Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to Consultation on Improving the Victim's Code

About the ICO

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

Our Response

The Information Commissioner responded to the first consultation proposal for revising the Code of Practice for Victims of Crime in 2019[1], setting out the relevant data protection considerations to be taken into account when drafting the revised Code. The points made in the first consultation response remain relevant, and this second response outlines our views in terms of the revised Victims' Code and the Government Response to the 2019 consultation.

The Information Commissioner's Office has recently undertaken an investigation into the practices used by police forces in extracting data from the mobile phones belonging to victims (and others) in the context of criminal investigations. In addition, she is looking more broadly into the path that victims' data takes through

[1] https://ico.org.uk/about-the-ico/consultations/ministry-of-justice-proposals-for-revising-the-code-of-practice-for-victims-of-crime-consultation/

the criminal justice system from allegation, through disclosure, prosecution and compensation.

There are opportunities to reinforce victims' data protection rights through incorporation in the Victims' Code, and this is likely to be a key recommendation following our investigation. We propose that any future iteration of the Code incorporates references to data protection and privacy when processing the personal data of victims of crime. We welcome the opportunity to respond to this further consultation.

Information rights

The proposed revised Code clearly sets out a number of Rights that will be conferred upon victims. However, it could do more to emphasise the importance of victims being afforded due consideration of their privacy and information rights. We are aware from the work of Claire Waxman, Victims' Commissioner for London in her London Rape Review[2] of the impact that unnecessary or disproportionate processing of their data can have on victims of crime, especially at a time when they may already be suffering trauma as a result of the crime.

You may wish to consider referencing Article 8 of the European Convention on Human Rights (ECHR) (given further effect in UK law by the Human Rights Act 1998) that provides the right to respect for their private and family life, their home and their correspondence. In the section of the draft Code entitled "How you can expect to be treated", you should make clear the extent to which victims should expect to be able to withhold private information – particularly that which is most sensitive – and how they are be able to exercise their information rights under the

[2] https://www.london.gov.uk/sites/default/files/vcl_rape_review_-_final_-_31st_july_2019.pdf

GDPR and the DPA 2018, as appropriate. It should also set out the victim's right to expect that only the minimum amount of their personal data necessary will be processed (collected, stored, or shared) by any of the service providers when they engage the relevant service, and that their data will be held securely and only used in order to facilitate the provision of the particular service.

All agencies and organisations processing victims' personal data need to do so fairly and lawfully, including when they grant access to that data to other organisations. This means being clear about the lawful basis for the processing, whether this be under the GDPR or the DPA 2018. This is particularly important in the case of victims of serious sexual offences, where the data being processed might be highly intrusive and sensitive. From a law enforcement perspective, this generally means that the data subject (i.e. the victim) has *consented* to the processing or the processing is *strictly necessary*.[3] Each of these bases for processing have specific conditions to be met if they are to be valid.

We understand that the Code needs to be easily understood by victims, especially at times when they are vulnerable. It is important, however, that victims are clear as to the extent they have a choice *not to* engage a particular service or what happens when any particular Right is engaged. The proposed practitioners' guidance should assist service providers in understanding what information should be provided to victims in this respect. For example, in the case of Right 4 (referral to victim support services), it must be made clear whether the engagement of this Right by a victim would result in their personal data being disclosed by the police to another service provider. Equally, it must be clear whether personal information would be shared should the victim not explicitly engage this Right.

[3] See s35 DPA 2018

The practitioners' guidance should also ensure that service providers are clear about how they need to make victims aware of how their personal data will be processed. The appropriate lawful basis for referring victims to victim services or support agencies needs to be considered and documented by service providers in the first instance. This will help service providers with effectively communicating to victims how they should expect their data to be processed, including what may or may not be shared.

In the "Enhanced Rights" section, the draft Code explains that those with enhanced rights may be offered additional support and states that "Such support may include being offered a referral to a specialist support service". However, the following paragraph explains that:

> "Once a service provider has identified that you are eligible for enhanced rights under this Code, they must ensure that this information is passed to other service providers with responsibilities under this Code and, where appropriate, to victim support services."

This could cause confusion around whether individuals should expect this referral to occur automatically and what the rationale for this is, or whether they have a choice. Further clarity may be needed so that victims fully understand the process.

This links to the proposed Right 3 (being provided with information). Under the DPA 2018 and the GDPR, there is an obligation on the police to provide information

to victims about how their personal information will be processed.[4] It would be helpful if this was referenced within Right 3.

Guidance for service providers

It can be challenging for organisations/service providers to navigate complex legislation and to have appropriate policies and procedures in place as well as ensuring that all practitioners act in ways that conform with victims' data protection rights. Legal gateways and lawful bases for information sharing can also be complex and situation-dependent, and we welcome your commitment to providing guidance for service providers that clearly sets out their obligations when considering the Rights set out in the proposed revised Code. For example, what data protection requirements should a police force consider when referring to victim support services? What is the lawful basis for sharing their personal data? What data should be shared? What if the victim expresses a wish for their data not to be shared? What if the victim changes their mind?

We would welcome the opportunity to engage with the Ministry of Justice in relation to the data protection aspects of the practitioners' guidance when it is being drafted.

Victim Personal Statement

In relation to the proposed Right 7 (the Victim Personal Statement (VPS)), victims must be provided with sufficient information so that they are able to understand exactly how their statement will be processed. We acknowledge that the government response to the consultation states that "if the case reaches court, the VPS may be included as evidence and the suspect will usually be able to see it".

[4] See s44 DPA 2018 & Article 13 GDPR

The Code focuses on whether the VPS will be read aloud in court and how much control a victim has over this. It should be stated unambiguously that victims can express a preference as to whether it is read aloud. Further clarity should be provided in the Code to ensure that victims fully understand what will happen to their VPS, who may have access to this information and for what purposes, even where it is not read aloud.

With regard to accessing a copy of the VPS, the government response to the consultation states that:

> "Concerns were raised by some respondents about victims potentially being given a copy of their witness statement if their VPS forms part of that statement. We propose to address these concerns by making the right to request a copy of the VPS applicable only where it has been completed on a standalone VPS template."

The Code however states that "If you make a personal statement, you can request a copy from the police". Whilst we appreciate that the use of a VPS template will assist practitioners, we would have concerns if individuals were being denied their right of access due to a template not being used. Under data protection legislation, individuals have a right to request any information which relates to them. This information should only be withheld where an exemption to disclosure applies. Any information which falls under an exemption should be redacted from disclosure rather than access to an entire document being restricted.

The right of access, in data protection terms, therefore needs to be considered in conjunction with the disclosure of the VPS, and this should be clarified in the practitioners' guidance. Information should only be withheld from disclosure in cases where an appropriate exemption can be applied.

Data Sharing

In our response to the first consultation, we made reference to data sharing and outlined our concern that data protection legislation is sometimes wrongly cited as a barrier to data sharing. Rather, it should be viewed as a framework of safeguards to ensure fair, lawful and proportionate data sharing. We acknowledge the references to improved data sharing where it is appropriate in order to allow the flow of information through the criminal justice agencies under Right 4. The Code may benefit from providing further clarity to victims about when they can expect their data to be shared and what types of data would be shared.

Appropriate data sharing arrangements must be in place, to ensure compliance with legislation and ensure mutual responsibilities are clearly understood. The Information Commissioner is currently updating her Data Sharing Code of Practice to reflect changes in data protection legislation, following a formal consultation last year. Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing large volumes of what is often sensitive (special category and criminal offence data).

Article 10 GDPR

It is important to note that where data is processed under GDPR, the rules for special category data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal

data relating to criminal convictions and offences, or related security measures which are set out in Article 10, and this also applies to the processing of the data of victims of crime. The Information Commissioner is currently drafting detailed guidance relating to the processing of Article 10 data with the aim of publishing later this year. This guidance should be considered when drafting the practitioners' guide.