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 on 'Violence and Aggression in the Workplace'

## Introduction

1. The Information Commissioner is pleased to respond to the Department of Health (DoH), regarding its public consultation on 'Violence and Aggression in the Workplace'.

2. This Office has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the UK Data Protection Act 2018 (DPA 2018) and additional information rights legislation. Given our role as a regulator, it would not be appropriate for us to respond with a view on the different questions and options proposed within the online survey. However, there are data protection and information governance implications in the proposals which we have raised below for your consideration.

3. The Violence and Aggression in the Workplace Framework outlines the HSC commitment in partnership with staff representatives, to ensure the prevention, reduction and management of violence and aggression towards staff in the workplace. The framework also aims to ensure that associated structures, policies and support are in place to enable staff to work safely. We understand that the framework applies to all HSC staff, students and volunteers.

4. Whilst implementing the proposed framework, HSC organisations will need to consider their compliance with the data protection legislation including confidentiality, data security, and the right to be informed. Consequently, our response to the consultation will predominately relate to the provision of guidance which the DoH may wish to communicate to those implementing the policy.

## Involvement of Data Protection Officer

5. HSC organisations should be advised to seek expert advice from their Data Protection Officer (DPO) during the implementation of the framework. Part of the DPO's role under the UK GDPR is to advise and inform their organisation of their obligations under data protection law.

## Data Protection by Design and Default

6. To ensure that the proposed framework is implemented in an appropriate manner, DoH should consider reminding organisations of their



Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

obligations under data protection by design and default under Article 25 of the UK GDPR. Implementing technical and organisational measures at the initial phases of the design process and operation could lead to the safeguarding of privacy and data protection principles from the onset of this policy.

**Data Protection Impact Assessment**

7. HSC organisations need to consider carrying out a Data Protection Impact Assessment (DPIA) covering how they plan to process personal data in relation to the Violence and Aggression in the Workplace Framework. There is guidance available on our website about conducting a DPIA.

8. Article 35(1) of the UK GDPR requires controllers to carry out a DPIA prior to conducting processing that are likely to result in a high risk to the rights and freedoms of individuals. It is for the controller to determine whether the threshold of requiring a DPIA is reached. Our guidance expands on what factors organisations should consider in this regard.

9. In addition, section 1.2 of the draft framework recognises that illnesses and mental capacity may also lead to unintentional incidents of violence and aggression. If these incidents are similarly captured under this framework, then consideration should be given to Article 35(3) of the UK GDPR which states that a DPIA is required if there is processing of data concerning vulnerable data subjects.

10. Furthermore, it is generally good practice for controllers to complete a DPIA to analyse the proposed processing and help identify and minimise data protection risks. A DPIA does not have to indicate that all risks have been eliminated but rather help controllers document and assess whether or not any remaining risks are justified.

**Data Sharing**

11. The framework makes reference to sharing information with other bodies, for example, the Police Service of Northern Ireland (PSNI). There may be instances of uncertainty as to whether organisations can lawfully disclose personal data to third parties. For this reason, DoH should advise controllers that our online toolkit may aid their decision-making process in such instances. The toolkit is designed to help controllers to understand whether a disclosure is likely to be compliant with the data protection



Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

legislation. Our guidance regarding sharing personal data with law enforcement authorities will also be of use.

*Data Sharing in an Emergency*

12. Data protection law allows organisations to share personal data in an urgent or emergency situation, including to help them prevent loss of life or serious physical, emotional or mental harm. In an emergency, it is advisable that you share as much data as is necessary and proportionate.

13. However, urgent situations maybe foreseeable and for this reason controllers should forward plan to ensure that they are well prepared to handle such events appropriately. Whilst the proposed framework helps to identify when an individual should contact PSNI, DoH must remind HSC organisations that they will need to build upon the framework and implement relevant policies, procedures and training resources to help prepare staff for urgent situations and swiftly identify what types of data will likely be relevant for sharing.

14. To demonstrate compliance with the accountability principle, HSC organisations must document the personal data processing and data sharing which occurred during and after the emergency situation. The record should be completed as soon after the event as possible, if not during.

15. We have published further guidance about data sharing in an urgent situation or in an emergency on our website.

*Frequent Sharing of Personal Data*

16. When there is a need to share data on a **more frequent** or larger scale basis, having a data sharing agreement in place is a way that allows organisations to share information quickly and lawfully. A data sharing agreement may be appropriate between HSC organisations and/or PSNI. Further guidance on this matter has been published in our Data Sharing Code of Practice.

**Anonymisation and Pseudonymisation**

17. There are proposals outlined in the framework which may not require the processing of personal data such as the creation of summary evaluation reports. Consequently, the DoH and/or HSC organisation(s) must consider adopting privacy enhancing techniques to comply with the

data minimisation principle. This may be of particular importance in relation to the sharing of PIAs and also the creation and analysis of reports relating to the management of incidents.

18. Information should be anonymised when personal data is not necessary for the relevant task(s) and re-identification is not required. During the anonymisation process, it is important to consider personal information and identification in its broadest sense, taking into consideration the ability to identify a particular individual through direct and/or indirect identifiers which 'link' or 'relate' to a singular person. Controllers should also be mindful of 'jigsaw' identification whereby identification occurs through non-identifying information from a single source being combined with information from another recipient and/or system.

19. Pseudonymisation is a technique to replace, remove or transform information that identified individuals. This should be considered when information must remain personal whist also maintaining the confidentiality of an individual's identity.

**PIA Redaction**

20. Further clarification is required in relation to what information will be redacted from PIAs when they are shared internally and/or externally. We strongly advise that the DoH reviews the above section titled "*Anonymisation and Pseudonymisation*" in the event that the intention is to de-identify the information in order to safeguard the identity of individuals.

**Accuracy**

21. As part of the framework, HSC organisations may wish to record the outcomes of an alleged criminal offences reported to the PSNI, i.e., if the aggressor has been charged. However, it is important to note that such records need to be kept updated and potentially rectified for example, in instances where the outcome is overturned.

22. In addition, as far as possible, there is a need to be able to distinguish between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

**Integrity and Confidentiality (Security)**



Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

23. Given the nature of the personal information that will be processed, specific and detailed consideration should be given to ensuring appropriate security measures are implemented so that personal information is not compromised.

24. This would include both technical and organisational measures. Such measures may include comprehensive information governance documentation, granular permission access to the system(s), encryption software and audit capabilities.

**Lawful Bases**

25. HSC organisations should be reminded that they will need to consider their lawful basis, or bases, for processing under Article 6 of the UK GDPR. Additional bases for processing will need to be identified under Article 9 of the Regulation should personal information relate to special category data and/or a Schedule 1 condition for data pertaining to an alleged criminal offence or conviction.

26. DOH should assess their references to and reliance upon consent and whether this is an appropriate basis for processing data in this situation. This will be of particular importance to Section 5.3 of the framework which stipulates that confidential PIAs must only be shared when the individuals provide their consent. Accordingly, readers should be clear on the distinction between voluntarily participation in PIAs and consenting to processing. Failure to clarify this matter may inadvertently mislead or cause confusion about individual's personal data rights.

**Rights of Individuals**

27. Individuals have rights afforded to them under data protection law. These should be considered in advance of introduction of the proposed framework and in its accompanying guidance. The framework should include guidance on how these rights will be promoted and facilitated. For more information, please see our guidance on individual rights.



Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510