NLEDP Privacy Impact Assessment Summary

May 2018

1 National Law Enforcement Data Programme

The National Law Enforcement Data Programme (NLEDP) is replatforming the currently separate Law Enforcement data systems, the Police National Computer (PNC) and the Police National Database (PND), onto a single technology platform under the name of the Law Enforcement Data Service (LEDS).

The intention is to support Law Enforcement and other competent authorities with current and joined-up information, on-demand and at the point of need, in order to prevent crime and better safeguard the public.

The key objectives of the Programme are to deliver a LEDS that will:

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

PNC and PND datasets will co-locate onto LEDS to improve accessibility for those users who need access to the suite of data sets. Security provision will be put in place to ensure that users who only need to access specific data sets are not able to access all the merged data. Law Enforcement will have an enhanced set of national information accessible, for the first time, through a single system. Benefits will include faster and improved searching of records, better identification of individuals and more effective information sharing between law enforcement and other authorised organisations.

Background

The PNC was introduced in 1974 and holds personal data and other information relating to individuals (known as 'nominals') including arrests, charges and court disposals (including convictions), together with other information about vehicles and property. Organisations with access to the PNC directly upload data to the central dataset.

The PND was introduced in 2009 and receives intelligence data from Law Enforcement Agencies (predominantly police forces) on a daily basis concerning persons, events, locations, organisations (including criminal) and objectives. The records that compose the nationally-accessible PND are copies of locally-held records on individual force systems.

2 Privacy Impact Assessment

The NLEDP conducted the 1st iteration of a Privacy Impact Assessment (PIA) of LEDS in February 2017. Both the PNC and PND as individual systems were subjected to Privacy Screening Assessments in their current form and potential privacy issues arising from the co-location of these systems onto the same platform were considered. Privacy and related risks were identified before mitigations were proposed and evaluated.
The following primary risks were identified within the 1st iteration of the LEDS PIA:

System	Issue	Concern	Mitigation
PND	Facial search	Inconsistent application of common retention policy for custody images at a local force level. Human operator confirmation for facial image matching has always been used to mitigate concerns of automated matching of images.	Local custody image retention policy is under review to ensure retention length is necessary and proportionate.
	Data quality	Data held on local force systems that feed into PND varies in quality and structure and accuracy. Inconsistency in local force data quality impacts on PND data quality.	Subject to resourcing, compliance with existing policing guidance on the management of police information (MoPI) may be thoroughly addressed. A Working Group dedicated to Data Standards is working with PND Users to improve PND data quality standards.
PNC	Proportionality of holding certain records	The retention of arrest data (not charged or convicted), charging data (not convicted) or very minor historical conviction data can be perceived as not proportionate in data protection terms.	The proportionality of holding this data is under review, including primarily considerations regarding the purpose for which this data is held on systems.
LEDS	Potential consequences of co-location / merging of data	Greater amounts of data are made available to Users – in both volume and type – that hinder rather than benefit Users' strategic or tactical objectives due to information overload.	Considered mitigations include partitioning specified data pools, rather than fully merging them, on LEDS. Detailed access-based-controls for both roles and organisations are also being developed within the Programme and will be clearly marked within Data Sharing Agreements.
		Some Users are able to access a greater-than-appropriate level of data for their individual role or organisation.	
		Individuals are brought to the attention of Law Enforcement Agencies for the wrong reasons or through inappropriate means.	
		Quality of PNC data is adversely affected by corresponding PND data.	
		Conflicts arise as a result of differing data management strategies in different User organisations.	
	Retention variance	Retention periods vary between PND and PNC.	Whether or not to maintain data separation with specific retention regimes for data based on its provenance or to move to a single retention regime, likely based on MoPI, remains under consideration.

3 Next Steps

The 1st iteration of the PIA has been socialised with key internal and external stakeholders prior to its public socialisation with civil society organisations, including the Information Commissioner's Office (ICO), the Independent Digital Ethics Panel for Policing (IDEPP) and the Biometrics & Forensics Ethics Group (BFEG). Minor edits and comments from these stakeholders will be taken on board and incorporated before the 1st iteration of the PIA is publicly published.

LEDS' PIA is an iterative process that will continue beyond this initial iteration, with a PIA to be published on an annual basis to take note of privacy-related changes created from the NLEDP. To this end, substantive comments received from individual and collective consultation on the 1st iteration PIA, including the 1 December consultation with civil society organisations, will be incorporated into and inform the development of the 2nd iteration of the PIA.