

The Information Commissioner's response to the Department of Justice consultation on the 'Draft Modern Slavery & Human Trafficking Strategy'

Introduction

1. The Information Commissioner is pleased to respond to the Department of Justice (DoJ) consultation regarding its 'Draft Modern Slavery & Human Trafficking Strategy'.
2. The Information Commissioner's role includes the regulation of 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. When considering the proposed questions in the consultation document, we identified a number of common data protection themes and have detailed our comments below for your consideration.
3. We acknowledge that this long-term modern slavery and human trafficking (MSHT) strategy has been drafted in accordance with the DoJ's obligations under the Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015 as amended by the Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022.
4. The overall aim of the strategy seeks to "*Equip Northern Ireland to identify and eradicate*" MSHT through three strands known as the three P's: *Pursue, Protect* and *Prevent*. Each strand requires or considers the processing of personal information.

Article 36(4) and the statutory obligation to consult with the ICO

5. Objective 1.1 seeks to "*ensure that modern slavery legislation is used effectively and remains relevant and fit for purpose*". As a consequence of this commitment, we understand that amendments to the 2015 and 2022 Acts could be implemented. We would therefore like to draw your attention to the DoJ's potential obligation under Article 36(4) of the UK GDPR.

5. Article 36(4) of the Regulation states: "*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*".
6. If a decision is made to amend legislation, the DoJ may need to initiate the requirement to consult with our office. Your [Data Protection Officer](#) (DPO) will be able to guide you on this, including providing assistance with regards to completing the Enquiry Form, which can be found [here](#).

Data protection by design and default

7. The DoJ must adhere to its obligations under [data protection by design and default](#) as outlined in Article 25 of the UK GDPR. Not only would compliance with this provision help ensure that personal information is appropriately safeguarded but it should also assist in building trust among the multi-agency partnership and victims of MSHT.
8. This approach requires the DoJ to seek expert advice from its DPO with regards to the proposed strategy. Part of the DPO's role under the UK GDPR is to advise and inform their organisation of their obligations under data protection laws.

Data Protection Impact Assessments (DPIAs)

9. Implementing data protection by design and default also requires the DoJ to develop a set of practical actionable guidelines by the assessment of risk posed under the draft strategy. For this reason, the DoJ should undertake, and regularly review, [Data Protection Impact Assessments](#) (DPIAs) in relation to initiatives which involve the processing of personal data.
10. DPIAs are a statutory requirement when processing presents high risks to the rights and freedoms of individuals. One criteria which necessitates a DPIA relates to personal data processing activities pertaining to [vulnerable individuals](#). Children are regarded as

vulnerable when their personal data is being processed as they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences. This can also be true of other vulnerable sections of the population such as victims of MSHT.

11. When processing activities do not present a high risk to individuals, the ICO advises that DPIAs are undertaken as a matter of 'good practice'. This is because they can help map out processing activities and demonstrate why the processing is necessary and proportionate to the purposes of processing.

Open and transparent processing

12. Processing personal data in an open and [transparent](#) manner is also key to securing and maintaining the trust of victims of crime. When appropriate, the DoJ must ensure that they, and organisations within the multi-agency partnership, clearly communicate their processing activities to individuals in a way which is easily accessible. This is to ensure that individuals are informed about how their personal data will be used, and understand their rights in relation to it.

Data sharing

13. The ICO recognises that the success of pursuing and preventing crimes relating to MSHT will be influenced by data sharing practices. It is important to note that data protection law is not a barrier to sharing personal data when it is necessary and proportionate to do so. Rather, data protection provides a framework to ensure that information is shared in a fair manner.
14. Whilst tools such as a [Data Sharing Agreement](#) (DSA) and/or Memorandum of Understanding (MoU) are not statutory requirements, they can help form and demonstrate compliance with the data protection legislation. We therefore recommend that the DoJ consider the benefits of implementing a DSA and/or MoU if it has not already done so. For further guidance pertaining to data sharing, please visit our [Data Sharing Information Hub](#).

The UK National Referral Mechanism

15. The consultation document explains that if a victim of MSHT does not provide their consent, their personal data cannot be uploaded on to the UK National Referral Mechanism (NRM). As per the consultation, we understand that the NRM process ensures victims receive appropriate support and assistance but it is also a mechanism for accruing and processing data about trafficking and exploitation in Northern Ireland.
16. However, section 4.24 of the strategy details that an anonymous referral to the NRM could be made under section 13 of the 2015 Act. Under this section, the referral could be made without the consent of the individual. This approach would continue to facilitate the collection of information pertaining to MSHT in Northern Ireland.
17. Having considered the information available in the consultation document, it is not clear whether individuals must consent to the NRM *process* or whether consent relates to the [lawful basis of processing](#) under data protection law. As such this must be made explicitly clear to avoid unnecessary confusion. More so, if consent has been identified as the lawful basis for processing, then we recommend that consideration is given to whether this is the most appropriate basis.
- 18.** With regards to anonymous data, information which has been truly anonymised falls outside the scope of the data protection legislation. However, the DoJ and organisations within the multi-agency partnership must ensure that individuals cannot be identified directly or indirectly from the data. This includes identification through a 'jigsaw' technique whereby the integration of two or more systems/sources provides enough information for an individual to be identified. We therefore recommend that the DoJ review our [draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies](#).

Expunging convictions for MSHT victims

19. Objective 1.1 stipulates that consideration will be given to "*expunging convictions for MSHT victims who have been unfairly prosecuted following forced exploitation / prostitution*". When considering this commitment, it will be important for the DoJ to detail the qualifying criteria for expunging convictions and prosecutions. This includes identifying which type of offences would be eligible to be expunged and from which dates.
20. During the assessment of the qualifying criteria, the DoJ must consider its proposals in relation to the data protection principles, specifically the [lawfulness, fairness and transparency principle](#). This includes recording and assessing the risks and harms associated with the processing of personal data, for instance, could the criteria unfairly discriminate against, and have adverse effects upon, particular individuals or groups?

Data protection training

21. Objective 1.3 seeks to ensure "*effective development, learning and identification of best practice across the criminal justice system*" and will involve training relating to MSHT, including but not limited to, vulnerable witness training for solicitors.
22. We are of the view that training and guidance should be extended to data protection and personal information handling practices. The training should be issued at the beginning of an individual's career and refreshed at regular intervals. You may find [the ICO's online training resources](#) of use in this regard.