Information Commissioner's Office

Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

The Information Commissioner's response to the Department of Health and Department of Justice NI joint consultation on a Draft Domestic and Sexual Abuse Strategy 2023-2030

Introduction

1. The Information Commissioner's Office (ICO) is pleased to respond to the Department of Health (DoH) and Department of Justice (DoJ) joint consultation in relation to a Draft Domestic and Sexual Abuse Strategy 2023-2030.

2. The ICO regulates the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000 (FOIA), among other pieces of legislation.

3. The ICO is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO does this by providing guidance to individuals and organisations, solving problems where we can, and taking appropriate action when the law is broken.

4. Data protection legislation protects individuals' personal data rights. When personal data is lost, stolen, or used inappropriately it can lead to harm, distress and negative impacts on personal rights and freedoms. Strong personal data protection policies and procedures should be a central feature of a strategy for victims of domestic and sexual abuse so as to minimise the risk of additional harms or distress to vulnerable individuals and families.

5. The content of the draft Domestic and Sexual Abuse Strategy is closely aligned with the Information Commissioner's Opinion 'Who's Under Investigation? The processing of victims' personal data in rape and serious sexual offence investigations'. We would recommend that you consider this Opinion, and the recommendations therein, as you work towards finalising this strategy.

The different legal frameworks

6. Whilst the UK GDPR applies to the general processing of personal data, there is a separate data protection regime that applies to certain authorities when processing personal data for law enforcement purposes.

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

7. Law enforcement processing is instead covered under Part 3 of the DPA 2018. The law enforcement purposes are defined in the DPA 2018 as "*the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including safeguarding against and prevention of threats to public security*".

8. Each of the two regimes have their own requirements in terms of the lawful bases/conditions for processing that organisations can rely on to process personal data, the rights that are afforded to data subjects and general compliance requirements.

9. It will be important for all agencies involved in this strategy to be aware of the correct legislative regime that applies to their processing.

Data Protection Impact Assessment

10. A Data Protection Impact Assessment (DPIA) is a process that helps data controllers identify and minimise the data protection risks of a project or processing operation. Article 35(1) of the UK GDPR sets out that: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purpose of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*."

11. The multi-agency approach outlined within the draft strategy will, by its very nature, involve the processing of highly sensitive personal data (including special category data) which, if lost, stolen, disclosed or used inappropriately could lead to a high risk to the rights and freedoms of the individuals involved.

12. While the Multi-Agency Risk Assessment Conference (MARAC) Operational Board has existed for some time, the draft Strategy appears to suggest that new bodies will be created to assist in bringing the work of the strategy forward, including a multi-agency Expert Reference Group and multi-agency Task and Finish groups.

13. A DPIA will be an important tool to confirm the roles and responsibilities of the agencies and bodies already involved in this

work, and to set out the roles and responsibilities of the groups to be created.

14. Undertaking a DPIA will aid the process by providing clarity on areas such as what kind of personal data is shared and why; the role of the different agencies involved and whether any joint controllership arrangements exist; what happens to personal data after it has been shared; whether sharing and further processing is necessary, proportionate and lawful and help the agencies involved identify less risky ways to use and share this personal data whilst still fulfilling the objectives of the multi-agency assessment process to keep victims safe.

15. Completing a DPIA will also assist the agencies involved in the delivery of the strategy with their obligations under the UK GDPR and DPA 2018 in relation to accountability for how they are meeting their data protection obligations, implementing data protection by design and default.

16. It is therefore recommended that a DPIA is carried out on the strategy and any policy proposals arising from the strategy. A DPIA will help ensure that proposals improve outcomes for victims of domestic and sexual abuse and their families, whilst also protecting their personal data rights (and those of the perpetrator).

17. It is also recommended that the individual agencies involved carry out their own DPIAs on the risks arising from their particular involvement in the processing in order to identify appropriate measures to take to minimise those risks to the rights and freedoms of individuals involved.

18. Should any of the DPIAs identify a high risk that the agencies cannot mitigate, they must consult with the ICO in relation to the proposed processing, in accordance with Article 36(1) of the UK GDPR.

Data sharing

19. There are data sharing references and inferences throughout the draft strategy, as part of the overall strategic aim for stakeholders to work together in tackling domestic abuse and violence.

20. Data protection law enables organisations to share personal data securely, fairly and proportionately. It will be important for organisations engaged in data sharing connected with this area of work to bear in mind the ICO's Data sharing code of practice, which goes into more detail on the steps that organisations need to take to share data, while protecting people's privacy.

Considerations for data sharing under Part 3 of the DPA 2018

21. While most data sharing is covered by the general processing provisions under Part 2 of the DPA 2018 and the UK GDPR, data sharing by a competent authority for specific law enforcement purposes is subject to a different regime.

22. Competent authorities will instead have to look to Part 3 of the DPA 2018, which provides a separate but complementary data sharing framework. However, there are common elements to both regimes which means that data sharing processes under either Part 2 or Part 3 can be adapted, rather than having to start a new process.

23. Particular care should be taken in cases where competent authorities wish to share information collected for law enforcement purposes with other agencies for non-law enforcement purposes. This is due to section 36(4) of the DPA 2018 which states that "*personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law"*.

24. Section 36(4) may therefore prevent the PSNI and other law enforcement agencies disclosing information collected for law enforcement purposes to the other agencies without it being authorised by law (such as statute, statutory Code of Practice or common law).

25. It is therefore imperative that there is a clear legislative basis for multi-agency information sharing involving personal data collected for law enforcement purposes.

26. The ICO's Data sharing code of practice contains a section specifically on law enforcement processing in a data sharing context. The ICO has produced additional guidance on sharing

personal data with law enforcement authorities within our data sharing information hub, which provides helpful checklists, tools and case studies to make it easier for law enforcement bodies, as well as other organisations, to request and share personal data with confidence.

Data sharing agreements

27. It is best practice to put in place data sharing agreements between the agencies involved. These agreements should be based upon the ICO's Data sharing code of practice.

28. Below are some areas that data sharing agreements should take into account. Please note that whilst the legislative references that follow below are particular to data sharing under the general processing provisions of Part 2 of the DPA 2018 and UK GDPR, the same general principles will apply to data sharing under Part 3 of the DPA 2018 for law enforcement purposes, subject to the specific nuances within those provisions.

Lawful basis

- Personal data must be processed in a lawful, fair and transparent manner. This means that processing must have a lawful basis as set out under Article 6 of the UK GDPR. If the data in question includes 'special category' data, a condition under Article 9 of the UK GDPR must also be met for processing to be lawful.

- If the data relates to criminal convictions or offences then additional safeguards must be in place and under Article 10 of the UK GDPR it can only be shared if UK law permits. The DPA 2018 sets out the relevant UK law covering this type of processing in Schedule 1.

- The lawful basis for sharing personal data relating to multiple parties (the victim, the perpetrator, other family members) should be established on a case by case basis according to the type of personal data, who it relates to and the purpose for sharing.

- As detailed in the Information Commissioner's Opinion 'Who's Under Investigation?', it is unlikely that consent will be an appropriate basis/condition to rely on for lawful processing and reliance on consent statements from victims and witnesses is not appropriate.

The UK GDPR sets a high standard for consent. For example, a controller must be able to demonstrate that a victim's consent is freely given. This may be difficult to demonstrate where power imbalances exist e.g. between victims and the police or other professionals.

- Whether the agency involved is a public body or a third or private sector body may also have a bearing on the lawful basis and indeed the lawfulness of certain types of data sharing.

Transparency

- Agencies must also comply with the transparency requirements of the UK GDPR. The requirements vary according to whether data was obtained from the individual directly or via a third party. Article 13 of the UK GDPR sets out what information individuals should be provided with where data has been obtained directly from them, and Article 14, where it has not.

- This 'privacy information' includes details of what kind of personal data is being processed, the purposes of processing and which organisations or bodies that information is being shared with.

- These requirements, could, in certain circumstances, prejudice the multi-agency assessment process. There are exemptions available that may be relied on in these cases. For example, Article 14(5)(b) of the UK GDPR sets out that the requirements do not apply when the provision of this information to the individual is likely to "*render impossible or seriously impair the achievement of the objectives of that processing*". Schedules 2, 3 and 4 of the DPA 2018 contain further exemptions which can be considered on a case-by-case basis.

Data minimisation

- Article 5(1)(c) of the UK GDPR sets out the principle that data processing should be adequate, relevant and limited to what is necessary. This means that agencies must ensure they only share the personal data which is necessary and proportionate to achieve their purpose.

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Storage limitation

- Article 5(1)(e) of the UK GDPR sets out that personal data should only be kept in a form that permits identification of individuals for as long as necessary. The factors that determine appropriate retention periods will vary according to the type of data and circumstances involved. Data sharing agreements should set out in more detail the factors that determine how long this should be, as well as the procedure for dealing with cases where different organisations have different statutory or professional retention periods.

Integrity and confidentiality

- Article 5(1)(f) of the UK GDPR sets out that personal data should be processed in a manner that ensures appropriate security against unlawful or unauthorised processing, accidental loss, destruction or damage.

- Data sharing agreements should set out how this will be achieved and include detail about the technical and organisational arrangements for secure transmission of the data and procedures for dealing with a data breach. Getting the basics right is, in this context, as important as the technical fixes.

- A personal data breach is defined as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*". Personal data breaches which are likely to result in a risk to individuals' rights and freedoms must be reported to the ICO within 72 hours of establishing that the breach has taken place. Where the breach is likely to result in a high risk to individuals' rights and freedoms, the duty to report also extends to the those individuals affected.

- Data sharing agreements should set out the procedures for detecting, investigating, managing and reporting breaches of personal data shared by the relevant agencies, both in terms of reporting to the ICO and affected individuals.

- The requirement to communicate a personal data breach could, in some circumstances, place a criminal investigation at risk. For

example, if it means informing third parties (such as the perpetrator) that they are being discussed.

- Schedule 2 of the DPA 2018 sets out exemptions to Article 34(1) and (4) of the UK GDPR (the requirement to communicate a personal data breach to affected individuals), with Schedule 2, Part 1 providing an exemption where personal data is being processed for the prevention or detection of a crime.

Data protection and personal data rights

- Data sharing agreements should set out clearly the personal data rights of the victim, their family and the perpetrator and how these will be upheld. The obligation to uphold these rights applies to each of the agencies processing shared data.

- If it is determined that the agencies involved are joint controllers then consideration should be given to how best to facilitate individuals in exercising their data rights. This may involve identifying a coordinator to take overall responsibility.

Accountability

- Each agency must be responsible for and be able to demonstrate compliance with the six data protection principles set out in Article 5(1) of the UK GDPR. Having a DPIA and appropriate data sharing agreements in place will aid the agencies involved in demonstrating accountability.

Dissolution

- Data sharing agreements should set out a clear procedure for when the data sharing arrangement is dissolved and what should happen to any shared data held by partner organisations.

Data and research

29. The draft Strategy sets out that "*data and research*" on the prevalence of domestic and sexual abuse specific to Northern Ireland is "*insufficient, with limited potential*" and that this is an issue to be considered further.

30. As part of these considerations, agencies should bear in mind the research and statistics exemption set out within Schedule 2, Part 6, Paragraph 27 of the DPA 2018.

31. It will also be important for agencies involved in this work to be mindful of whether the data they are processing constitutes personal data or not.

32. Personal data is information that relates to an identified or identifiable living individual. What identifies an individual could be as simple as a name, number or other identifiers. Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of the UK GDPR. Only information which is truly anonymous is not covered by the UK GDPR.

33. The ICO has produced detailed guidance on determining personal data which will be useful in relation to the above. In relation to guidance on anonymisation, we are working to update existing Data Protection Act 1998 guidance to reflect the UK GDPR provisions. In the meantime, existing guidance on anonymisation is a good starting point.

Children and vulnerable individuals

34. Victims of domestic and sexual abuse are likely to be vulnerable, and may also include children and young people, which is an additional vulnerability. The UK GDPR states that "*children merit specific protection with regard to their personal data*".

35. Agencies must work to ensure that the needs of such vulnerable individuals are met. The ICO's Strategic Plan (ICO25) is concerned with ensuring a better understanding of how the personal information of vulnerable individuals is used and accessed, with specific reference to children.

36. As part of meeting the needs of vulnerable individuals, including children, agencies must ensure that those individuals are aware of how their personal information is being used as part of the process, and their rights in relation to this processing.

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

37. The right to be informed and the importance of providing appropriate privacy information will be crucial to meeting the needs of these individuals.

38. For all individuals, Article 12 of the UK GDPR requires organisations to provide information to them in a way that is concise, transparent, intelligible, easily accessible, and uses clear and plain language. In relation to children's personal data, particular care must be taken to ensure that the information provided to them is appropriately written, using clear and plain language that a child would understand.

Given the links between this draft Strategy, the Information Commissioner's Opinion 'Who's Under Investigation?', and the aims set out within ICO25 to protect the most vulnerable, our office is keen to provide further assistance to the DoJ and/or the DoH on this area and any others of a similar nature. We would be happy to meet with you to discuss this further.

Should the DoH or DoJ require clarification on any of the points made within this consultation response, please do not hesitate to contact us on 0303 123 1114 or by email at ni@ico.org.uk.