Upholding information rights

45 Melville Street, Edinburgh, EH3 7HL
T. 0303 123 1115 E. scotland@ico.org.uk
www.ico.org.uk

Margaret Mitchell MSP
Convener, Justice Committee
c/o Justice Committee Clerks
Room T2.60
The Scottish Parliament
Edinburgh
EH99 1SP

24 May 2019

Dear Convener

Police Scotland's Interim Vulnerable Persons Database

Thank you for your letter of 26 April concerning Police Scotland's interim Vulnerable Persons Database (iVPD) and its compliance with data protection law.

The iVPD came to our attention in September 2017 when Police Scotland contacted us upon realising that what was intended to be a temporary system had not been built in a way which enabled it to delete personal data which was no longer relevant.

As Police Scotland was proactive in contacting us about this issue, and fully intended to put proper mechanisms in place, we did not deem formal enforcement action to be required, nor would it have been a proportionate response. However, we sought regular progress updates and also monitored the volume and nature of complaints from the public (which have been relatively few) which related to information which may be held on the iVPD. As the Committee will be aware, Police Scotland implemented automated weeding on 4 February 2019 which saw over 300,000 nominals deleted immediately.

Data protection impact assessment

As the regulator of data protection law in the UK, the ICO is concerned with the processing of personal data by data controllers and processors on electronic systems and, in certain circumstances, in manual filing systems too. Processing is wider than the electronic means used; it includes amongst other things the lawful basis and purpose of the processing, the relevance and accuracy of the personal data held, and the data protection rights of the individuals concerned.

In October 2018, Police Scotland sent us its data protection impact assessment (DPIA) on the collection and sharing of information about persons experiencing individual or situational vulnerabilities with partner agencies, focussing primarily on disclosure to third sector organisations.

We replied with five recommendations which we required Police Scotland to address. These were:

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.

For the Committee's information, I have enclosed our response to Police Scotland's DPIA. We also held a meeting with the Police on 15 February 2019 to discuss our response in more detail.

Justice Committee questions

In addition to these recommendations, I have provided answers below to the specific questions you asked.

- *whether the iVPD satisfies the General Data Protection Regulation (GDPR)*

  Our concerns on this matter are with the processing of personal data relating to vulnerable persons, of which the iVPD is only one of the elements to be considered. We believe there is further work to be done by Police Scotland to bring this processing into full compliance with the GDPR.

- *whether Police Scotland's DPIA sufficiently covers the issue of consent*

  The DPIA covered a wide range of circumstances and purposes for processing, some of which would never be compatible with consent. The recitals to the GDPR say that consent should not provide a valid legal ground for processing

personal data where there is a clear imbalance between the individual and the data controller. Where the controller is a public authority, it is unlikely that consent was freely given in the specific circumstances. Our recommendation was that each purpose should be separately assessed. The appropriate legal basis for processing personal data could then be considered on that basis.

- *whether consent is retrospective*

  Under the GDPR, consent must be freely given, specific, informed and unambiguous indication of the person's wishes. If consent was to be sought retrospectively, it could not meet these requirements as some processing would have already occurred.

- *whether Police Scotland is required to review its existing consents and consent mechanisms to ensure that they meet the GDPR standard*

  Any review of consent mechanisms should have taken place prior to the GDPR coming into force on 25 May 2018. As mentioned above, consent is unlikely to be valid where there is an imbalance of power in the specific circumstances between the individual and Police Scotland as a public authority controller.

- *whether Police Scotland is required to contact all of the individuals whose details are stored on the iVPD to inform them of their right to give consent to their details being shared with third parties as well as their right to withdraw that consent*

  Under the right to be informed in the GDPR, all controllers have to provide certain information to those individuals whose data they are processing irrespective of the conditions for processing that are applied. This includes information about their data protection rights, how to exercise them and details of the recipients or categories of recipients of the personal data.

- *whether Police Scotland adequately publicise these rights and have made it sufficiently easy for individuals to contact them to withdraw their consent*

  Police Scotland has taken steps to train officers and provided them with contact cards to provide to people with information about how to withdraw consent or find out more information. Privacy notices are available on Police Scotland's website[1].

[1] https://www.scotland.police.uk/access-to-information/data-protection/privacy-notices

- *whether Police Scotland have put the necessary arrangements in place to inform people that their details are stored on its iVPD and that they are able to request access to that data*

  As stated in our answer above, officers have contact cards to give to individuals. The cards include a link to the online privacy notices which contain information about the right to access a copy of personal data held by Police Scotland. Controllers are not required to name or provide information about the specific system or database on which the personal data will be held.

- *whether Police Scotland have put suitable arrangements in place to ensure that people are aware of their right to object, either verbally or in writing.*

  Again, this information is available from the link on the contact card.

Conclusion

We believe Police Scotland still has work to do to bring its processing of personal information about vulnerable persons into full compliance with data protection law. We continue to monitor Police Scotland's response to our advice, which was given without prejudice to any future intervention by the Information Commissioner in accordance with her tasks and powers, and in line with her Regulatory Action Policy[2].

We trust this assists the Committee but would be happy to provide any further information or clarification as required.

Yours sincerely

Dr Ken Macdonald
Head of ICO Regions

Encl. The ICO's response to Police Scotland's DPIA on 'Risk and Concern'

[2] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf