriately mitigated to reduce any potential impacts on individuals. As a result, this DPIA is not required to be submitted to the Information Commissioner for prior consultation as detailed under s.65(2) DPA.

The nature of the processing

Introduction

LEDS will provide law enforcement agencies with current and joined up information, on-demand and at the point of need, in order to prevent crime and better safeguard the public. In addition, it will:

- Rationalise national information systems
- Enhance the national information dataset
- Deliver more service capabilities from the national information dataset; and
- Reduce the cost of providing and maintaining national policing information.

If data in LEDS is processed by a Competent Authority (s.30 DPA) and the processing is for law enforcement purposes as defined in s.31 of the DPA then the processing is covered by Part 3 of the Act. If data is processed for a purpose which is not a law enforcement purpose (whether or not by a Competent Authority) then the processing will be under the regime set out in the GDPR (where appropriate as applied by the DPA).

Processing under Part 3 of the DPA or under the GDPR must meet the six Data Protection Principles (the Principles) under which controllers are responsible for ensuring and demonstrating compliance with;

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

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

Principle 6 – data should be processed in a secure manner

The types of data processed

The third Principle requires that the personal data processed must be adequate, relevant and not excessive for the purposes for which it was processed. Data processing is any operation performed on information (or sets of information) involving:

- The collection
- Recording
- Organisation
- Structuring; or
- Storage of data

LEDS supports law enforcement purposes as defined in Part 3 DPA. There are also other policing purposes, such as safeguarding responsibilities, captured for the purpose of general data processing under Part 2 DPA.

LEDS will process data relating to:

- Individuals suspected of committing offences (including those arrested and under investigation) and on individuals who have been convicted of offences
- Driving licence holders
- DVLA records but with no licence
- Registered keepers of vehicles
- Firearms licence holders
- Economic status (where details relating to lifestyle and possessions may be relevant)
- Health status (where this is relevant to law enforcement and safeguarding)
- Personal preferences or interests (where this might be relevant to law enforcement)
- Reliability or behaviour
- Location or movements
- A missing or found person
- A person who has escaped from lawful custody or detention
- A person who has been recalled to a specific institution
- A person subject to legal processes (waiting to appear at court)
- A wanted person (identified with a wanted report)
- Details of certain court orders made against a person
- Data relating to vulnerable individuals
- Intelligence data; and
- Data for a contact person or organisation

Organisations processing data in LEDS

There are four key categories of organisations that will process LEDS data:

- UK Police forces – includes the 45 geographical police forces in the UK, including the Police Scotland and the Police Service of Northern Ireland. (See Appendix A for the full list).
- UK Policing organisations – includes British Transport Police, National Crime Agency.
- UK policing organisations who exercise their powers locally – such as Port of Tilbury Police.
- UK non-police organisations – includes other organisations like the Financial Conduct Authority and Highways England who use the data to support wider law enforcement, e.g. safeguarding the public. It also includes organisations with prosecutor functions to perform, e.g. the Competition and Markets Authority and Royal Mail. Some organisations access the data to carryout personnel vetting function, whilst others receive specific downloads. Their access has been approved via the PNC Information Access Panel (PIAP). A comprehensive data review of these organisations will be undertaken to ensure processing is lawful and fair in accordance with the first principle.

- International organisations such as the Crown Dependency police forces – these are in Jersey, Guernsey and Isle of Man and have access to PNC. (See Appendix A).

Access will be reviewed by controllers in line with their data responsibilities. Compliance by police forces is the responsibility of chief constables (or commissioners). After the data review process, access by the majority of non-police organisations are likely to continue. However, it is anticipated that the review will highlight some anomalies. In these cases, recommendations will be made on rectifications to that access in LEDS. This will be undertaken in compliance to the Principles.

A list of organisations *directly* (internal facility) accessing data via LEDS can be found in Appendix A.

A list of organisations *indirectly* (external facility) accessing data via LEDS, serviced by the ACPO Criminal Records Office (ACRO), can be found in Appendix B.

Processing Driver and Vehicle Licensing Agency data

The Driver and Vehicle Licensing Agency (DVLA) currently holds over 30 million driver records. This includes the driver's photographs, if one exists[1]. They are responsible for the registration and licencing of vehicles and issue, revoke and amend driving licences.

Individuals' personal data will not appear in LEDS simple because they hold a driving licence or are recorded as the registered keeper of a car. However, LEDS will allow authorised officers (or 'constables') to access DVLA data through an Application Programming Interface (API). That DVLA data will no longer be copied to LEDS will increase the integrity of the data and support the fourth Principle.

While there are no purpose limitation for Vehicle Registration Data, driving licence data may only be accessed when specifically investigating traffic incidents.

For some data, the Police also provide driver data updates to the DVLA, e.g. through the creation of vehicle records for vehicles not registered or licensed by the DVLA, for example, diplomatic vehicles. Other data updates currently provided to the DVLA are:

- Disqualified driver's discrepancy report; and
- Vehicle theft/recovery notifications

Driver licence data will be the first set of data processed on LEDS. Other sets of data will continue to be added onto the platform, on an incremental basis. Data relating to vehicles does not form part of the RTA purpose limitation.

DVLA also maintain data on licence endorsements issued by the Court Service, following a conviction for a motoring offence. Driver offence data will be part of later deployments of data onto LEDS. The API will eradicate previous time delays in the transfer of data between DVLA and the Police. DVLA data will not be stored on LEDS as the requested

[1] A photo will not exist if a person has a paper licence issued before July 1998, has not moved address since then and is still under 70.

data will be available direct from its source. This provides greater data protection for members of the public, by default.

The data relationship will be managed using a Data Processing Agreement. In relation to the initial processing of DVLA driver licence data, the DVLA will be a controller and the NPCC will be Processors of that data. The various data relationships will be determined by the sets of data being processed and the roles involved.

Table No.1 shows the DVLA data being processed for driver licence data via LEDS;

Driver Data	Controller(s)	Purpose for Processing	Police Processing Type
Driver identification personal details, address, date of birth	DVLA	Law Enforcement – Part 3 DPA	Access
Driver category Entitlement category	DVLA	Law Enforcement – Part 3 DPA	Access
Driver records Health data, including eyesight/hearing	DVLA	General Data – Part 2 DPA	Access
DVLA markers	DVLA/Police	Law Enforcement – Part 3 DPA	Access
Police reports/ points/disqualifications (force level)	DVLA/Police	Law Enforcement – Part 3 DPA	Access
Endorsement history, current points tally, start & end data	DVLA	Law Enforcement – Part 3 DPA	Access

Details of processing

LEDS processing operations include;

- Creating the data record (excluding drivers)
- Amending the data record (excluding driver)
- Deleting data (excluding drivers)
- Retaining data (excluding drivers)
- Validating data
- Reviewing data
- Retrieving data
- Accessing data
- Applying data
- Sharing data; and
- Analysing data

How is data used?

In compliance with the first Principle, the data in LEDS will mainly be used for policing purposes and for other purposes compatible with the purpose for which the data was collected. This means that the data will be used for **law enforcement** and it can also be used for **general processing purposes**. If the processing is for law enforcement purposes it is defined as:

- The prevention, investigation and detection of criminal offences or
- The prosecution of criminal offences or the execution of criminal penalties; and
- The safeguarding against and the prevention of threats to public security.

If the processing is by "competent authorities" (as listed in Schedule 7 of the DPA), Part 3 of the Act applies to the processing.

Data in LEDS will also be used for general processing purposes, which includes those purposes consistent with policing purposes as described in College of Policing Authorised Professional Practice (APP) on Management of Police Information (MoPI):

- Protecting life and property
- Preserving order
- Safeguarding purposes; and
- In circumstances of significant public interest and purposes of public safety (for example, vulnerable and missing persons)

Any unused data, initially intended for law enforcement, will fall under the general processing regime, Part 2 DPA. Both types of data will be subject to the LEDS Retention Policy and Retention Schedule. These will be based on the data deletion rules established by the NPCC. The DPA in part 3 chapter 2, section 39(2) requires that appropriate review periods need to be established for periodic review.

Table No.2 shows the types of policing scenarios and how it is most commonly used:

Policing Role	Personal Data	Part 3 – DPA	Part 2 – DPA
Frontline response to incidents (often complex and confrontational situations)	Yes	Yes	No
Protecting against potential and actual risks to individuals (addressing any vulnerabilities)	Yes	Yes	No
Gather information that *may* support law enforcement objectives	Yes	No	Yes
Interview victims, witnesses and suspects of alleged crimes	Yes	Yes	No

Building links in the local community to engage, reassure and support	Yes	No	Yes
Work in partnership with others/general stakeholders	Yes	No	Yes
Effectively engage with victims, witnesses and the vulnerable to provide initial support and direct towards relevant services	Yes	No	Yes
Maintain awareness of potential risks to individuals	Yes	No	Yes
Maintain awareness of actual risks to individuals, taking appropriate action to protect and support those in need of public protection	Yes	Yes	No
Conduct effective investigations as requested in line with standards of investigation for case files and court proceedings	Yes	Yes	No
Gather and handle information, intelligence, and evidence, from a variety of sources, in line with legislation, policies and guidance e.g. mobile phone extractions.	Yes	Yes	Maybe
Taking the appropriate action to support investigations, law enforcement and criminal justice proceedings.	Yes	Yes	Maybe

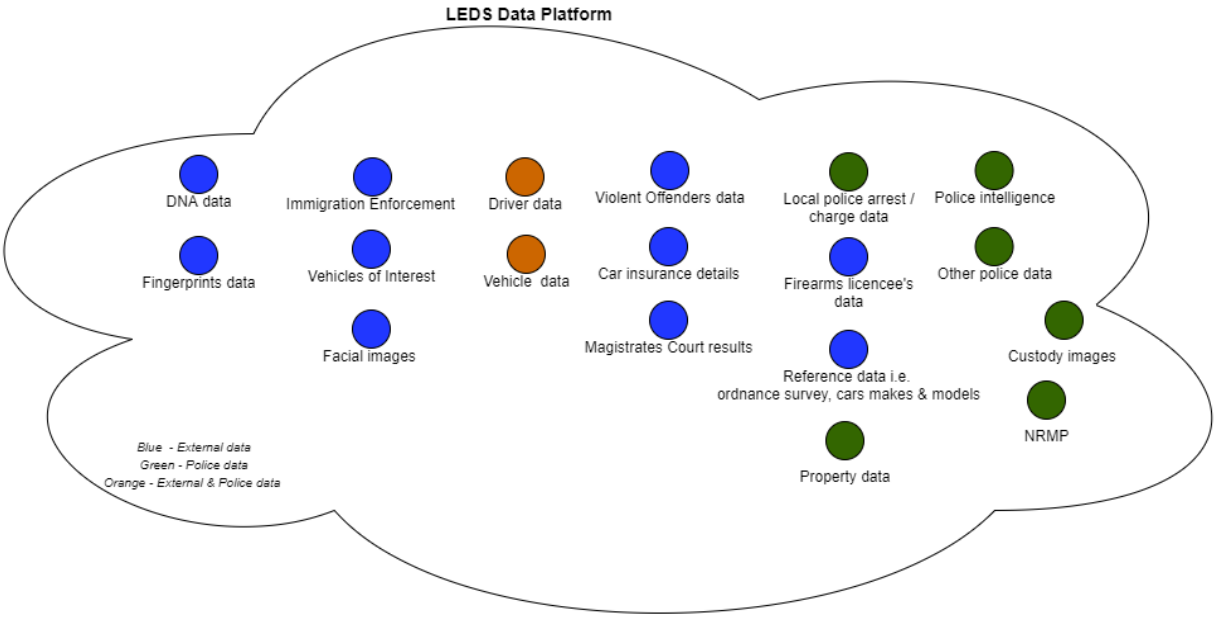
How is data collected?

Data can be collected;

- By direct entry onto LEDS.
- By data entered into another system, then transferred to or accessed by, LEDS. For example, when Magistrates' Court update court results, via the Bichard 7 interface.

The data will also be processed via an API. It will help to reduces the number of disparate interfaces currently needing support. Organisations are being encouraged and supported by the Programme, to use the API service, where feasible.

Diagram No.1 illustrates the sources of data that will be processed by LEDS:

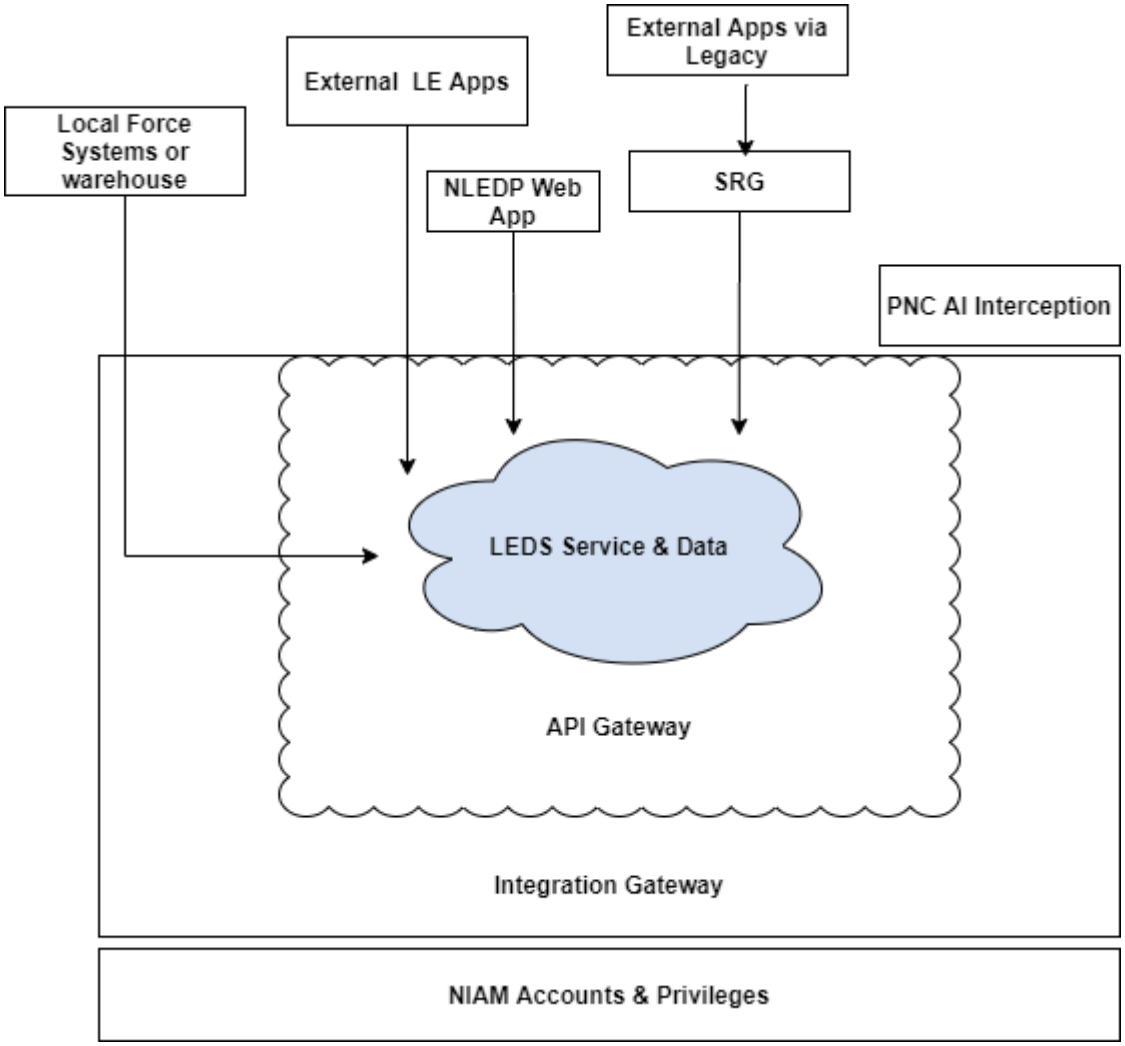


What are the access routes to LEDS data?

Access to LEDS will be through the LEDS web application. It will verify requests according to role-based access controls. Users will be granted differing levels of access according to their organisations law enforcement requirements to the data.

Depending on the levels of permissions, users will be able to read, create and amend records. Others, such as some of the commercial organisations, will have indirect access to pre-defined data downloads. The most sensitive data, such as information about victims and witnesses will have additional controls to manage access and search facilities to their data. Interfaces currently used by forces for custody applications, mobile applications and for command & control will continue, unchanged by the LEDS technology.

Diagram No. 2 shows the access routes into LEDS:



Gateways into the data will all be required to meet a minimum standard set by the National Policing Information Risk Management Team (NPIRMT). They are responsible for assessing the security functionality of all organisations accessing LEDS data. LEDS Integration Gateway requires Access Tokens to show the context of requests. This will be supported by the National Identity and Access Management tool (NIAM).

Appendix C lists the sources of data for LEDS.

Who has access to the data and by what methods?

The key users of the service are authorised officers using physical devices such as;

- Desktop computers
- Laptop computers
- Tablet devices; and
- Smartphones devices

Other authorised users (listed in Appendix A & B) will, mainly, access LEDS from desktop computers. Viewing data via a browser as a web application.

Access to LEDS data can also be provided via specialist super users, providing services to frontline officers and other organisations, e.g. the Borders Forces Watchlist and Information Control Unit (WICU), who assist Immigration Enforcement with information from LEDS. Other methods include, control rooms, bureau staff (usually affiliated to local forces) and officers performing their own checks under Part 3 DPA, by virtue of their Chief Constables (Commissioner) competent authority status. They are currently staffed with experienced operators who can create, amend or delete data. Access is managed at force level, supported by supervisory auditing capabilities.

Locally issued hand-held devices will be owned and managed by the issuing organisations are built to allow them to be remotely wiped. Personal data will not be available on local devices beyond an officer's live session. Device will be locked out after it has been used. The data will be formatted to aid the users experience and devices must use passwords and other access control methods designed to restrict accidental disclosure including regular audits. Occasions of inappropriate use by authorised users, e.g. taking photos of a screen containing the personal data of others can never be 100% eliminated.

The Governance Information Risk Return (GIRR) assessment process will also include a security review of each accessing organisations remote devices, against its readiness to access LEDS. The conditions of use will be stipulated in the relevant data agreements.

Who will share the data?

Data will be shared by the controllers with each other (under the terms of a joint controller arrangement) Data will also be shared by the controllers with other organisation which are not joint controllers under the terms of controller/processor contracts or memoranda of understanding. The list of organisations which will have access to LEDS is at Appendix A.

There are several departments within the Home Office that access PNC data. The Home Office are named competent authorities in the DPA and will be a controller. They are able to create and update PNC. For example, the Border Forces and UK Visa and Immigration, within the Home Office can:

- Add, amend and delete a wanted or missing person report; and
- make an update to an existing LEDS profile

In addition, the Home Office Data Integrity Teams reconcile fingerprints and DNA data vi. As part of their work to improve the quality of data on PNC, they are permitted to amend Police data. This permission is expressly provided by the chief constable (or commissioner) owning that data. This role is not expected to change with the introduction of LEDS. They can add, amend and delete a wanted or missing person report as well as:

- Update addresses
- Update local police reference numbers
- Update custody location details; and
- Delete a person.

A list of all Home Office units with access to PNC data are listed in Appendix D.

For the purposes of LEDS, the NPCC will continue to provide leadership and direction as a coordinating body for police forces as approved under s.22a of the Police Act 1996 Act.

There is no coordinating body tasked with the collective oversight and leadership responsibilities for non-police organisations. However, all organisations with access will be expected to follow the same policies, practices and guidelines as Police forces when processing data, including regard to the LEDS Code of Practice and Guidance Document.

A limited number of private companies will have access to a specific & pre-determined set of data. For example, HPI performs checks against the data in LEDS to see if vehicles have been reported as stolen by a Police force. Others, such as the Royal Mail, undertake prosecutions in relation to the security of their operations and have access to police data to support these functions.

The Information Commissioner can take regulatory action for breaches of the DPA in respect of sharing data unlawfully, including sharing data overseas where there is no guarantee of an adequate level of protection for the rights and freedoms of data subjects. Where this is required, a policy document must be in place, demonstrating that it is safe to do so.

Sharing responsibly will provide accurate and joined-up information in order to bring offenders to justice, to prevent crime and better protect the vulnerable. The Programme, haven taken advice from the ICO, Office of the Data Protection Officer (ODPO) and Home Office lawyers that will facilitate the determination of future data roles as they relate to the data flows. The processing relationships will be determined in line with the incremental development of the programme and the specific sets of data being made available via LEDS.

The UK entered a 1-year transition period when it left the European Union on 31st January 2020. At the time of writing, UK law enforcement agencies continue to have access to the Schengen Information System (SISII). They are therefore, subject to the SISII regulations. This allows the UK to share alerts on wanted or missing persons and objects, both inside the EU and at the external borders.

Intelligence agencies (MI5, MI6 and Government Communications Headquarters) will also have access to data. It will be the responsibility of each organisation to ensure that the data they share falls within data protection requirements

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

Of the following data processing criteria, seven (shown in bold) are likely to constitute 'high risk' and have been used in determining whether to conduct a DPIA.

1. **Evaluation or scoring** – LEDS data can be used indirectly, to identify patterns in the data as well as providing statistical data. This can be used by strategic decision makers to draw inferences, enabling effective operational and policy decisions to be made. Data could relate to an individual's economic situation, health, location or movements. LEDS will permit this information to be stored.

2. Automated-decision making with legal or similar significant effect – LEDS will not be used to make any solely automatic decisions that could potentially lead to a discriminatory course of action against the member of the public. For example, no processing activity would ever be solely used to trigger an automatic arrest of a member of the public.

3. Systematic monitoring – LEDS services will not be used to directly observe, monitor or control members of the public. Some LEDS data will be processed without the knowledge of the data subject (for example intelligence data).

4. **Sensitive data or data of a highly personal nature –** LEDS will hold large amounts of sensitive data. This type of data increases the risk to the rights and freedoms of individuals if misappropriated, damage could be done to a person's reputation or other freedoms they are entitled to enjoy within their private life.

5. **Data processed on a large scale** – Data on LEDS will be processed on a large scale. Typically, there has been an average of 11 million transactions completed per month by both policing and non-police organisations. This amounts to nearly 131 million PNC transactions a year.

6. **Matching or combining datasets –** LEDS will be combining existing datasets from multiple sources. LEDS will combine data originating from two or more data processing operations. LEDS relationships will involve multiple controllers and processors of data which makes it high risk to individuals.

7**. Data concerning vulnerable data subjects –** LEDS will hold data in relation to a wide spectrum of people. There is an imbalance in the relationship between controllers and individuals. For example, children are not regarded as being able to properly consent or oppose to their data being processed until 13 or 16 years old (GDPR). This would also apply to those that are mentally ill, asylum seekers or have certain physical disabilities.

8. **Innovative use or applying new technological or organisational solutions** – LEDS be regarded as a novel form of using and collecting data. It combines a variety of law

enforcement data sources onto a single platform, with access to images and fingerprint data.

9. **Prevention of data subject from exercising a right –** Certain other rights under the GDPR, such as the right to object and the right to data portability, do not transfer to data collected under Part 3 of the Act. These rights will apply to, for example, data collected and processed for safeguarding or immigration purposes. There are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising those rights when considered under law enforcement purposes. If inappropriately managed, there is a risk that interference with this data may not be proportionate and the processing of data may infringe the rights and freedoms of individuals. In mitigation, there will be a Data Protection Officer (DPO) for LEDS.

Are processors used?

Yes. They will provide the platform that will host the cloud service and will process personal data only on behalf of the controller. There will also be third-party suppliers of software applications and data storage. Data processing contracts will be used to state the duties of all processor towards the controller. A processor cannot appoint a sub-contractor to assist with its undertaking without prior authorisation of the controller.

Section 44 DPA requires processors to provide information that will assist individuals understand how their personal data is going to be processed. This will be available along-side the LEDS Privacy Notice.

What are the retention periods?

The fifth principle requires that data is not kept for longer than is necessary.

Table No.3 shows the current retention, review and disposal landscape for policing information:

Record/Data Set	Framework
Fingerprints/DNA status[2]	• Protection of Freedoms Act 2012 • Criminal Procedure and Investigations Act 1996 • The principles of management of police information (2014)
Property/Evidence	• Criminal Procedure and Investigations Act 1996 • The principles of Management of Police Information (2014)

[2] The confirmation is available via links from NDNAD and IDENT1 back into LEDS.

Operational Info (POLE) (missing persons, intelligence, safeguarding, local crime files etc)	• The principles of Management of Police Information (2014)
Operational Info (POLE) (PNC arrest, charge and conviction records)	• 100-year rule (2009)
Operational Info (General) (procedural, operational orders, performance etc)	• National Retention Schedule (2016) • Force business need
Custody Images	• The principles of Management of Police Information (2014) • Custody Images Review (2017) • Police and Criminal Evidence Act 1984

Elements of the data in LEDS may be kept for longer than others to provide both an investigatory and audit thread. Some of the data will be retained in accordance with the national retention criteria such as criminal offences under MoPI. This is based on an assessment of the risk posed to the public by that individuals act(s). Other data is deleted when it is no longer relevant, e.g. located objects are deleted after 7 days. The DPA requires appropriate time limits are established for periodic retention reviews of law enforcement data under part 3, Chapter 2 s.39(2).

The relevant data controllers will develop;

- A LEDS Retention Policy
- A LEDS Retention Schedule

The Home Office and the police will continue to co-operate in taking this forward. Information about previous criminal justice outcomes will be retained on LEDS and subjected to rules of retention for that type of data. The Police currently store details of all recordable offences and other specific offences on PNC until the individual is 100 years old. Non-conviction data e.g. missing persons, warning markers and court orders covering specific periods will be flagged for review and or deletions within PNC. The responsibility to determine the appropriate policy and schedules for retention rests with the controller

The primary purpose is to review law enforcement retention and disposal procedures and ensure the validity and legality of the data held in LEDS. This includes a process for reviewing and deleting court convictions. Once completed, it will provide guidance that will feed into the LEDS Retention Policy and Schedule. Until the approach has been finalised, the current retention regimes will continue to be used. The DPIA will continue to track developments and updates provided in future iterations.

Information about previous criminal justice outcomes will be retained on LEDS and will be subject to rules, already being practiced, taking account of relevant case law.

How is data stored?

The data will be stored electronically on Commodity Cloud. The process and authorisation to proceed with the chosen commodity cloud service was overseen by the National Police Senior Information Risk Owner (SIRO). This service will be hosted via servers located in the UK, on the processor's premises.

How will data be deleted?

In compliance with the fifth Principle, the DPA requires appropriate time limits are established to enable reviews to determine whether deletion should take place. Data in LEDS will be deleted in the following ways:

- Directly - The deletion of data from LEDS is a mixture of direct deletions by those organisations and personnel that have the appropriate rights to perform this function. For example, organisations that own the data will be able to delete entries and LEDS logging function will maintain logs for the data processed including deletions.

- System – Deletions can also take place via processing through another system. For example, if a main address is deleted and updated with another in that system that will be reflected in LEDS.

LEDS will be developed with protections built-in by design. The Programme is examining the possibility of using automatic deletions.

What security measures are in place?

LEDS is hosted in secure data centres with the appropriate level of physical security. Security operating procedures are in place and LEDS is subject to regular accreditation and reviews.

Police forces and other law enforcement organisations, processing LEDS data, are required to comply with detailed security requirements. These are overseen by a national accreditor and include provisions for all aspects of security, both physical and technical.

Access to LEDS data is restricted not only through role-based access but through technical measures. This means any attempts of access from an unauthorised network will rejected and monitored. There are a range of protective monitoring capabilities to detect and respond to suspicious activity.

Password requirements for access to LEDS are based on National Cyber Security Centre (NCSC) guidelines and is applicable to all user roles, third-party contractors, suppliers and staff responsible for the management of LEDS. Users with dual function for data access and administration will be allocated separate accounts.

Audit trails and records are maintained, which includes successful and failed searches. Users are also required to provide reasons for their access to LEDS when requesting data. All components of the service will be UK based.

The national accreditor for policing systems is NPIRMT. They set out the requirements for the physical features of all aspects of LEDS.

Are any new technologies in use?

Yes. LEDS will create a cloud-based, national platform for accessing law enforcement data, via a web-enabled interface. The service will replace PNC and PND over time and introduce a new safeguarding database for missing people.

Developments in the technology will remain under review via the DPIA.

The scope of the processing

What is the nature of the data?

The data in LEDS will be personal and sensitive personal data. The following list represents the sets of data that will typically be held on LEDS:

- Names/aliases/nick names
- Address(es)
- Date of birth
- Place of birth
- Sex Gender
- Ethnicity/race (codes in development)
- Height/physical description
- Images (custody)
- Marks & scars (any identifying marks)
- Custody record number (taken from the force custody system)
- Physical description (including hair colour, eye colour, facial features)
- Health flags (particularly in relation to safeguarding both officers and individuals)
- Status & identifiers for biometrically processed data held on another database (e.g. fingerprints via the IDENT1 system)
- Employee numbers
- National insurance numbers
- Vetting status/outcome
- Contact details; and
- Driver records (this data will now be accessed via an API which will provide real-time access to DVLA owned data).

The data will also relate to objects, places, events and companies.

What is the volume and variety of the data?

LEDS will collect large volumes of data and will include multiple categories of people. For example, victims, witnesses, community contacts and those involved in committing offences.

Table No.4 shows the most recent figures for datasets held in PNC for the end March 2020.

Dataset	No.
Dangerous Nominals	229,538
Active Dangerous Nominals	111,617
Firearms licence Applications	4,527,935

Firearms licence Certificates	2,019,507
Firearms licence Persons	2,065,828
Firearms licence Person Photos	1,959,542
NABIS Ballistics Incidents	74,673
National Ballistic Items	157,838
Named person data (arrested & convicted)	13,056,237
Vehicle data (including NI)	67,833,377
Drivers data (not including NI)	60,948,329
Property data	40,884
Visor Nominals	229,538 (111,617 are active)

The overall total is not cumulative so a person could, potentially be included on all totals. LEDS will not hold driving licence data.

What might be the sensitivity of the personal data?

LEDS will process sensitive data, where it is necessary for law enforcement investigations. LEDS will process sensitive personal data on:

- Race and ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union memberships
- Status & identifiers for biometrically processed data
- Health data
- Data related to sexual preferences, sex life, and/or sexual orientation.
- Criminal convictions and other out of court disposals
- Arrests and Charges
- Whether a person is wanted; and
- Whether a person is missing

The processing of sensitive data for a law enforcement purposes must be strictly necessary and satisfy one of the conditions for sensitive data processing, within schedule 8 DPA or alternatively be obtained with the consent of the data owner.

For example, as part of a law enforcement investigation data from victims and witnesses mobile phones may be stored on LEDS. The information will initially be entered into a forces local intelligence system and, if the intelligence data became relevant, uploaded into LEDS (via PND). This type of data will almost certainly be of a sensitive nature. NPCC guidance and templates are in place to manage data extracted from mobile phones.

In June 2020, the ICO released its investigative report on mobile phone data extractions. It highlighted the importance of ensuring the processing was strictly necessary and not merely a routine exercise.

The report considered the use of consent by forces, as a legal basis for processing sensitive data. It did, however, acknowledged the value of adopting ‘consensual approach’ as key to maintaining public confidence. The ICO noted pointed to the in-balance of power between the police and members of the public. This in-balance means that obtaining true consent was limited. For example, a victim could feel that a lack of consent to extract data may adversely impact the outcome of the case in Court. The report highlights the importance of meaningful, informed engagement with mobile phone owners, keeping them fully informed about their rights and choices.

What is the extent and frequency of the processing?

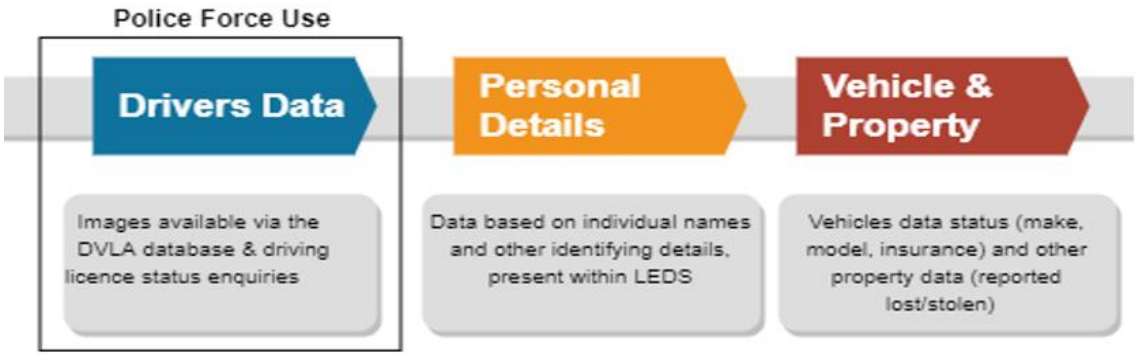
LEDS data will be processed 24 hours a day, 7 days a week and 52 weeks a year. There will be peaks and troughs for data use, but the service will be continuous.

What is the duration of the processing?

The processing of data on LEDS is not time limited and so will continue indefinitely or until LEDS is replaced. If LEDS is replaced, the data sets will continue to be processed in a successor system.

The initial data set processed via LEDS will be DVLA driver data with data relating to names and vehicles to be added incrementally.

Diagram No. 3 shows the Programme stages of delivery for processing data via LEDS:



What is the number of data subjects involved?

There is an average of 12.6 million person records currently on PNC. The largest category of data capture relates to offenders, with almost 11.5 million records.

What is the geographical area covered?

LEDS coverage will extend to all UK Police forces, specific law enforcement and safeguarding agencies across in the UK and all three Crown Dependencies Jersey, Guernsey and Isle of Man. For the purposes of the DPA, they are international organisations. To transfer data to the Crown Dependencies the controllers need to meet the requirements of Chapter 5 of Part 3 of the DPA.

Police forces and the National Crime Agency (NCA) interact with overseas law enforcement organisations and exchange data on a case by case basis. This function will continue using LEDS and will be managed by agreement.

It is not yet known whether the UK will be able to access data held on the SISII after the EU exit transition period ends. If access is unchanged, LEDS will hold alerts on wanted or missing persons, vehicle, documents and objects. Where this applies, the Home Office will be responsible for ensuring that each accessing organisation is compliant with international data sharing legislation requirements, prior to granting access to LEDS data. It is also expected that LEDS will hold details of criminal convictions for UK citizens overseas, as PNC currently does.

The context of the processing

What is the relationship with the individuals?

Members of the public are most likely to have one or more of the following profiles in LEDS and records may relate to adults, children and/ or vulnerable people.

Table No.5 illustrates a typical scenario within LEDS and what profiles may be applied:

Scenario	LEDS Profile
A person is suspected of committing or planning to commit a criminal offence, or is subject to a civil order or restriction	'Suspect'
A person has been arrested and convicted of a criminal offence, or has accepted a police caution	'Offender'
A person has a legally enforceable restriction placed on their activities by the courts, the police or another official body with such powers e.g. a disqualified driver	'Controlled Person'
A person is sought by Immigration Enforcement because they have over-stayed their UK visa, have been refused entry into the UK or are vulnerable and have been reported missing by Immigration Enforcement (IE)	*IE may notify Police, who will create an entry into LEDS in order that the person is located.* A person may be arrested or directed to contact IE, depending on the circumstances.
A person is actively being sought because they may have information critical for an investigation or other enquiry, but not a suspect.	'Locate'
Law enforcement has a safeguarding responsibility towards a person	'Safeguarded Person'
A person is applying for, been refused for, holds or has held, a Firearms Certificate	'Firearms Licensee'
A person has been reported missing, and their details have been recorded	'Missing'

A person has reported lost/ stolen property, named as a nominated contact where there is a law enforcement safeguarding responsibility or a person is named in the content of a crime or intelligence report, e.g. a victim.	'Contacts'

The DPA requires that law enforcement data processing should strive to, where relevant, maintain a clear distinction between different categories of personal data;

- people who are suspected of having committed, or about to commit, a criminal offence (suspects) – includes arrests
- those convicted of a criminal offence
- people who are alleged or proven victims of a criminal offence (victims); and
- Individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

LEDS will maintain a separation as much as is possible between suspects and offenders from those of victims and or witnesses. The details of the later will not be returned on standards searches performed on LEDS.

In addition, the DPA states that the data collected in LEDS must be able to be distinguished between personal data based on facts from that which is based on a matter of opinion or assessment. For example, data relating to arrests and convictions separate from that of witness statements. LEDS will not be *merging* any datasets.

Processing Children's Data

On occasions, data in LEDS may relate to young children and it is possible that other data systems may include links to persons of any age and vulnerable groups.

LEDS will allow the creation of records for children under the age of ten for non-offence data, though these instances will largely be for safeguarding reasons. This data already exists in PNC, albeit in a small proportion.

The age of criminal responsibility in England and Wales is 10 years old and LEDS will not permit the creation of criminal records for anyone lower than this age.

When managing children's data, judgements need to be made on the nature and purpose of the processing involved against the potential risks it poses to children. Information intended to inform children about what happens to their personal data and their rights, will be clear and simple to understand. The Programme will liaise with the relevant children charities to further support this.

Additional audit functions will be used to ensure that access to their data is only permitted where there is a genuine reason to access that data.

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

The majority of the processing in LEDS will be under the DPA and the rights conferred in Part 3, chapter 3. However, there are some differences between Part 2 and Part 3 rights. This means that some rights are not applicable to the law enforcement purpose.

The below, details the rights and the level of controls an individual has over their own data;

- The right to be informed – the Controller has an obligation to inform individuals how their data has been obtained and detail how it will be used, retained, stored and who it will be shared with. The LEDS privacy notice will underpin this right.
- The right of access – This is referred to as the Subject Access Request (SAR) process. In England and Wales this is processed via ACRO. Members of the public have a right to access their personal data, thought exemptions apply. This means that some information cannot be disclosed, and an individual's control is limited. This right does not extend to access to information that identifies others. LEDS is not expected to introduce any new processes in the exercising of these rights. At the time of writing, the SARs process is yet to be determined for other non-police organisations who will continue to have oversight
- The right to rectification - the right allows a member of the public to request to have their personal data rectified if it is inaccurate or uncomplete. The Privacy Notice will detail this process.
- The right to erasure – Individuals, will in certain circumstances, have the right to request the deletion or removal of personal data. The Privacy Notice will detail these circumstances and the process.
- The right to restrict processing - Individuals, will in certain circumstances, have the right to request the deletion or removal of personal data. The Privacy Notice will detail these circumstances and the process.
- The right to data portability – this right relies on consent of the data owner and will not apply to data processed under part 3 DPA.
- The right to object – This right will not apply to data processed under part 3 DPA and can only be exercised where the data is being used for a non-law enforcement purpose, e.g. processing under a public task.
- Rights in relation to automated decision making and profiling – this relates to a decision made via automated means, without human involvement. Members of the public have a right to be informed about this type of processing and may request a decision be taken using human intervention. The LEDS Privacy Notice will detail if and when automated decision making takes place.

Where applicable, the Controller can restrict these rights where necessary to;

- Avoid the obstructing of an investigation
- Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences
- Protect public security
- Protect national security; and

- Protect the rights and freedoms of others.

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

While individuals may not wish criminal record and criminal intelligence data to be used in police investigations and for safeguarding purposes, they will expect that it is used. The first data protection principle requires that processing is fair and lawful. In these circumstances, personal data must be necessary and collected in a way that supports the purpose for which it was collected.

The LEDS Privacy Notice will be used to inform the public about the data being processed in LEDS. It will also explain the nature of the data captured and the individual rights over their data.

Do they include children or other vulnerable groups?

Yes. Information is stored both in relation to children or vulnerable person's criminal history and because of their vulnerability, for example, when they are victims of crime.

On occasions, data in LEDS may relate to younger children and it is possible that other data systems may include links to persons of any age and vulnerable groups. LEDS, for example, will process data where a child is suspected of being in imminent danger of a forced marriage, an abduction or of female genital mutilation.

When managing children's data, thought will be given to the nature and purpose of the processing and the potential risks that data poses to their future life chances. Information meant to inform children about their data, will be clear and simple to understand

Are there prior concerns over this type of processing or security flaws?

Yes. A number of privacy concerns have been highlighted through continued engagement with the LEDS civil society forum and other contributors. Both technical and procedural mitigations have been applied to reduce any potential impacts to members of the public (see Identification and Assessment of Risk section below).

They have been managed by applying a range of mitigations to reduce the impact on members of the public. In recent years, data breaches where personal data has been accessed and or disclosed, have become larger and their impact more widely felt.

Data principle 6, requires that controllers implement technical and organisational measures to appropriately secure the data from such breaches. For example, protecting access to the data, its loss, destruction and damage.

They will continue to be applied throughout the Programmes lifespan and into the sustainment function, where applicable. All 'high level risks' are being mitigated through the Programme governance structure, with ownership allocated where necessary. A review of all mitigations will take place in the subsequent DPIAs.

Concern is naturally raised over the data in LEDS, due to the volume of that data being processed. The focus is on how that data will be protected, who is accessing it, why as well as how to guard against scope creep. Secured hosting for LEDS has been accredited, which is a UK first. The Programme have used disclosure tools to ensure that the System Processor provides a full and detailed account of their processes. This has enabled a thorough assessment of otherwise commercially sensitive information.

All suppliers to the Programme will be required to sign a Security Aspects Letter (SAL). This document provides the specific details concerning security guidance, polices and standards which must be followed for data protection compliance.

The controller has considered completing both a Children's Right Impact Assessment (CRIA) and Family Impact Assessment (FIA). At present, it is felt that no further benefits above and beyond that supported by a DPIA would be achieved. The proportion of children data captured on PNC and PND under the ages of 18 (as compared to adults) is low and lower still for children aged 10 years and under. This position will remain under review in subsequent DPIAs.

Criminal records will be recorded for offenders aged 10-17 years old.

Is LEDS novel in any way?

Yes. LEDS will create a platform to access data currently stored separately on PNC and PND. The service offers authorised organisations and users the opportunity to store and access data from any web-enabled interface. This will mean a significant change from users who had previously accessed PNC via directly connected terminals. In LEDS, there will be no need for additional terminals. Instead users will be trained to access data via a new Web Application. LEDS will also provide an API and is being designed in line with Government Digital Service (GDS) guidelines.

.

Any relevant advances in technology or security?

The Home Offices' Enterprise Services are responsible for the overall strategic protective monitoring service across Digital Data and Technology (DDAT) with Police and Public Protection Technology (PPPT). LEDS will utilise network access controls and encryption to protect sensitive data. These will be subject to audit controls that will be used to monitor access to data. Users will be required by the service to note a purpose for accessing individuals' personal data.

A proactive and protective monitoring service will be established. This will provide visibility and understanding of LEDS data. They are tasked with ensuring an improved security risk profile for LEDS and will continue to be internally operated, developed and monitored within the Home Office until superseded by the agreed sustainment function.

Any current issues of public concern?

Yes. The two main issues of public concern are the retention of custody images and the retention of convictions. There are also less widespread, but still real concerns about the way in which the required reviews of retained data in MoPI are being undertaken

The Home Office Custody Image Review (written in response to the *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012]* in which the courts found that retaining images for non-convicted individuals was unlawful) stated that police forces should review custody images under the rules set out in MoPI.

This review has caused concern as;

a) The deletion process is manual and not automatic (DNA and fingerprints deletion are automatic); and

b) Retention periods in MoPI are longer than those in the Protection of Freedoms Act for DNA and fingerprints.

There is also increasing concern that the current 100-year rule for the retention of criminal record and arrest information is disproportionate and incompatible with the third and fifth data protection principles. This was reflected in the judgement of *Gaughran -v- The UK 2020*, which stated that appropriate safeguards must to be in place to review retention periods and considerations must relate to the seriousness of the offence. In addition, the outcome of the Judicial Review on Broadfoot is awaited and is expected to offer further assistance in this area.

Information held on children or in relation to a law enforcement contact, while under 18 years old, should be managed in alignment with MoPI.

The use of live facial recognition technology is another area of public concern. LEDS will not contain any biometric data, though HOBS will. LEDS will contain data from matching in these biometric systems and will hold biometric images by virtue of the datasets collected. For example, it will indicate a match of a nominal to an existing profile on the national DNA database (NDNAD) or the national fingerprints database (IDENT1).

LEDS will have the ability, using the HOB facial search capability, to compare one image with another uploaded image already retained within LEDS. The images, which the stored data is searched against, might originate from CCTV, social media or have been provided by friends and family (in relation to a missing person). It will not include live images from surveillance CCTV or body worn cameras. However, local forces may download any image to a local force system, in order to populate their facial identification systems. In these cases, the forces would be expected to ensure proportionality of their actions by

undertaking a risk assessment. These images are currently searched against custody image data.

Is LEDS signed up to any approved code of conduct or certification scheme (once any have been approved)?

Yes, through the Programme, LEDS will align with the following:

- The LEDS Code of Practice and Guidance Document
- The Governance Information Risk Return (GIRR) process. This provides assurance and confidence that information shared between the national policing community is trusted to be managed appropriately. Each organisation sharing information utilises similarly appropriate information risk management regimes
- BS 10008 - 'Evidential weight and legal admissibility of electronic information specification'. This standard relates to the authenticity and integrity of electronic information which may be used as legal evidence. LEDS will need to provide business data and audit data to an evidentially sound and defensible standard. A policy document is being developed for LEDS.
- ISO 27001 - Information and Security standard which is a framework that assists organisations to manage and protect their information assets.

The purpose of the processing

1. Law enforcement purposes defined as:

- 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 the public (safeguarding)
- The prevention of threats to public security.

Whilst LEDS is a system largely operated within the scope of Part 3 DPA, some processing purposes will be under the provisions of the Part 2 DPA which deals with general processing. Under Article 6 of GDPR, a lawful basis must be identified before processing of any personal data. Processing operations are described above. There are 6 lawful bases for processing:

2. General Processing

- Where the individual gives their explicit consent
- To meet contractual obligations entered into by the individual
- To comply with the Controllers legal obligations
- To protect individual's vital interests
- For tasks performed in the public interest or exercise of authority vested in the Controller
- For the purpose of legitimate interests pursued by the Controller
- In circumstances of significant public interest and for the purposes of public safety

Any basis of processing must have a clear basis in law and must also be documented. The public interest processing basis will largely apply to Part 2 data. In these cases, individuals will be unable to rely on the data rights of erasure and data portability, however it does not affect their right to object to the processing.

Other applicable processing basis include processing data for a legitimate interest, under Article 6 (1) (f). The burden is on the Controller to demonstrate its interests in processing the data are legitimate. This basis is most likely to be used where the individual would deem it reasonable and where there is likely to be minimal impact on their privacy, e.g. where the individual is a child.

The LEDS Privacy Notice will be used to clearly identify the purposes of processing personal data within LEDS.

What does LEDS want to achieve?

LEDS is designed to allow more effective national data sharing to support law enforcement and safeguarding purposes. It will do this by allowing user organisations to have better

opportunities to access and share data. This will support operational objectives and priorities, as derived from Part 3 s.36(3)(b) DPA.

The intended outcome for individuals

LEDS will benefit the public in the following ways:

- Improve public safety - LEDS allows risks to the public to be identified and mitigated
- More successful prosecutions - LEDS offers a comprehensive evidential tool and reduces the burden on officers
- Better operational outcomes - LEDS provides new opportunities to detect, prevent and disrupt crime
- Improved public safeguarding - As with reduced risk to officers, additional risks to the public can be identified and actioned, improving safeguarding; and
- Access to individual data will be specifically tailored to organisations and any potential impacts on data breaches are significantly reduced

What are the benefits of the processing – for law enforcement, and more broadly?

There are also operational benefits that will be realised when LEDS is delivered and in use, these include;

- Operational performance outcomes that link to law enforcement objectives
- Increased service availability - A more stable solution, LEDS will have greater resilience and availability than the current solutions, avoiding the debilitating impacts of a loss of service to law enforcement organisations
- Reduced time to make changes - With reduced complexity, the system can be changed/updated more quickly and cost-effectively
- Back office data processing costs reduced - centralised automation will reduce the amount of time analysts will need to spend processing data
- Back office time saved - are various opportunities to save time in the back office, for instance by improving the evidential base that analysts can work with, reducing the time needed to complete some investigations
- Front line time saved - officers will save time from more efficient ways of working, for example by reducing the time taken to confidently verify a person's identity
- Reduced risk to front-line officers - With richer, more timely information available to front-line officers, additional risks can be identified and mitigated or avoided before the officer is put in harm's way
- Reduced central technology operating costs - LEDS costs less to policing than PNC and PND; and

- Reduced national technology operating costs - the LEDS solution will be less expensive to operate than the current PNC and PND solution, reducing annual IT operating costs compared with current levels.

The expected benefits for a society as a whole

Improvements in relation to all the above purposes will generate benefits for society as a whole. They will be collected within a value model, with the intention to publish in the future, as appropriate.

Consultation process

Describe when and how you will seek individuals' views?

While we will not be consulting on LEDS or on this Data Protection Impact Assessment. A three-month public consultation on the LEDS Code of Practice has recently concluded. This was led by the College of Policing. It marks the first formal opportunity members of the public have had to review LEDS. A formal public response will be issued.

Who else does LEDS need to involve within the organisation?

The LEDS Programme Board is chaired by the National Senior Information Risk Owner (SIRO) for policing who are ultimately responsible for any risks as data owners. The National SIRO underwrites any risk to police owned data.

The Business Design Authority (BDA) consists of representatives from key stakeholders. These includes Court Service, Border Force, Immigration Enforcement, NCA and Disclosure and Barring Service. The forum is chaired by the NPCC PNC lead.

The Home Office Data Board provides top level oversight of the data strategy, policy and governance across the Home Office. The ODPO refer the highest risk DPIAs to the board for review. Home Office Legal Advisers, Policy and the Press Office will also be involved in the approval process. Upon the advice of the ODPO, the Home Office has strived to ensure that the controllership of LEDS data remains a priority for resolution, especially when noting the number of controllers and processors LEDS involves. This informed the approach to manage ownership in relation to the individual flow of data. They have also provided advise on the accessibility of individual data rights and controller responsibilities.

The Minister of State for Policing and the Fire Service and Minister for London will provide ministerial sign-off, before its publication.

This will be a continual process of consultation for the DPIA.

The proposed governance structure for LEDS

Once completed as a programme, LEDS will become 'live' and will be managed as a business function. A sustainable design to develop the people, processes and tools that will eventually take over LEDS is currently underway. The existing PND, PNC and LEDS governance approach will be replaced with a single, national provision. They will be responsible for determining the process by which to grant access and for ensuring regular reviews take place for data access and organisations adherence to data protection.

A Target Operating Model and LEDS Sustainment Strategy is in development. As part of this, three overriding principles of the governance structure have emerged and continue to evolve;

- LEDS will be a collaborative venture between the Home Office and law enforcement
- LEDS will adopt a pragmatic and collaborative approach to knowledge and skills transfer, working to a joint set of sustainment objectives; and
- LEDS beneficiaries should contribute towards its maintenance

The proposal is that the accountable service owner should remain within the Home Office Digital Data Technology directorate (HODDaT). Service ownership would potentially rest with the Police and Public Protection Technology (PPPT) IT Director.

An exception to this would be LEDS training. Training and tradecraft functions are due to be managed by PPPT IT but designed and delivered through the College of Policing. The scope is expected to include non-police organisations and processes developed to assure the completion of the relevant training. These details are still being developed compliance with the training package is likely to form part of data sharing agreements. The proposed governance structure continues to evolve, though it is expected that the eventual solution will be resourced by users, law enforcement staff as well as civil servants

All user organisations will be required to appoint a Senior User who will be responsible for the use of LEDS within their organisation.

Who else within the Home Office has access?

The Home Office is a named competent authority under schedule 7 DPA. Levels of access for these Home Office departments will be dependent on the specific business requirements and any statutory obligations that they may need to fulfil

A list of all Home Office units currently using PNC data is available in Appendix D.

Immigration Enforcement and LEDS

LEDS is not concerned with why a person is lawfully in the UK. Therefore, no profile will be created or maintained on LEDS simply because a person does not have settled status in the UK.

LEDS data can and will be accessed by authorised member of the Home Office's Immigration Enforcement. They use the Home Office's legal powers, under the Immigration (European Economic Area) Regulations 2016. For example, where Immigration Enforcement have not been able to trace a person through routine enquiries, they will notify the Police. The Police will create an entry on LEDS to circulate a person's details. They can access data relating any of the roles within LEDS, e.g. as a suspect, offender or controlled person. This also includes access to markers on a person relating to

their welfare as well as other warming indicators, e.g. where they may have previously absconded or are violent.

Immigration Enforcement can access information relating to any EA national seeking settlement, if they have had a custodial sentence and may be subject to removal from the UK.

Unless it was a relevant factor, no immigration status for victims and or witnesses would be visible to Immigration Enforcement in LEDS.

The recent code of practice for victims of crime stresses that the foremost concern should be treating victims as victims, reducing further victimisation by systems and processes. LEDS will not make victim data routinely searchable to users without a justification.

Being a victim of crime is not a valid reason, on its own, for a profile to exist in LEDS.

The DPIA will continue to monitor plans as they emerge in this area.

Consulting information security experts, or any other experts?

Yes. There is a security team within the Programme which access external security teams. The security functionality of all organisations will be managed nationally via the NPIRMT.

All forces and law enforcement organisations with access to national networks and systems must complete an annual GIRR. Compliance with the GIRR assures that information shared between connected organisation and accessed on national networks and systems, will be appropriately protected. This confirms that no additional risks will be introduced into the wider policing community and is aligned with ISO 27001.

Within the Home Office, security governance expertise is provided through the Security Working Group, which serves as the primary information assurance management function. They brief the National Police Accreditor and are responsible for seeking guidance and approvals as required.

Consultation that is relevant to this development

Where it is feasible, the DPA asks that controllers consider consulting directly with members of the public when processing personal data.

The Programme has worked alongside the civil society forum in order to best achieve this end. These representatives assist with the development of LEDS, ensuring that ethical considerations of the data continue to take prominence. The forum provides a safe space for discussions of ideas, concerns with a view to increasing data protection and individual rights.

The ODPO have also provided advice and assistance on data protection. In particular, they have given advise on Controllers, joint-controllers and processors. They have also provided advise on the LEDS privacy documentations.

Assessment of necessity and proportionality – compliance and proportionality measures

What is the lawful basis for processing?

The processing of data must be lawful. The controller is responsible for establishing that the processing is based in law.

There are 6 lawful bases for processing data under Article 6(1) and at least one will apply in order to comply with the principles of lawfulness and accountability;

- The consent of the data subject
- Performance of a contract
- Compliance with a legal obligation
- Necessary to protect the vital interests of a person
- Necessary for the performance of a task carried out in the public interest
- In the legitimate interests of organisation (except where those interests are overridden by the interests or rights and freedoms of the individual).

As controllers, the Home Office and Polices forces perform multiple functions. Therefore, in certain circumstances, data processed initially under Part 2 DPA may, at a later stage and upon evidence, become necessary for a law enforcement purpose. For example, an investigation after the initial report of a missing person. The data will then be processed as part of a lawful basis, under Part 3 DPA. There are only two lawful bases for processing under Part 3; the processing must either be:

- for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security or;
- with the consent of the data subject.

This change of purpose poses significant implications on individual data rights. Namely, that change in purpose, impacts the level of control individuals have over their data. controllers must be able to clearly demonstrate which lawful basis is being relied upon at all times, if queried. This must not be retrospectively applied.

This lawful basis should put individuals in control and build better trust between law enforcement and the public. Consent will not always be the most appropriate basis to use for processing data but where it applies, the controller must make a clear and transparent consent request. The data subject must be given an ongoing choice about what happens to their data and be informed about how data will be used. Individuals can request the deletion of their data after withdrawing consent.

The LEDS Retention Policy will detail how data will be reviewed and refreshed.

Table No.6 shows the lawful basis for processing data under Part 2 DPA;

Policing function (Controllers)	Personal Data	Lawful Bases	Conditions
Gather information that may support law enforcement objectives	Yes	public task 6(1)(e)	public interest
Building links in the local community to engage, reassure and support	Yes	consent 6(1)(a)	explicit consent
Work in partnership with others/general stakeholders	Yes	public task 6(1)(e)	public interest
Effectively engage with victims, witnesses and the vulnerable to provide initial support and direct towards relevant services	Yes	public task 6(1)(e)	public interest
Maintain awareness of potential risks to individuals	Yes	public task 6(1)(e) *this function may be subject to a change of purpose.	public interest
Gather and handle information, intelligence, and evidence, from a variety of sources, in line with legislation, policies and guidance	Yes	public task 6(1)(e)	public interest
Criminal offence data	Yes	public task 6(1)(e)	‘official authority’ of the Police

Article 8 ECHR

The European Convention of Human Rights, via the Human Rights Act 1998, introduced the concept of the respect for private and family life. Article 8 states that there shall be no interference by a public authority with the exercise of this right except 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 Courts in *R (Bridges) v CCSWP and SSHD [2019]* stressed that when using technology, it was important to pause and consider the potential impact upon privacy rights. It 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."

Article 8 rights are not absolute rights and any interference will 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],* 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."

The legal framework in which the LEDS operates comprises a number of elements in addition to the Common Law, namely:

- Primary Legislation – The main legislative guidance is DPA 2018.
- Secondary Legislative Instruments - A draft Statutory Instrument entitled the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 is being developed. Once this is laid before Parliament, it will enter into UK law.
- LEDS Code of Practice and Guidance document – After consultation, this is expected to be laid before Parliament in late 2020; and

- National Standards and Policy – There are national retention policies for data management as well as those for managing risk to data and audits, mentioned above.

Sections 29(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 place when processing sensitive personal data. LEDS will also publish have a LEDS Privacy Notice.

A national audit capability has been established that will oversee local provisions for audit and monitor compliance. The joint-controller agreement also includes measures to support consistent compliance and the management of data rights.

The fifth Principle requires ongoing monitoring and review of processing. LEDS data will be deleted in line with policy, taking account of any assessment such that it is retained for a continued policing purpose. This is in accordance with MOPI.

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

Yes. Processing personal data on a national level via LEDS will serve to achieve the law enforcement purpose, described above.

Is there another way to achieve the same outcome?

No. LEDS fulfils the Government's strategy on law enforcement and supports the benefits noted above. It is not possible to protect the public, arrest and prosecute suspects without police intelligence being made available at the point of need to the police and other authorised law enforcement or safeguarding organisations.

What are the conditions for undertaking sensitive processing?

Processing for law enforcement purposes must be strictly necessary and satisfy one of the eight conditions for sensitive processing in schedule 8 DPA or obtained by consent. These are also mentioned above.

How will you prevent function creep?

One way to combat function creep is to adopt data privacy by design. All organisations deemed controllers will be required to maintain local DPIAs. They will have an audit capability and a disciplinary policy in place. This could potentially be used in investigations but will depend upon the structure of each organisation as well as their internal disciplinary process.

The LEDS Business Change function and associated readiness activities will ensure that all the necessary pre-requisites are all in place before any authorised access to the data on LEDS is allowed.

In addition, a governance process will be designed and established after delivery. This function will provide a national governance approach. It is expected to improve efficiency in the use of existing resources, increase public safety outcomes, support transparency and legal compliance obligations.

The controllers are committed to producing the LEDS DPIA annually. It will be a living document and will continue to raise any data protection concerns.

Data quality, consistency and retention

High quality data are key to any successful implementation and the realisation of benefits from LEDS. This is helped by ensuring that any data collected is fit for purpose and used for the purpose for which it was intended. It should meet the expectations of those involved in the process. The controllers will ensure that the appropriate agreements, policies, guidance and procedures are in place prior to any processing of data. This is supported by Information Asset Owners and data stewards and DQ reports to identify issues.

How do you intend to ensure data quality and minimisation?

In accordance with the Principles, the Home Office and NPCC will be responsible for ensuring organisations put in place measures to ensure that the data in LEDS is accurate and correctly entered. Data quality will remain the primary responsibility of all controllers at the entry level.

The Programme will utilise a dashboard product and apply a data quality maturity model. This is a quality improvement tool which has been specifically created for LEDS. It is a detailed business change process, requiring the Police to change the way they think about the data they hold and to explicitly consider the quality of data that will be uploaded and subsequently shared on a national level in LEDS.

It will improve the quality of data migrated onto LEDS by identifying records, based on an assessment of risk to public protection. With robust management of the tool, it will;

- Highlight poor quality data and support police forces in implementing data quality improvement programmes. This will be largely legacy data.
- Support effective use of data by working closely with police forces to understand the value that these important datasets represent. This maximises both technical and cultural solutions for improving data quality; and
- Ensure that any use of data is undertaken within the legal and regulatory framework.

The Home Office will be responsible for collecting and reporting on data quality, providing feedback to all organisations. This will be based on nationally agreed minimum data standards.

How do you intend to provide privacy information to individuals?

Working with the NPCC and other controllers a Privacy Notice will be produced outlining:

- the details of the controller(s)
- the details of the DPO
- the right of access by the individual
- the legal basis for processing
- the type of data held
- who has the data been disclosed to
- the period of retention
- the right to make a complaint
- the right to rectification of inaccurate data; and
- the rights in relation to automated decision-making and profiling.

Restrictions to the provision of these privacy information, must be necessary and proportionate. It must be justified in reference to one of the conditions in s.44(4) DPA.

What measures do you take to ensure processors comply?

It is the controllers' responsibility to ensure that the processors comply with the sixth Principle, by safeguarding access to the data. As such it will:

- Set rules for access - Access to the data in LEDS and the systems will be based on the classification of the information, system criticality and appropriate business need to access the data. Security controls will be applied using a risk-based approach, concentrating on protecting the most important data and business activities.
- Set rules for onward sharing – data processing contracts will be used to manage the requirements and expectations of all processors and 3rd party suppliers.
- Require an audit regime to be set up - Access to, and use of, audit tools that interact with LEDS will be segregated and access restricted to prevent inappropriate disclosure and tampering of log data. Implementation of BS10008 [10] is underway within the programme. All relevant data is available in a single location for security teams to access and analyse.
- Enforce security standards – The Programme has established the LEDS-NIAM Integration Working Group responsible for the requirements for the NIAM delivery. They will report back into the Security and Infrastructure workstream and the NLEDP Security Working Group.
- Inspection against national auditors – Security functionality of all organisations will be managed nationally by the NPIRMT. All forces and agencies with access to the national networks and systems must complete an annual risk return to ensure continued access to LEDS.

- The LEDS Code of Practice and Guidance Document will discharge statutory responsibilities to monitor on relevant police forces and require all other organisations to take it into account.
- Organisations are likely to be inspected by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), as is currently the case.

A processor shares much of the accountability for the data processing. A data processing contract will be in place to manage these relationships. Like controllers, they are obliged to keep records of all categories of processing activities, including details of:

- the controller and any other processors
- processing categories
- international transfers
- general description of technical and organisational security measures.

The Home Office are building the technical capability for logging access and all relevant processing activities into the platform as required by law. This will enable those with the responsibility for conducting audits. By delegation, from the Home Office, the National Systems Audit Team will proactively maintain data security, integrity, drive compliance and support the investigation of malpractice.

Contracts will be reviewed regularly by the agreed LEDS sustainment body.

How do you safeguard any international transfers?

Jersey, Guernsey and Isle of Man are overseas jurisdictions for the purposes of data protection and will access the data in LEDS via agreements.

Well established protocols for transfer of data to Europe already exist via the Schengen procedure and there are appropriate safeguards in place in relation to that data. It provides access to the European Schengen Information System and supports a wide range of law enforcement checks and border controls.

The NCA currently manage Schengen enquiries, on behalf of the UK. The effects of the UK leaving on this service is yet unknown. Further developments will be reflected in future DPIAs.

Controllers may be party to international agreements in their own right. It may involve disclosures to other international law enforcement agencies. This includes those concerned with the safeguarding of international and domestic national security. Where this is the case, an agreement will be in place, as well as publicly detailing how that data is to be internationally protected from misuse.

Safeguarding access to the system

Under Part 3 DPA, there is a general obligation to implement appropriate technical and organisational measures to comply with the principles of data protection into processing activities.

LEDS has been accredited as OFFICIAL. This includes the Governments Security Classification (GSC) caveat, OFFICIAL-SENSITIVE. A technical security risk analysis was conducted, to identify the specific controls required and an Information Risk Assessment Report (IRAR) has been developed. This was overseen by the National Accreditor. LEDS will need to meet the needs of multiple law enforcement organisations, with varying degrees of access to the data.

Safeguarding access to the data

The LEDS business rules define who accesses the data in LEDS. This will be in place prior to the processing of data by other organisations. Data will be made available based on a range of techniques, including being a member of the appropriate user group with the correct user ID and a data review process.

The Security Operating Procedures (SyOps) will set out the generic minimum requirements that must apply to the access and administration of LEDS setup. It will apply to all users involved in the production, development and testing of LEDS, including administrators, developers and auditors. The SyOps, will enable the programme to implement a secure service in accordance with the sixth data principle. It must be read and signed by all resources involved in LEDS, informing them of their responsibilities towards the system and the data. Once signed, acts as a formal acceptance of data protection obligations.

Auditing use of LEDS

In addition to securing access to the system and to the data within that system, LEDS will include auditing capabilities that will deter misuse. Where misuse does happen, it will help to identify and provide evidence. All activities within the system and access to it, will have a mandatory logging functionality. This is in accordance with s.62 DPA.

Logs for LEDS will be kept for at least the:

- Collection
- Alteration
- Consultation
- Disclosure (including transfers)
- Combination; or
- Erasure

This will include the details of searches and other data retrieval, for what was done and when it occurred.
In addition to identifying misuse of access rights, the audit provisions will help to identify any unauthorised attempt to access data from an external source or attempts to by-pass access controls from within the approved users. The log will be available to local auditor's, national auditors and the ICO, if requested.

The activities of auditors, themselves, will be logged and subject to audit by the national auditors.

Identification and assessment of LEDS 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.	Some organisations with access to law enforcement data are not named specifically as competent authorities (Sch. 7 DPA 2018) and may not have a statutory function which brings them into scope of the meaning of a competent authority	Possible	Severe	High
2.	Police data is currently operating between several retention /deletions policies [PNC 100yrs rule & MoPI]. These data sets have rules which LEDS will continue to enforce. There is a risk that some of the police retention rules will be deemed inadequate for a modern service or fail to be applied correctly in all instances.	Possible	Significant	High
3.	There are risks that processing in LEDS will impact data quality and accuracy, in particular; a) That data is not accurate (accuracy) b) That data has not been entered in time (timeliness) c) That data which should have been deleted has not been deleted (currency). This is due to the fact that LEDS is getting data from other local & national systems. There may be different working practices that have emerged over time. There may also be other variables that impact how that data is treated locally.	Probable	Significant	Medium
4.	Other organisations, asides the Police forces/staff have the ability to create and amend records in LEDS. For example, other prosecuting agencies can create and update data in LEDS after making an arrest or issue warning markers.	Probable	Significant	High

5.	There is a risk that individuals will be unable to exercise their data rights over their own data in LEDS. Processing LEDS data will also fall under Part 2 DPA/GDPR and differential processing regimes may mean that SARs are not responded to correctly or in time.	Possible	Significant	High
6.	There is a risk that the printing capability available in LEDS could lead to data being accessed by those without authority as a result of prints being lost or misplaced.	Possible	Significant	High
7.	LEDS will be linking data from multiple sources, including data relating to convictions and intelligence data. There will be a risk to data if LEDS users are unable to adequately distinguish the various types of data. DPA requires that where possible, LEDS should distinguish fact from opinion data.	Possible	Significant	High
8.	There is a risk that data relating to vulnerable groups in society, e.g. children, disabled, mentally impaired etc. will not be adequately protected from authorised users seeking to take advantage of their access to the data. Children are specifically singled out under DPA/GDPR.	Possible	Significant	High
9.	There is a risk that personal data, accessed by officers on the streets via mobile devices, could be compromised if these devises are lost or stolen. (Devices are owned by the issuing forces).	Possible	Significant	High
10.	There is a risk that members of the public will not know how or where to access their personal data rights due to number of organisations and data roles involved.	Possible	Significant	High
11.	The Home Office are named as a competent authority in the DPA, however, it is a large government department, performing many functions - from immigration services to data quality/analysis. Some functions will also be able to input into LEDS.	Possible	Significant	High

12.	With large amounts of data being hosted and accessed via LEDS there is a risk that data minimisation will be difficult to implement all of the time. The purpose for processing data must be explicit.	Possible	Significant	High
13.	There will be multiple ways of accessing the LEDS platform. Not all organisations will be utilising the Programmes preferred access route: Application Programming Interface (API). This route increases data integrity. as it offers the most up-to-date data exchange. (LEDS will continue to provide access to batched data, whilst promoting API).	Probable	Minimal	low
14.	There is a risk that increasing numbers of commercial companies gaining access to the data on LEDS. This could lead to scope creep if remits are not tightly defined.	Remote	Minimal	Low
15.	There is a risk that the training for LEDS will be take longer than anticipated. This is because of the number of users/organisations accessing/using the data on LEDS.	Probable	Significant	Medium
16.	There is currently no process in place for reviewing and deleting court convictions on PNC. Agreement for LEDS processing of convictions needed between Home Office, MoJ, Court Services & Probation Service.	Probable	Minimal	Low
17.	There is a purpose limitation for DVLA driver data used by Police - They are permitted to access driver licence data when it is in relation to an offence under the Road Traffic Act 1988 – Greater clarity is required to avoid risks to data protection.	Probable	Significant	Medium

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.	Some organisations with access to law enforcement data are not named specifically as competent authorities (Sch. 7 DPA 2018) and may not have a statutory function which brings them into scope of the meaning of a competent authority.	The LEDS data access review will examine all organisations with current access to PNC data with a view to establishing the purpose of their access. Data agreements will be used to manage specific data responsibilities.	Eliminate	Low	Yes
2.	Police data is currently operating between several retention /deletions policies [PNC 100yrs rule & MoPI]. These data sets have rules which LEDS will continue to enforce. There is a risk that some of the police retention rules will be deemed inadequate for a modern service or fail to be applied correctly in all instances.	Policy unit will draft recommendations for managing data retention in LEDS, based on data retention protocols set by the National Police Chiefs' Council. This will enable the technical build to continue until an agreement has been achieved. LEDS is being designed to be technically adaptable so it can adopt the rules as agreed. Impact of caselaw on LEDS date retention, e.g. Broadfoot judicial review, will continue to be monitored.	Reduce	Medium	Yes

3.	There are risks that processing in LEDS will impact data quality and accuracy. In particular; a. That data is not accurate (accuracy) b. That data has not been entered in time (timeliness) c. That data which should have been deleted has not been deleted (currency). This is due to the fact that LEDS is getting data from other local & national systems. There may be different working practices that have emerged over time. There may also be other variables that impact how that data is treated locally.	The data quality and improvement process will assure local data quality before it is migrated onto. This will increase data consistency and conformity across wider law enforcement. The 6 data principles will guide LEDS development and policy and procedures will be implemented to improve the service. The implementation of the Code of Practice will help to define what quality means and any associated expectations from all data owners. The data contracts/agreements will also be used to define controller roles and expectations.	Reduce	Low	Yes
4.	Other organisations, asides the Police forces/staff have the ability to create and amend records in LEDS. For example, other prosecuting agencies can create and update data in LEDS after making an arrest or issue warning markers.	Only controllers of the data can authorise changes. Controllers must be consulted beforehand and abide by their contracts. The data contracts/agreements will also be used to define controller roles and expectations.	Eliminate	Low	Yes
5.	There is a risk that individuals will be unable to exercise data rights over their own data in LEDS. Processing LEDS data will also fall under Part 2 DPA and differential processing regimes may mean that SARs are not responded to correctly or in time.	Individuals data rights will be detailed in the LEDS Retention Policy, Retention Schedule, DPIAs and Privacy Notice. ACRO are likely to continue to process SAR's for Police forces. LEDS will have a dedicated web page aimed at assisting members of the public with their rights. Links	Reduce	Low	Yes

		to the available options will be provided.			
6.	There is a risk that the printing capability available in LEDS could lead to data being accessed by those without authority as a result of prints being lost or misplaced.	Printing capabilities will only be available where it supports a business need. This will be assessed as part of the data review of all organisations. LEDS will ensure that where necessary data continues to be shared as PDF files in order to create an audit trail. Prints will contain a watermark on all pages, noting the source of the data so it can be easily traced. The 'copy and paste' functionality will be disabled – to avoid printing work arounds. Training will contain modules on protecting data when printing from LEDS.	Reduce	Medium	Yes
7.	LEDS will be linking data from multiple sources, including data relating to convictions and intelligence data. There will be a risk to data if LEDS users are unable to adequately distinguish the various types of data. DPA requires that where possible, LEDS should distinguish fact from opinion data.	LEDS will not be 'merging' individual's data together. The data display will clearly show what & who it relates to, e.g. a person as victim, witness or suspect etc. The retention policy & retention schedule will regulate how both types of data will be managed. This will limit access to data where the purpose is no longer relevant.	Eliminate	Low	Yes
8.	There is a risk that data relating to vulnerable groups in society, e.g. children, disabled, mentally impaired etc. will not be adequately protected from authorised users seeking to take advantage of their access to the data. Children are	All users accessing data must populate a justification box. No access will be granted without this information, which will inform the auditing process.	Reduce	Low	Yes

	specifically singled out under DPA/GDPR.	Role-based access controls in LEDS will mitigate the risk of unauthorised access through analysis of log files, accessible by those with the right permissions, e.g. supervisory role. The audit logging levels within LEDS application are enough to allow National Auditors early visibility of any abnormal usage. LEDS will have a mandatory logging functionality in accordance with s.62 DPA. Only Auditors with the LEDS audit role will be able to see audit data.			
9.	There is a risk that personal data, accessed by officers on the streets via mobile devices, could be compromised if devises are lost or stolen. (Devices are owned by the issuing forces).	The roles management system will have a maximum lockout period. Once reached, access to the data will be terminated. Personal data will not be stored on local devices beyond the live user sessions. Devices stops working if it is more than a certain distance from an officer (implemented by some forces).	Accept	Low	NA
10.	There is a risk that members of the public will not know how or where to access their personal data rights due to number of organisations and data roles involved.	ACRO are likely to process SAR's for Police forces in England & Wales. Individual data rights will be detailed in the LEDS Retention Policy, Retention Schedule, DPIAs and Privacy Notice.	Reduce	Low	tbc

		A separate GOV.UK website will be created solely for LEDS - this is where the DPIA will be stored and where members of the public can access their rights. This space will store LEDS: DPIAs, Data Retention Policy, Data Retention Schedule, Privacy Notice, Code of Practice & other relevant documents. All appropriate links will be available, including information on Subject Access Requests (SARs).			
11.	The Home Office are named as a competent authority in the DPA 2018, however, it is a large government department, performing many functions - from immigration services to data quality/analysis. Some functions will also be able to input into LEDS.	See appendix D – for a full list of Home Office units with access to LEDS Data. A data access review is being conducted on all units to ensure full compliance.	Reduce	Medium	Yes
12.	With large amounts of data being hosted and accessed via LEDS there is a risk that data minimisation will be difficult to implement all of the time. The purpose for processing data must be explicit.	A Privacy Notice will be created for LEDS, detailing how the controllers will apply the data processing principles. A list of all organisations accessing LEDS and their purposes will be made available as part of the DPIAs supporting documentation.	Reduce	Medium	Yes
13.	There will be multiple ways of accessing the LEDS platform. Not all organisations will be utilising the Programmes preferred access route: Application Programming Interface (API). This route increases data integrity. as it offers the most up-to-date data exchange. LEDS will continue to provide access to file extracts, whilst promoting API.	Access is via SRG & the integration gateway. The Programme is investing in updates to SRG to enable it to continue to act as an intermediary into LEDS API. LEDS will now access DVLA data via an API, instead of batched data extracts as originally proposed. This is an	Reduce	Medium	Yes

		example of good LEDS practice. Data Processing Agreements & the Code of Practice will inform data users about their obligations. Much of the batched data relates to stolen vehicles sent regularly.			
14.	There is a risk that increasing numbers of commercial companies gaining access to the data on LEDS. This could lead to scope creep if remits are not tightly defined.	See appendix A. Some commercial organisations will be permitted access (depending of their specific business needs). They will perform a public functions/law enforcement/safeguarding purpose.	Reduce	Low	Yes
15.	There is a risk that the training for LEDS will be take longer than anticipated. This is because of the number of users/organisations accessing/using the data on LEDS.	The Home Office are working to complete the training requirements. Also working to provide guidance on continuing professional development requirement. The Business Change team is well engaged with stakeholders and a plan has been approved for transitioning organisations onto LEDS. Each organisation will be allocated a local implementation manager who will act as a conduit.	Reduce	Medium	Yes
16.	There is currently no process in place for reviewing and deleting court convictions on PNC. Agreement for LEDS processing of convictions needed between Home Office, MoJ, Court Services & Probation Service.	The introduction of LEDS retentions reviews, conducted by the data controllers, is likely to address this risk.	Accept	Medium	NA

17.	There is a purpose limitation for DVLA driver data used by Police. They are permitted to access driver licence data when it is in relation to an offence under the Road Traffic Act 1988 – Greater clarity is required to avoid risks to data protection.	Home Office Policy are making the necessary enquiries to reduce this risk to data and provide greater clarity.	Accept	High	NA

Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Data Protection Officer advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	A review should be carried out on each release of functionality	The DPO should also review ongoing compliance with DPIA

Appendix A
A list of organisations with access to LEDS[3]

Geographical police forces (UK)

Avon & Somerset
Bedfordshire
Cambridgeshire
Cheshire
City of London
Cleveland
Cumbria
Derbyshire
Devon & Cornwall
Dorset
Durham
Essex
Gloucestershire
Greater Manchester
Hampshire
Hertfordshire
Humberside
Kent
Lancashire
Leicestershire
Lincolnshire
Merseyside
Metropolitan
Norfolk
North Yorkshire
Northamptonshire
Northumbria
Nottinghamshire
South Yorkshire
Staffordshire
Suffolk
Surrey
Sussex
Thames Valley
Warwickshire
West Mercia
West Midlands
West Yorkshire

[3] This is subject to the outcomes of the data access review

Wiltshire
Dyfed-Powys
Gwent
North Wales
South Wales
Police Scotland (including national support systems)
Police Service of Northern Ireland

Non-geographic police
British Transport Police
Civil Nuclear Constabulary
Ministry of Defence Police
National Crime Agency (domestic and international)

Local Police (limited access)
Mersey Tunnels Police
Port of Liverpool Police
Port of Tilbury Police

Policing oversight and Inspections
Independent Office for Police Conduct
College of Policing

Safeguarding and disclosure
Access NI
ACRO Criminal Records Office - Hampshire Police
Children and Family Court Advisory and Support Service (CAFCASS)
Disclosure and Barring Service (DBS)
Disclosure Scotland
Gangmasters and Labour Abuse Authority

Investigations and prosecutions
Competition and Markets Authority
Service Police Crime Bureau (Royal Military Police)
Trading Standards (national role)
Charities Commission for England & Wales
Scottish Society for the Prevention of Cruelty to Animals

Justice
Criminal Cases Review Commission

Travel infrastructure
Highways England
Driver and Vehicle Standards Agency

Driver and Vehicle Licensing Agency
National Ports Office - Met Police
National Air Traffic Services Ltd
Marine Management Organisation

Health and social security
National Health Service Counter Fraud Authority
Health & Safety Executive
Medicines and Healthcare Products Regulatory Agency

Postal Infrastructure security
Royal Mail

Environment
Environment Agency
Natural Resources for Wales
Scottish Environment Protection Agency

Finance
Financial Conduct Authority
HM Revenue & Customs
Serious Fraud Office

Government Departments and Organisations
Cabinet Office
Department for Work & Pensions
Houses of Parliament (Commons and Lords)
National Assembly Wales
Home Office

Commercial Organisations
Datatag ID Ltd
Live Stream Data Systems - (ANPR systems provider)
HPI
Experian
The Gun Trade Association
RetainaGroup
Total Car Check limited
UK Vehicle Limited
Vehicle Information Services (CDL)
Verisk Insurance Limited

Non-police prosecuting authority
Insolvency Service

Government department
Ministry of Justice
Her Majesty's Prison and Probation Service

Intelligence Agencies
GCHQ (Government Communications Headquarters)
MI6
MI5

International Organisations
Guernsey Police
Isle of Man Police
States of Jersey Police
Jersey Customs and Immigration Service
Jersey Financial Services Commission

Appendix B
A list of organisations with indirect access to LEDS data – serviced by ACPO Criminal Records Office

ACRO Serviced

Cygnet Hospital, Clifton
Civil Aviation Authority
DEFRA - Department for Environment, Food & Rural Affairs
Department of Health and Social Care Anti-Fraud Unit
Eastern Inshore Fisheries and Conservation Authority
Edmonds Marshall McMahon
Food Standards Agency
Gambling Commission
Maritime and Coastguard Agency
Office of Communication
Office of Rail Regulation
Royal Society for the Prevention of Cruelty to Animals
Royal Borough Kensington and Chelsea Council
Security Industry Authority
TM Eye Ltd
Prudential Regulation Authority – Bank of England
Unregistered Schools Taskforce (UST) Ofsted
Education Workforce Council
General Dental Council
General Optical Council
General Pharmaceutical Council
General Teaching Council Northern Ireland
Information Commissioner's Office
Teaching Regulation Agency
Nursing & Midwifery Council
Social Care Wales
General Osteopathic Council
Judicial Appointments Commission
The National Gallery
Office of the Immigration Services Commissioner
Cabinet Office
Ministry of Justice
Office of the Biometrics Commissioner
Archbishop of Canterbury
US Embassy

Appendix C
Sources of LEDS data

Police Force Custody Interfaces
Motor Insurance Database Web Service
National Firearms Licensing Management System
Home Office Violent and Sexual Offenders Register
Home Office - National DNA Database
Home Office - Schengen Information System
Home Office - Fingerprint system
Bichard 7 – Ministry of Justice Criminal Justice Secure Exchange
Disclosure and Barring Service - Barring List
Driver license, vehicle data, trade plates disqualified driver data
Ordnance Survey
Society of Motor Manufacturers and Traders
Motor Cycle Industry Association
Schengen Linking Alerts Services
PNC Data inputters
Local Police Force systems

Appendix D
A list of Home Office units with access to data in LEDS

Home Office

Home Office - Borders Force
Home Office - UK Visa's & Immigration
Home Office – Immigration Enforcement
Home Office - Forensic Information Databases Service
Home Office - Football Unit
Home Office – Office for Security and Counter-Terrorism