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 consultation on 'Raising a Concern in the Public Interest (Whistleblowing) HSC Framework and Model Policy'

Introduction

1. The Information Commissioner's Office (ICO) is pleased to respond to the Department of Health (DoH) consultation in relation to Raising a Concern in the Public Interest (Whistleblowing) HSC Framework and Model Policy.

2. The Office regulates the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000 (FOIA), among other pieces of 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 consultation document. However, there are data protection and information governance implications in the proposals which we have raised below for your consideration.

3. The ICO recognises that the proposed framework and model policy has been designed to ensure that HSC organisations have adequate measures in place to enable staff and other individuals to raise concerns in the public interest. However, whistleblowing processes include the processing of personal data and as such, the proposed framework should be read in conjunction with the data protection legislation.

4. Our response to the consultation will predominantly relate to the provision of guidance which the DoH may wish to communicate to those implementing the framework.

Involvement of Data Protection Officer

5. Given the sensitive nature of the material covered within the Whistleblowing procedure, HSC organisations should seek expert advice from their Data Protection Officer (DPO) during the initial stages of designing whistleblowing systems, policies and procedures. Part of the DPO's role under the UK GDPR is to advise and inform their organisation of their obligations under data

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

protection laws.

Data protection by design and default

6. The ICO understands that one of the most effective ways to encourage individuals to raise a wrongdoing concern is to ensure that the relevant HSC organisation have an appropriate corporate culture which reflects their intention to handle personal data with integrity and in confidence. For this reason, processes must properly reflect data protection by design and default as required under Article 25 of the UK GDPR.

Data Protection Impact Assessment (DPIA)

7. A Data Protection Impact Assessment (DPIA) is an integral tool to help strengthen data protection compliance. Whilst Article 35(1) of the UK GDPR states that a DPIA is only required in certain circumstances (such as where the processing is likely to result in a risk to rights and freedoms of individuals) it is good practice for controllers to carry out DPIAs in relation to the processing of personal data.

8. DPIAs must be kept under continuous review, including if there is a substantial change to the nature, scope, context or purposes of processing. It is therefore advised that the framework references this obligation and HSC organisations are directed to the ICO's DPIA guidance here.

Identifying personal data

9. It should be highlighted that concerns, including those raised anonymously, may include information which could lead to the identification of the whistleblower and others. Consequently, HSC organisations must give adequate consideration to personal data in its broadest sense and how to mitigate inappropriate disclosures of personal data.

10. When determining whether information is personal, controllers should consider whether an individual can be distinguished from other members of a group. The ability to identify an individual may present itself in the form of 'direct' and 'indirect' identifiers, but also

through 'mosaic' or 'jigsaw' identification. This form of identification is owing to non-identifying information from a single source being combined with information from another recipient and/or system and in the context of whistleblowing, may be of particular concern when a concern pertains to a specific incident.

11. Where organisations are uncertain if data is personal, the controller should treat the information as though it is.

Data minimisation and encouraging self-identification

12. Whilst paragraph 5.3 of Appendix A stipulates that it may be "*much more difficult*" for an organisation to investigate a concern if the identity of the whistleblower is withheld, we appreciate that there may be incidents when the identity of the reporter is not necessary. This may include instances when there is strong factual evidence to demonstrate the alleged wrongdoing.

13. For this reason, we recommend that a revised framework take steps to mitigate against unnecessary self-identification. Measures to consider could include providing a list of examples to show when self-identification may be unnecessary and ask HSC organisations to communicate this to individuals.

Data minimisation and privacy-friendly techniques

14. In the context of the whistleblowing process, including the maintenance of a central register of formal concerns and analysis reports provided to both senior management and the Audit Committee, organisations must adopt privacy-friendly practices to mitigate against the unnecessary processing of personal data.

15. When the processing of personal data is not necessary for the relevant task(s) and re-identification is not required, the information should be anonymised to comply with the data minimisation principle. In doing so, care should be taken to ensure that all data is truly anonymised Once anonymised, the data protection legislation would not be applicable.

16. Consideration should be given to pseudonymisation when identification remains necessary for the purposes of processing.

Organisations should be reminded that pseudonymised data remains personal and data protections laws will apply. Our draft anonymisation, pseudonymisation and privacy enhancing technologies guidance may be of use in this regard.

Integrity and confidentiality (security)

17. A whistleblowing platform must include technical and organisational measures to ensure the security of personal data. Such measures may include comprehensive information governance documentation, granular permission access to the system(s), encryption software and audit capabilities.

18. In addition, it is important to ensure that information about an alleged wrongdoer or witnesses are treated with them same security considerations as a whistleblower.

Lawful basis

19. HSC organisations should be reminded that they will need to carefully consider their lawful basis or bases for processing. Furthermore, the framework should provide clarification (where necessary) to determine whether consent is to be the lawful basis under UK GDPR or if references to consent relates to a different context. This may be of particular use in relation to paragraph 22 which articulates that where an individual has raised a concern in confidence, the organisation should not reveal their name or identity without the individual's consent, unless disclosure is required by law.

Consent and the Common Law Duty of Confidentiality

20. It may also be important to remind HSC organisations that personal data provided in confidence will likely attract the Common Law Duty of Confidentiality (CLDC). Failure to comply with the CLDC would likely render the processing activity 'unlawful' under UK GDPR Article 5(1)(a), otherwise known as the lawfulness, fairness and transparency principle.

Right to be informed

21. The ICO appreciates that the DoH's framework advises organisations to clearly communicate the whistleblowing process to individuals and ensure that they are made aware of any revisions to policies and procedures. This reflects the right to be informed under Articles 13 and 14 of the UK GDPR, which requires organisations to let individuals know about how their personal data will be processed.

22. To enhance the clarity around the right to be informed, it may be useful to categorise individuals and tailor information to those categories. This may help individuals to understand how their personal data is likely to be processed and what their data protection rights are.

Right of individuals

23. It would be beneficial for the proposed framework to include guidance concerning the right of individuals including the right to access, rectification, erasure, restrict processing and object.

24. In the event that a whistleblower, alleged wrongdoer or witness exercises their personal information rights, the controller should determine whether it is appropriate to uphold the request and if so, take the appropriate action which may including disclosing and/or withholding personal data, ensuring that personal data is anonymised and/or destroyed, amending data and more.