

LEDS Open Space:

Data Protection Impact Assessment

Drafting directions

This Document has been written with the aim of stimulating discussion on the development of the Code of Practice for LEDS It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to and viewed only by members of the LEDS Open Space.

Significant changes to document

Initial draft

30th April 2019

Purpose

1. This paper has been written to provide an update on the drafting of a Data Protection Impact Assessment (DPIA) for the Law Enforcement Data Service (LEDS). This paper will be discussed within the LEDS/HOB Open Space on 14th May 2019 and will aim to provide an update on the project progress since the last Open Space Meeting in February. The aim of this is to promote further discussion on proposed content of the DPIA and identify how the considerations of previous workshops have been taken into account in early drafting.

Summary

2. This paper provides an overview of the concerns raised about the previous Privacy Impact Assessment. In reviewing this and attached documents, members of the Open Space will be asked for their views on the prioritisation and treatment of these concerns.

Key questions posed by this paper

1. Do Open Space Members feel the list in Annex A is comprehensive?
2. If the list needed to be prioritized, how would this be achieved?
3. Are any items in this list of a lower priority / not essential?
4. Are there a number of 'must have' concerns to be resolved for the next draft?
5. What other organisations might be worthy of approaching to help with drafting the DPIA?

Data Protection Impact Assessment

Developing the DPIA document

3. The Privacy Impact Assessment development started in 2016, largely completed in 2017 and was [published in 2018](#). It related to the data processing undertaken in the Police National Database (PND) and Police National Computer (PNC) and provided a current view of the expected privacy impacts for LEDS. This PIA replaces the existing PND PIA and constitutes the first such impact assessment for the PNC; and considers processing within these systems prior to 25 May 2018 and the entry into force of the Data Protection Act 2018 (DPA). [REDACTED]
4. The publication was the first version of what was intended to be an annual series of LEDS privacy assessments; future versions will focus on LEDS as the new service and use the new Data Protection Impact Assessment (DPIA) process according to the DPA.
5. For a variety of reasons, it has not proven possible to update the PIA before now. However, the process has now started, and the Home Office estimates a final draft will be ready by September 2019 for formal consultation, with a likely publication date of December 2019. Between now and publication Open Space members will be consulted on the intermediate drafts.
6. Late on during the previous process, comments were received from civil society, privacy and ethics groups. Some of those comments were taken on board, but many could not be substantively addressed without considerable rework. The decision was therefore taken to publish the PIA and provide a more substantive update in the following version. The table in Annex A is a substantive summary of the comments received in relation to the PIA from civil society, privacy and ethics groups.
7. The broad concern is that the Privacy Impact Assessment is currently operationally focused rather than viewing the impact from the perspective of individuals and particular groupings.

LEDS/HOB Open Space Non Paper

Annex A Table of Concerns in relation to the existing LEDS PIA and suggestions for the future DPIA		
	Concerns from existing PIA	Suggestions for future DPIA
1	Depth of coverage within the PIA. More details required.	The Privacy Impact Assessment (PIA) describes the likely new system (LEDS) and its privacy concerns, but as the knowledge about what LEDS will deliver firms up further and more extensive details will be required to match any possible or actual increase (or decrease) in functionality, purpose, uses, and sharing.
2	Data Aggregation. More details on the impact of the aggregation of PNC and PND data.	<p>The impact of the aggregation of data elements from PNC and PND needs to be elaborated. The privacy concerns are greater than a sum of the PNC and PND components. The DPIA will need to consider the privacy implications and mitigations that relate specifically to the functioning of the LEDS platform as a new system. Discrepancies in data activities between PND and PNC, and across Forces, are acknowledged, but the ethical, legal and rights implications (apart from operational problems) need also to be brought out.</p> <p>This is particularly so in respect of the potential for a larger number of results, including personal data, which otherwise might not have been offered about individuals previously. This is heightened in circumstances where no wrongdoing is suspected.</p> <p>The DPIA should identify;</p> <ul style="list-style-type: none"> • What measures have been taken, or will be taken, to ensure that as little information as possible is shared (a) about people not suspected of any wrongdoing, and (b) that is not relevant to the specific cases investigated?
3	Risk identification. More details on the potential interference with individual rights and freedoms	<p>The concern here is for a full articulation of risks to various individual rights, including those relating to privacy, freedom of association, freedom of expression and freedom of assembly. This risk identification should not be limited to the identification of new risks from the change to LEDS from PNC and PND, but, start from a “zero base”.</p> <p>This would enable a more consistent balance between the clear benefits of LEDS with any adverse effects on categories or groups of people who may be brought into contact with law enforcement, including through (real or perceived) use of LEDS analytical systems or processes and through the creation, collection and sharing of data through the use of new technologies.</p>

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention

4	Wider impacts should be addressed in a published Policy Equality Statement.	Any adverse impacts to individual rights and freedoms should be addressed within the Policy Equality Statement (PES) which should be published alongside the assessment document. Or else an existing Equality Statement should be referenced. This PES should cover adverse effects, including assessment of any (real or perceived) stigmatisation and any (real or perceived) weakening of the presumption of innocence, and the formation of safeguards aimed at mitigating these effects.
5	Initial Screening questions. Making the research questions more exhaustive.	The initial questions aimed at sparking the conversations to gather information for the DPIA should be made more exhaustive to ensure more depth in the responses. This should include questions about LEDS as a new system co-locating PNC and PND and in future increasing the users with access to a more powerful tool.
6	Overarching Ethical considerations need to be developed for LEDS drawing upon existing (where possible) sources.	The possibility of merging the previous two databases (beyond co-location) needs to be explored from a privacy and ethical position. It would also be important to develop an inventory of ethical principles to guide the ongoing development of the LEDS. This would need to draw upon existing and new sources, including from the law enforcement community; the practical and academic data protection community; good-practice guidance documents in democratic, political and management theory; and in cultural understandings of ethical practice and relationships.
7	Dissemination of learning throughout the Law Enforcement community as analysis is conducted for the DPIA.	During the development of the DPIA the learning should be disseminated to the law enforcement community and beyond. This would protect the interests both the law enforcement community who will use LEDS and the public whose privacy and other rights might be affected by the new programme.
8	Include evidence base of public perceptions and public acceptance.	The DPIA needs to include firm evidence of the public perception and or acceptance of capabilities. Public and 'stakeholder' consultations need to be further specified within the DPIA and those consultations need a greater breadth. Need to consider a role for a Parliamentary debate.
9	Governance and oversight.	Governance and oversight elements, including rules, need to be more fully fleshed out and defined in more assertive 'should' or 'will' terms rather than 'might' or 'can'. LEDS will need an overarching governance model, which could embrace privacy safeguards as well as other assurances, the requirements for this should be more fully articulated within the DPIA.
10	User constituency and what access to information they	The DPIA needs clearer and fuller discussion of the access to, and use of, the LEDS platform, and of the uses to which the information will be put by the variety of potential users. This to include which users have access to what information and for what purpose. Any expansion of the participation in LEDS to further organisations

	have on LEDS and for what reasons.	beyond law enforcement will require fuller articulation in the DPIA. Information sharing should have full justification alongside transparent governance procedures for that data access.
11	Fair processing, big data and data minimisation.	Greater consideration within the DPIA of data minimisation and how this will be considered in future. Similarly, the DPIA will need to consider the potential for the software itself to be non-neutral in the way it operates, and what steps will be taken to avoid this. The DPIA needs to describe better how access to data through access controls will be limited.
13	Controls against Function Creep within the DPIA.	There is a risk of mission creep. The DPIA needs to articulate what mitigations will be put in place to appropriately limit creep and to ensure appropriate consultation around changes of scope. There is a need to consider a role for Parliament too.
14	Data Security and better descriptions of the requirement for protections.	The DPIA should require, as a mitigation, the use of appropriate security measures such as encryption, anonymization, pseudonymisation, and provisions for secure database backup. It should also include more on the impact on security of the use of mobile devices to access LEDS and the requirement to provide appropriate security. These concerns extend to an articulation of parameters used to protect information in the cloud environment. Protections also need to apply to data extracted from LEDS.
15	Data deletion and data accuracy and how this will be impacted by automation.	Data retention and erasure issues and mitigations need to be more fully articulated in the DPIA.
16	Custody Image use and any wider application of Custody Images.	Facial recognition and the use of custody images are prominent in the LEDS future and need more ethical consideration within the DPIA as does any facial search capability. It may be advisable to set universal retention policies in the near future and this should be included in the DPIA. A National Custody Image Database like for fingerprints and DNA, might be an answer The DPIA should determine the parameters around access to custody images on a searchable basis, particularly if the system doesn't restrict access based on nature of crime. There is concern around the ability to search large volumes of low level crimes. Essentially, access controls are required to reduce abuse of searching of custody images. The impact of this needs to be articulated alongside the need for detailed audit logs in relation to access to custody images. The DPIA should talk about roadside-facial-spot-checks using a facial image. Specifically, the fundamental privacy implications of automated tools being used to forcibly reveal the identity of members of the public.

17	Predictive policing within LEDS.	The use of the LEDS platform for the purposes of predictive policing should be addressed with the DPIA, and ethical issues and safeguards highlighted.
18	Data Standards.	The DPIA should make clear what standards are to be adopted.
19	Data Subject access requests.	<p>It is not clear how, or if, meeting Subject Access Requests will be affected by LEDS, and how other statutory rights (e.g., to erasure) will be realised if, for instance, additional more sensitive information is merged together. It will often not be possible to tell subjects exactly what data is held on them or exactly how it is being used as this could compromise the prevention and detection of crime. But the DPIA needs to make clear who makes the decision on whether and what to disclose, and what level of accountability and scrutiny there is for these decisions.</p> <p>Additionally, data subjects should understand and possibly be able to access the log of instances of when their data has been searched. The reason for data search would be of interest to the subject, particularly if they're being stopped and having their record searched regularly without then being arrested / charged / convicted. The DPIA should consider this and explore proactive notification to individuals that their data had been accessed.</p>
20	Non-crime related data.	<p>The DPIA should set out a clear policy on victims and witness data, perhaps by keeping such data in a separate data pool. The ethical issues surrounding data on victims, medical and health information, and non-crime-related information (e.g., DVLA data) need further identification and definition.</p> <p>The use of medical and health information need far greater justification within any DPIA if it is to be considered. The existing medical information including that relating to Mental Health needs to be examined within the context of accuracy in the use of LEDS.</p>
21	Role based access.	Given the increase in available sensitive and personal data that will result from the merger of these data sets, regulating access to searchers of the LEDS on a need to know basis is essential. The DPIA should set out how this role-based access regime would work.
22	EU GDPR/Policing Directive considerations.	The DPIA will need to include how examination should be made of the possible implications of the EU's General Data Protection Regulation (GDPR) and of the Policing Directive, both of which will be incorporated into UK law.
23	Data audit provisions.	The DPIA should include more information on the audit provisions as a mitigation against data misuse.

24	Management Statistics – what will be measured and what will be shared.	The DPIA should include further details regarding LED's audit functions with respect to management statistics as mitigation against potential misuse.
----	--	---

Key questions posed by this paper:

1. Do Open Space Members feel the list in Annex A is comprehensive?
2. If the list needed to be prioritized, how would this be achieved?
3. Are any items in this list of a lower priority / not essential?
4. Are there a number of 'must have' concerns to be resolved for the next draft?
5. What other organisations might be worthy of approaching to help with drafting the DPIA?