The Information Commissioner's response to Domestic Abuse consultation

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK. 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. She welcomes the opportunity to respond to this Consultation.

Many of the Consultation questions fall out of the scope of the Information Commissioner's regulatory role as they are directed towards organisations that deal directly with domestic abuse. For this reason key data protection points are addressed below rather than using the questionnaire. Where possible, the headings used in the Consultation are maintained.

The Information Commissioner recognises the importance of preventing domestic violence, protecting victims and prosecuting perpetrators. Data protection law provides a framework for controllers of personal data to apply appropriate safeguards to protect it. This is particularly important in this context, given its sensitivity and the potential for harm if there is inappropriate disclosure, or loss.

The Consultation refers to the Data Protection Act 1998. This has now been superseded by the Data Protection Act 2018. On 25 May 2018 the GDPR (General Data Protection Regulation) came into effect. Stakeholders handling domestic abuse cases will need to refer to both pieces of legislation. The ICO has already published a substantial amount of guidance about the new legal framework for data protection[1].

Under the new laws, there are obligations requiring controllers to conduct DPIAs (data protection impact assessments) in certain circumstances. A DPIA is a process designed to help systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of a controller's accountability obligations under the new framework and demonstrates how you comply with data protection obligations. Detailed guidance on DPIAs[2] has recently been published on the ICO website. It is

[1] https://ico.org.uk/

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

highly likely that the processing of personal data related to domestic abuse will require a DPIA, for example, Domestic Abuse Court Orders and the Domestic Violence Disclosure Scheme. If there are to be changes in the legislative framework addressing domestic abuse then there are new obligations for government to consult with the Information Commissioner. Article 36 (4) of the GDPR sets out that:

Member states shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

Further engagement with the Information Commissioner at the drafting stage would help ensure that compliance will be addressed at that early stage, which should support practitioners further down the line.

The new legislation also includes new obligations for controllers regarding information rights for individuals, including the right to be informed; the right of access and the right to rectification. The application of these requirements needs to be given particular attention in the context of domestic abuse, recognising the importance of victims being able to trust organisations that are handling their personal data. Lines of responsibility also need to be clear to data subjects so that they can check the information which is being held about them.

Introduction of a new statutory definition of domestic abuse

The Information Commissioner welcomes the proposal to introduce a new statutory definition of domestic abuse as this should provide clear boundaries for controllers who are processing personal data for purposes related to domestic abuse:

Any incident or pattern of incidents of controlling, coercive, threatening behaviour, violence or abuse between those aged 16 or over who are, or have been, intimate partners or family members regardless of gender or sexual orientation.

The abuse can encompass, but is not limited to:

- *psychological*
- *physical*
- *sexual*
- *economic*
- *emotional*

This measure should support consistency and clear purpose across agencies. A statutory definition could provide legal certainty which would

help organisations when identifying a lawful basis for processing in data protection law.

It is also noted that government are proposing to accompany the legislation with underpinning statutory guidance. The Information Commissioner would welcome the opportunity to contribute to the work developing this statutory guidance by offering expertise on compliance with data protection law for practitioners.

Reporting domestic abuse to statutory agencies

Data protection is sometimes wrongly cited as an absolute barrier to data sharing. Instead, data protection law should be more correctly viewed as a framework of safeguards for fair and lawful processing including proportionality; clear purposes; data quality assurances and ensuring that appropriate security measures are in place.

There are provisions in data protection legislation to allow for the disclosure of personal data but these need care and should be underpinned by clear policies within organisations. A legal gateway would provide certainty to agencies needing to share personal data in this context. Given the nature of data related to domestic violence, there is significant potential for harm to the individual if things go wrong. When making decisions about sharing, controllers should also take into account that there may be risks for individuals when personal data *isn't* shared.

It is helpful that there are already considerations about which organisations would fall in the scope of being a "relevant" third party (which, of course, will vary from case to case). This encourages a framework around the sharing which should reduce the risks of excessive sharing and heightened risks of inappropriate disclosures. All links in the chain need to understand their obligations to data protection and appropriate security measures need to be in place.

The Information Commissioner has published the Data sharing code of practice[3] to support controllers making decisions in this aspect of processing. This will be reviewed to reflect changes in the legislation

Domestic abuse protection order

Electronic monitoring (for example location or alcohol monitoring) of perpetrators is identified as one of the measures that could be attached to the new order. Under new data protection laws it is highly likely that this would require a DPIA which would assess proportionality and unpick data protection compliance risks, for example determining whether continuous monitoring could be justifiable. Controllers with responsibility for

[3] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

monitoring should also ensure that they procure systems that enable them to be compliant with the law.

The Information Commissioner's understanding is that it would be for the court to decide the issue of necessity and proportionality of monitoring before making such an order. It should do so in the knowledge of the capabilities of the process. For example, if it was mandating 24 hour surveillance, it should be satisfied that this meets the necessity and proportionality test under Article 8 in doing so. That would then likely render the collection lawful, provided the data subject was also fully informed of the consequences and implications of the tagging and could modify their behaviour accordingly, if they chose.

Domestic Violence Disclosure Scheme (DVDS)

The consultation proposes to put the guidance underpinning the DVDS into law. The Information Commissioner can see the value of it being given legal certainty. The Information Commissioner responded to the consultation on the DVDS in 2012. Since then, it would be expected that the Scheme will have been embedded and that there will be a substantial body of evidence to inform its effectiveness. It is important that this empirical evidence is considered and it is hoped that the responses to the consultation will provide this.

In 2012 some of the key points the Information Commissioner raised concerned the fairness (openness) of processing and striking a balance between this and anonymity; clear guidelines for practitioners to ensure that data is processed securely and assessing legitimacy of requests for disclosure. These points still stand, and it would be a prudent to review these points and others in the light of current insights, and before the Scheme takes on a statutory footing. For information, a copy of our response is attached to this response.

Online threats and the role of technology in domestic abuse

The Information Commissioner has recently published her Technology Strategy[4] for the next three years. In it, she commits, among other things, to engage with other organisations to embed data protection by design in new initiatives. She is also interested in collaborating on work that raises public awareness about privacy settings on social media. In challenging contexts, such as domestic abuse, it would be worthwhile collaborating on how victims of domestic abuse and other vulnerable adults can be better supported to manage online risks.

[4] https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/

Improving performance using data

A number of suggested priorities are set out in the consultation document:

☐ Improving the collection and reporting of data on when domestic abuse is a feature of a case/intervention

☐ Improving collection and reporting of data relating to the gender and relationship of the perpetrator and victim

☐ Improving data to enable better tracking of outcomes in domestic abuse cases/intervention

☐ Linking data to enable better tracking of interventions and reoffending

☐ Linking data to enable better understanding of the interactions/relationships between domestic abuse and other types of offending

☐ Other (free text)

☐ None of the above

☐ Don't know/No answer

Depending on how this is taken forward, as broad initial comments, the Information Commissioner would support the first point, as in any case, this must be compliant with the framework that is provided by data protection law. Clear benefits can be derived from improving data quality, and this should connect with purposes for processing the data, and ensure its relevance. Tracking of outcomes would be welcome, and should inform future work on deciding justification, effectiveness, proportionality and necessity. This evidence is often lacking, so improvements in this area should be encouraged. Similarly, linking data to prevent reoffending could have clear value, but measures should be in place to avoid function creep, and if there are initiatives to expand this into the scope of automated processing or profiling, then a new DPIA should be conducted in order to review its compliance.

Elizabeth Denham

Information Commissioner

29 May 2018