Open Rights Group response to consultation on Law Enforcement Data Service Code of Practice

9 September 2020

1- Thinking about the proposed layout, structure and language used for the Code and guidance document, do you feel it is clear and understandable?

Disagree

The documents are missing key content and clarity on areas including:

- The governance structures that will be in place currently and for deciding who shall be granted further access to LEDS.
- The types of data that will be collected and the different governing regimes that apply.
- Key information to individuals about their rights and the scope of infringement that may occur with their details on LEDS.

The governance structures that will be in place currently and for deciding who shall be granted further access to LEDS.

There should be publicly available information about the criteria being applied to determine suitability, allowing for scrutiny and challenge from external bodies of the types of organisation granted access to LEDS.

The types of data that will be collected and the different governing regimes that apply.

Section 15 of the Public Guide sets out the kinds of people that may be included on LEDS, but it does not inform what information will be held about the individual on the database. There is a vague reference to intelligence data that has been gathered too that also fails to elaborate on the types of personal data that will be present on the system.

This is important for accountability. For example, how will an individual be able to assess whether a request for data under the Data Protection Act 2018 has been fully complied with unless a clear set of types of personal data collected is made available?

Further there will be separate standards that apply between the different bases for processing data in LEDS (safeguarding, policing purpose, law enforcement purpose)

added to that the different regimes for personal data and special category data. Finally, the various kinds of people from victims to witnesses to suspects and the differing age groups from children to adults that could be included on LEDS all should be acknowledged and the different thresholds and governance arrangements for these groups set out.

Key information to individual's about their rights and the scope of infringement that may occur with their details on LEDS.

In the document "Why Might I be on LEDS?" regarding immigration enforcement for individuals reported missing it does not specify for how long an individual's data will be held. This should be clarified immediately.

2 - Do you feel that the Code and Guidance Document effectively support the implementation of the five aims that are outlined on page 6 of the Code (safeguarding people, promoting accountability, promoting understanding, enabling performance and promoting fairness)?

Strongly disagree

There is little to no information provided on improving the individual rights systems that are the basis for some of the necessary reforms for the PNC and PND. This is key to promoting accountability. Specifically lack of improvement in the individual rights framework on requesting a review of a LEDS entry, which the European Court of Human Rights had made a note to critique in the Gaughran case.

There are gaps in information to individuals on the types of data that will be collected about them if added to LEDS, and the governance procedures that will regulate the processing of data. This is key to promoting understanding. This is evidenced in the "Public guide document" at section 15 where the types of people are listed but a generic reference to certain types of information that will be held. The types of data listed should be exhaustive, particularly in the Public Guide the purpose of which should be to promote understanding of what data is held on LEDS and how data accessed through LEDS might be used.

While there is a singular statement at section 15.7 regarding the need for additional assessments for the adoption of advanced analytics, or facial recognition in the Public Guide, there is no such statement in the Guidance or in the Code itself. It should be made clear across all documentation relating to LEDS that the Guidance and governance arrangements set out here are not a greenlight for all forms of processing.

The most recent judgment in Gaughran from the European Court of Human Rights was scathing in its critique of the individual rights framework in the United Kingdom for an individual to challenge their inclusion in policing databases. The Court reflected on the Northern Irish systems for retention of data that "there is no provision allowing the

applicant to apply to have the data concerning him deleted if conserving the data no longer appeared necessary in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and person's current personality. Accordingly, the review available to the individual would appear to be so narrow as to be almost hypothetical".[1] This state of affairs is something that we would hope the wider LEDS development would actively engage with but nothing is being shown in relation to this Code that would suggest such a thing.

There is also no reference to the custody image review process that was established following the 2017 Custody Image Review by the Home Office.[2] While there are clearly areas of concern about the effectiveness of the custody image deletion process, failing to provide it in public materials will not assist in meeting the principle of accountability set out.

3 - Do the Code and Guidance Document set out and explain the ethical principles that individuals and organisations using LEDS should follow?

Disagree

It is encouraging to see the structures of The Code and Guidance to reflect the proposed principles for ethical and professional use of LEDS and the practice that certain individuals will follow such as the Chief Officer, Operational Manager, LEDS User, NPCC, and so on.

However there must be a greater focus on the governance and safeguards which will underpin this work. In particular there is little recognition of the separate types of data held in LEDS, and the different governance and standards that apply whether that is policing, law enforcement, safeguarding purposes, each of which will have a different set of standards that apply. Additionally there are differences between types of people on the database, from a missing person, to a suspect, to a witness. The ethical principles for working with their personal data within LEDS will also require greater separation and explanation.

The case of RMC and FJ v. Commissioner of Police of the Metropolis from 2012 set out the need to consider important factors prior to adding an individual to policing databases. The nature of an offence and the age of the person arrested are just two factors the Court set out.[3] The ethical principles in the Code and Guidance document make no reference to this consideration for when an individual should have an entry created in LEDS. This is particularly concerning given that LEDs will incorporate "intelligence" information, not

[1] Para. 94, Gaughran v. the United Kingdom, http://hudoc.echr.coe.int/spa?i=001-200817.

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

[3] RMC v. FJ para 49. https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf.

just arrest or conviction records but more subjective assessments such as allegations or where investigations had concluded but resulted in no caution or conviction.

4- Do the Code and guidance document make clear the range of organisations involved in LEDS, the roles of those organisations and how those organisations should process personal data?
(A list of organisations with access to LEDS data is available on the college.police.uk consultation page.)

Disagree

The specific documents produced provide some general explanation of the range of organisations (policing and non-policing) involved in LEDS, and the reason for their access. However, more should be done to make things clearer for members of the public. In particular setting out the type of information they will be able to access on LEDS would be important. There is little relevance to the phrase 'competent authority' to those with limited to no familiarity with the Data Protection Act 2018 Part 3. Section 13 of the Code of Practice for LEDS – Public Guide could be be improved by considering a more general explanatory point about the different types of personal data that different kinds of organisations will be able to access.

Further, there is need to clarify the scope of role-based access controls that LEDS will operate and with that the types of data that will be accessible with the given role.

5 - Thinking about privacy laws and regulations, do the Code and Guidance Document clearly set out the performance expectations and behaviours for LEDS users?

Disagree

The guidance does not go far enough in communicating the additional governance needs that a local force should be required to conduct in the event of their adoption of innovative or general profiling. Section 5 of the Code sets out the difference between policing purposes, law enforcement purposes and safeguarding purposes but it fails to expand set the limits of these purposes. This is important for the public and users of LEDS as it is crucial that new and innovative processing operations for example incorporating forms of data analysis must have a separate and additional governance procedure, requiring a separate expectation and behaviour of responsible consultation with stakeholders *prior* to the adoption of new processing operations.

The Code of Practice and guidance is not and should not be considered a green light for all forms of processing undertaken by LEDS. It should only relate to a narrow set of purposes. In the event a local police force should want to undertake some form of innovative work using personal data available in LEDS, such as advanced analytics then it must carry out a separate and additional impact assessment and consultation with local communities. For example, if West Midlands were to return their exploration of advanced

analytics with NDAS[4] the LEDS guidance or governance currently in place should not be considered a sufficient governance document and further data governance must be demonstrated alongside ethical standards and sufficient data quality both of which are key principles to LEDS.

We refer back to our answer to Q 2 where the need for additional governance is acknowledged in the Public Guide at section 15.7 but no other reference is made across any of the other Code documents. Document should be reviewed to ensure that the same standards are evident across each of the governance documents.

Further, the principle of non-discrimination in the use of data for policing purposes is only partially reflected here. The ICO's investigation into the Gangs Matrix[5] and the decision in Bridges v. South Wales both clearly set out that the data controller must pay closer attention to matters of discrimination and equality. In particular Bridges reiterated a positive duty in the Public Sector Equality Duty to require a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population[6]. The court had suggested that all police forces that intend to use a novel (and in the case of AFR controversial) technology would do everything reasonable to satisfy themselves that there is no racial or gender bias[7]. That would require further statement in our opinion than just consideration of the principle of preventing discrimination as the LEDS Guidance refers at page 41.

6 - Do the Code and Guidance Document clearly set out that all LEDS users should be given appropriate initial and refresher training?

Neither agree nor disagree

It is clear from the principles that initial and refresher training is a key part of the principles. It would be useful to clarify that the training is mandatory for *all* users of LEDS including commercial and non-policing organisations. The training should also require individuals to pass the modules to gain access, and regular checks against this should be carried out. It cannot be that the training is merely a how to guide but key lessons in the ethical, lawful and proportionate use of personal data held in LEDS.

7 - Does the Code state clearly that users have a responsibility to ensure that data held in LEDS is of the highest possible quality?

4 Police scrap artificial intelligence tool to predict violence, August 8 2020, The Times. https://www.thetimes.co.uk/article/police-scrap-artificial-intelligence-tool-to-predict-violence-zdln8bgz0.

5 ICO Gangs Matrix Enforcement Notice, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf

6 Bridges Judgement, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

7 *Ibid* 201.

Neither agree nor disagree

Data quality is recognised as an important part of LEDS with its inclusion as a principle. We would encourage the need for data quality to be backed with stronger safeguards and responses to inadequate, incomplete or incorrect data to be set out. Including the revocation of access to LEDS for users who fail to provide adequate data and for forces that represent a systemic failing to have their access to LEDS restricted as 'read only' or even complete restriction.

The process currently undertaken to improve the quality of data on LEDS, including the deletion of inadequate, irrelevant, or incorrect entries should be continued. The review, retention and disposal of data no longer necessary for the purpose for which it was collected is a key data protection principle. This reinforces the need for clearer statements about the types of data collected, for what purpose and the governance standards that accompany it.

8 - Does the Code clearly set out that personal data collected for law enforcement purposes and stored in LEDS needs to be lawful, adequate, relevant and not excessive in relation to the purpose for which it is processed?

Disagree

While Section 5.3 of the Code of Practice LEDS Guidance sets out the differences between policing purpose, law enforcement purpose and safeguarding purposes it leaves ambiguous the scope and limitations of law enforcement purpose. This purpose is one of the widest areas for processing activities, including at 5.3.5 setting out that this basis would allow processing providing the processing is authorised by law, and necessary and proportionate to that purpose. This leaves a wide discretion on the user of LEDs to assess for themselves.

The Code also fails to set out that the processing for law enforcement purposes will often be sensitive, special category data and require the user to demonstrate that the processing is strictly necessary, and cannot be achieved through less intrusive means.

The Code should seek to set out the limitations of that area including pieces like adopting new and novel processing activities on data held in LEDs which would require additional safeguards and scrutiny prior to any processing undertaken. In particular we would draw attention to the requirements under Article 35 and 36 of the GDPR. These two Articles require assessments (Article 35) and consultation with the supervisory authority (Article 36) prior to processing data where the assessment indicates that the processing would result in a high risk.

Given the sensitivity of the processing for law enforcement purposes, the Data Protection Act 2018 requires safeguards for processing. This includes an appropriate policy document in place that details the procedures for ensuring compliance with the law enforcement data protection principles; and policies on the retention and erasure of that data. The Code of Practice and Guidance while going some way towards responding to this requirement does not go far enough. It is important that local LEDS users

demonstrate prior to undertaking processing using LEDS that they have an appropriate policy document in place that satisfies these conditions. The Code could be a reference point but it is not a full account of all forces processing activities, nor should it be.

9 - Are the governance arrangements for maintaining the Code clear and easy to understand?

Strongly disagree

For the public there is clearly information lacking. In particular

- Temporary governance arrangements of LEDS.
- Information that is still under review for example the immigration enforcement retention times set out in the Why Am I On LEDS document.

These should be addressed and concluded prior to LEDS going fully live and being made available to policing and non-policing organisations.

10 - Do the Code and Guidance Document clearly explain the types of activity that will be exempt from the Code?

Strongly disagree

No. It is unclear what types of activity will be exempt from the Code and it should be set out clearly what these are, and the implications for this for the public's rights.