Reference: DPIA 2018-0010

[redacted]
Police Scotland, Clyde Gateway
2 French Street
Dalmarnock
Glasgow
G40 4EH

29 January 2019

Dear [redacted]

Re: Data Protection Impact Assessment – Risk and Concern

Thank you for submitting your Data Protection Impact Assessment (DPIA) 'Risk and Concern' to the Information Commissioner's Office, and for your subsequent submissions in response to our queries.

As we have discussed, while your DPIA demonstrates that you have identified some significant risks to compliance with the GDPR, the processing described has been in operation for some time. The DPIA has therefore been reviewed under the Commissioner's general obligations to provide advice, since it did not meet the conditions for prior consultation with the ICO under Article 36 of the GDPR.

It should be noted that this advice is without prejudice to any future intervention by the Commissioner in accordance with her tasks and powers, in line with her Regulatory Action Policy.

Based on the information provided, we require Police Scotland to:

1. Consider whether the scope of a single DPIA is adequate to the range of functions, purposes and legal bases for processing related to the interim Vulnerable Persons Database (iVPD).
2. Reconsider and explain the decision to rely on consent as the lawful basis for sharing personal data with non-statutory partner agencies.
3. Review and update provisions for transparency and the right to be informed in the front line collection of personal data.
4. Document an equal if not separate assessment of data protection risks relating to Concern Hub decision-making and disclosure.
5. Justify the necessity and proportionality of the retention of personal data on the iVPD where it diverges from National Retention Assessment Criteria guidance, or else amend the policy so it aligns with NRAC.

1. <u>Scope of the DPIA</u>

Police Scotland should consider whether the scope of a single DPIA is adequate to the range of functions, purposes and legal bases for processing related to the iVPD.

The iVPD is a large-scale, single database that captures the information of individuals who are, or are perceived to be, experiencing some form of adversity and/or situational vulnerability which may impact on their current or future wellbeing. The database has been in operation for a number of years as a function of Police Scotland's Risk and Concern project, and the introduction of the GDPR has led Police Scotland to identify data protection compliance issues and refer a DPIA to the Information Commissioner for advice.

Although the iVPD is the single means for processing the data of all vulnerable persons, Police Scotland should reconsider whether it is practicable and realistic to assess all risks against the singularity of the database. Policing aims and the rights of data subjects may be better served if data protection risks are considered against the distinct purposes of each category of concern, as detailed in the diverse Standard Operating Procedures relating to individuals recorded on the iVPD.

2. Lawfulness and Consent

Police Scotland should reconsider and explain the decision to rely on a lawful basis of consent for sharing personal data with non-statutory partner agencies.

When front line Police Scotland officers attend scenes of crime, incidents and/or concerns about individuals perceived as vulnerable, those officers collect relevant personal data from individuals at the scene and thereafter complete a Concern Report on the iVPD. The collection of personal data by front line officers and subsequent sharing by Concern Hubs with statutory agencies is carried out, depending on the particular circumstances of the individual, under one of the following legal bases:

Article 6.1: (c) Legal obligation; (d) Vital interests; (e) Public task.

Article 9.2 (for special category data): (g) Substantial Public Interest; (h) Provision of Health or Social Care (as provided for by DPA 18 – sch 1, 1 2d/2e).

Following a decision by the Force Executive, Police Scotland is relying upon the following legal bases for Concern Hubs sharing personal data with non-statutory partner agencies:

Article 6.1: (a) Consent.
Article 9.2 (for special category data): (a) Explicit consent.

Having identified consent as the appropriate legal basis for information sharing with non-statutory partners, Police Scotland has made the decision that front line officers are best placed to obtain that consent at the time of attending an incident. However, these officers cannot know with which partner agencies the Concern Hub will share information at the next stage of the processing, and therefore whether obtaining consent is necessary.

Police Scotland's written submission dated 15 November considers, for example, the risk that consent may be sought from an individual where an alternative legal basis for sharing may be used in Concern Hubs. This would result in a data

subject being given a false impression of control over the processing of their data which is likely to be misleading and inherently unfair.

The DPIA also identifies risks to the validity of consent, given the higher standard required under the GDPR, which defines valid consent in Article 4(11) as "freely given, specific, informed and unambiguous" and is further set out in Article 7. The ICO has also provided detailed guidance on the conditions for obtaining valid consent.

The validity of consent as 'freely given' under the GDPR is subject to the provisions of Recital 43, which states that:

> "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."

In addition to the inherent vulnerability of the individuals whose data is being processed at the time of an incident (see also European guidelines), the imbalance between data subject and controller in the case of Police Scotland as a public authority creates further problems for relying on consent. Police Scotland should reconsider whether the burden of proof and requirements for a legal basis of freely given consent for sharing data can be met by front line officers where they are seeking to obtain it (a) as a public authority; (b) from vulnerable individuals and children in particular; and (c) when they cannot be sure that this legal basis will later be relied upon for sharing by Concern Hubs.

Police Scotland is relying on consent for sharing special category personal data with non-statutory partner agencies, although identifies that this is unlikely to be compliant with the GDPR. In doing so, it appears to have rejected the legal basis of Public Task, which ICO guidance explains should focus on "the nature of the function, not the nature of the organisation". It would be helpful to understand Police Scotland's consideration of alternative legal bases for processing, and particularly its determination that Substantial Public Interest conditions would not be appropriate for sharing information with non-statutory partners.

3. The Right to be informed

Police Scotland should review and update provisions for transparency and the right to be informed in the front line collection of personal data.

Article 13 of the GDPR (right to be informed) requires that data subjects are provided with certain information at the point of data collection, including 13.1(c) the purposes and legal basis for the processing, and 13.1(e) the recipients or categories of recipients of the personal data.

Although trained and equipped with prompts such as Aide Memoirs to relay the appropriate information, Police Scotland recognises that officers at the scene of incidents are not always able to inform individuals exactly who their information will be shared with and on what legal basis it will be processed. Likewise, Police

Scotland acknowledge that data subjects are not provided with the Privacy Notice at the point of collection, which is currently only available to view by visiting the Police Scotland website.

When personal data is collected that has not been obtained from the data subject, particular consideration of data subject rights under Article 14 should also be in evidence in a DPIA. This should document the information that is provided to these data subjects, or the exceptions to the controller's obligation to provide information in these circumstances.

Police Scotland should review the adequacy of their provision of privacy information to data subjects and continue to ensure that comprehensive training is provided for front line officers.

4. Assessment and Disclosure

Police Scotland should document an equal if not separate assessment of data protection risks relating to Concern Hub decision-making and disclosure.

Within divisional Concern Hubs, the Concern Reports entered by front line officers on the iVPD are subject to a process of triage, research and assessment, and information is shared with relevant partner agencies within 24 hours where considered appropriate.

The DPIA should give attention to the exercise of data subject rights throughout the assessment and disclosure stage of the processing. In particular, the Article 18 right to restriction of processing warrants further consideration, notably when a data subject has successfully exercised their Article 21 right to object.

A core function of the Concern Hub includes responding to information requests from business areas within Police Scotland and external partner agencies. The Risk and Concern DPIA makes no reference to solicited information sharing, the exercise of relevant data subject rights or the security risks that may be associated with it. The 'iVPD Rules, Conventions and Data Input Standards' reference 'iVPD Security Operating Procedures', although these are not among the list of relevant guidance documents referred to in the DPIA.

The present information governance arrangements with external partners cannot be determined without the corresponding Information Sharing Agreements in place with partner agencies. These have been requested from Police Scotland, but have been withheld as they are undergoing re-writes to align them with the GDPR and the current DPIA.

The DPIA does give some account of information security, including exchange with partner agencies via the Egress IT solution, but this ought to be a more prominent and consistent feature throughout the assessment. For instance, the 'iVPD Rules, Conventions and Data Input Standards' prohibit sending Concern Reports to group mailboxes of divisional Police Scotland Concern Hubs, but do reference sending them to group mailboxes of partner agencies, a potential variance in security controls that is not considered in the DPIA.

A DPIA associated with the end-to-end processing related to the iVPD ought to provide an equal account of data protection risk at the Concern Hub stage as well as to the initial data collection. Police Scotland should ensure that they are accountable for data protection by design and default throughout the lifetime of the processing operation, from the accuracy of information collected in officers' notebooks to the governance of disclosure to partner agencies.

5. Storage Limitation

Police Scotland must either justify the necessity and proportionality of the retention of personal data on the iVPD where it diverges from National Retention Assessment Criteria guidance, or else amend the policy so it aligns with NRAC.

The iVPD has been subject to significant levels of public interest and press scrutiny owing to the size of the database (969,876 unique nominals). The DPIA notes (Q11) that a proportion of nominals on the database are classified as of No Concern/Not Applicable, but are considered necessary and relevant to record, for example a parent of a child, details of the interpreter or Appropriate Adult who assisted communication, or a witness.

Police Scotland should assess the necessity and proportionality of recording and further retaining the personal data of individuals of no concern on the Vulnerable Persons Database. Whilst a new weeding and retention policy is being implemented to help address this issue, Police Scotland should clarify the purposes for which the data of persons of no concern is retained, the categories of data that are recorded and the legal basis for doing so – particularly if this should include special categories of data.

The Weeding and Retention Policy considered by the iVPD Information Asset Owner Board outlines the National Retention Assessment Criteria (NRAC) as determined by the College of Policing. Paragraph 5.6.1 of the policy says that serious concerns should be held for a minimum of 12 years and a day. The NRAC puts the requirement to review whether it is still necessary to retain records for a policing purpose at a period of six years. There is no explanation for the 12-year stipulation for iVPD records where NRAC guidance puts the period at six years. This disparity should either be fully justified in the policy or rectified so that it is brought in line with NRAC guidance.

Next steps

This concludes our advice on Police Scotland's DPIA as submitted, however the ICO wishes to continue liaising with Police Scotland on this matter. This work will be led by our Scotland team who will be in touch in the near future. We note that the DPO has welcomed further engagement with the ICO on the processing relating to the iVPD, and we look forward to building on this advice in due course.

Yours sincerely…

Ian Deasha, Group Manager – Data Protection Impact Assessments

CC: [redacted] Data Protection Officer

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.
For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice