National Centre for Domestic Violence

Data protection audit report

May 2023

Information Commissioner's Office

Executive Summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Privacy and Electronic Communications Regulations (PECR) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The ICO received a complaint from a member of the public, in February 2022, following a data breach of National Centre for Domestic Violence (NCDV) personal data. The data breach had the potential to result in significant harm to data subjects so the ICO were keen to ensure appropriate measures were in place to mitigate the risk of a similar breach in future. This assurance was not fully obtained through the ICO's complaint handling process so NCDV were invited to participate in a consensual audit of their processes and procedures.

The ICO's assurance team contacted NCDV in April 2023 and NCDV accepted the audit invitation. NCDV cooperated fully and engaged well with the ICO throughout the process. The audit took place at NCDV's headquarters on 15 and 16 May.

The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which NCDV, within the scope of the audit, is complying with data protection legislation and assist NCDV in identifying and mitigating compliance risks in their current procedures. Following the complaint NCDV have been working hard to address some of the issues found through their own investigation and have enlisted the support or third party experts to advise on their overall strategy. Whilst there are several new initiatives, policies and management strategies being developed, these are not implemented yet. The audit considered what was 'in place' at the time it took place.

The scope of the audit covered the following key control areas:

a. Governance

The extent to which information governance accountability, policies and procedures, training, risk management, performance measurement controls and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.

b. Lawful basis for processing

The organisation has identified and documented appropriate lawful bases for the processing activities undertaken.

c. Transparency

The provision of clear and concise privacy information to data subjects which ensures that the organisation is transparent about their processing of personal data.

d. Data sharing

The design and operation of controls to ensure the sharing of personal data with processors or other data controllers complies with the principles of all data protection legislation.

e. Data Breach Management

The extent to which effective processes and procedures exist to ensure data breaches are identified, managed and reported in compliance to both the UK GDPR and national data protection legislation.

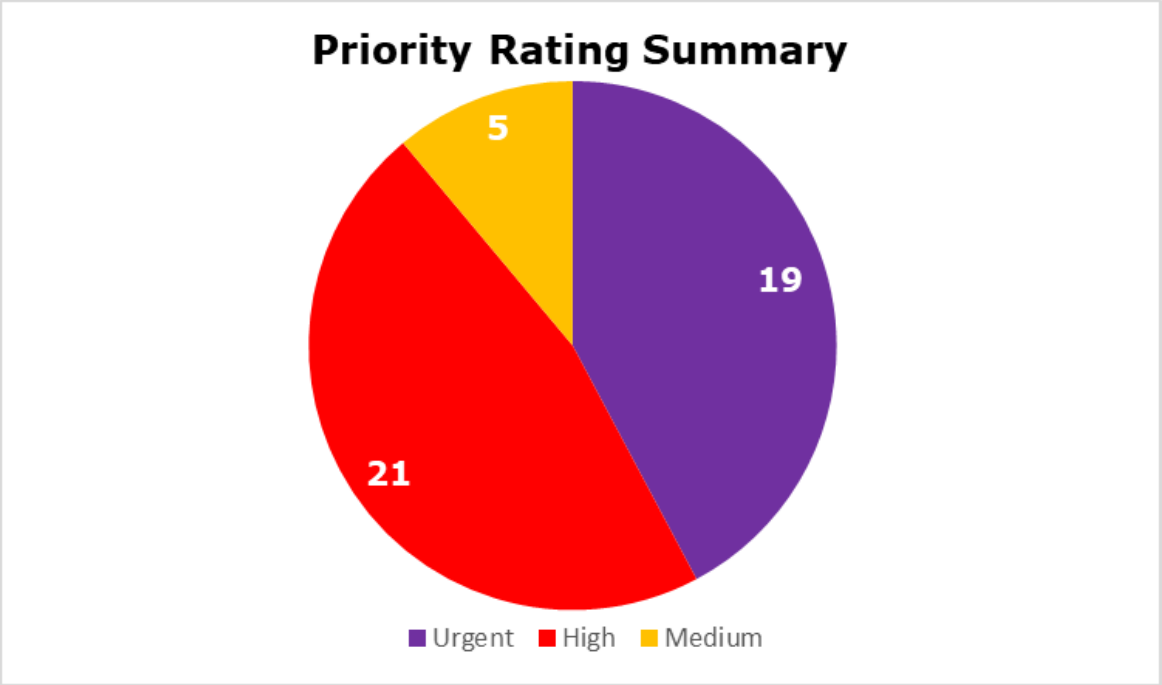
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures and interviews with selected staff.

Priority of recommendations summary

Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NCDV in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. NCDV's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Urgent priority recommendations are intended to address risks which represent clear and immediate risks to NCDV's ability to comply with the requirements of data protection legislation.

A summary of the ratings assigned within this report is shown below.



The pie chart above shows a breakdown of the priorities assigned to the recommendations made. There are 19 urgent, 21 high and five medium priority recommendations.

Areas for improvement

The ICO are encouraged by the willingness of NCDV to engage with the audit and the positive approach they have adopted to improving data protection practices. However, the audit identified some areas where further improvements are required to achieve compliance with data protection legislation.

- There is a limited technical understanding of the UK GDPR and DPA18. This means that, even where there is a desire to improve and achieve compliance, internal measures may not meet statutory requirements.

- NCDV's reporting lines and flow of information between the Board and key individuals is not sufficient to provide senior management with oversight of data protection activities and compliance.

- NCDV's data protection policies and procedures are not sufficient enough to meet the requirements of the organisation. They contain inaccurate and out of date information and are not reviewed and updated on a regular basis.

- NCDV's current data protection training does not meet the needs of the organisation and should be reviewed and updated. When the training is updated, NCDV must ensure that mandatory data protection training is delivered on a periodic basis. Furthermore, NCDV must implement specialised data protection training for staff with more specialist responsibility.

- NCDV have not clearly identified all their purposes for processing and processing activities which means that they have not been able to ensure all requirements of data protection legislation have been applied across all of their processing activities.

- NCDV do not provide data subjects with privacy information in line with the requirements of data protection legislation. This includes providing all the required information and in the correct timescales.

- NCDV's current use of consent as a lawful basis for processing is not compliant with Article 7 of the UK GDPR and therefore undermines the absolute rights afforded to data subjects under this part of the legislation.

- NCDV do not always correctly identify, based on the definitions within the UK GDPR, the processing relationship they have with third parties. This means that they may not always have correct or effective contractual arrangements in place.

- The arrangements in place with data processors are not specific enough to provide the highest level of assurance that NCDV's personal data will be handled in line with their expectations.

- Staff are not fully aware of how to identify and report a personal data breach. NCDV have a Data Breach Policy and a data breach training module within the induction training, however they both contain inaccurate information and do not provide enough guidance to ensure staff are fully aware of how to deal with a data breach.