Bedfordshire, Cambridgeshire, and Hertfordshire Police

Data protection audit report

May 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Bedfordshire, Cambridgeshire, and Hertfordshire Police (BCHP) agreed to a consensual audit of its data protection practices.

The purpose of the audit is to provide the Information Commissioner and BCHP with an independent assurance of the extent to which BCHP, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of BCHP's processing of personal data. The scope may take into account any data protection issues or risks which are specific to BCHP identified from ICO intelligence or BCHP's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of BCHP, the nature and extent of BCHP's processing of personal data. As such, the scope of this audit is unique to BCHP.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate

Audits are 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, remote interviews with selected staff, and a virtual review of evidential documentation.

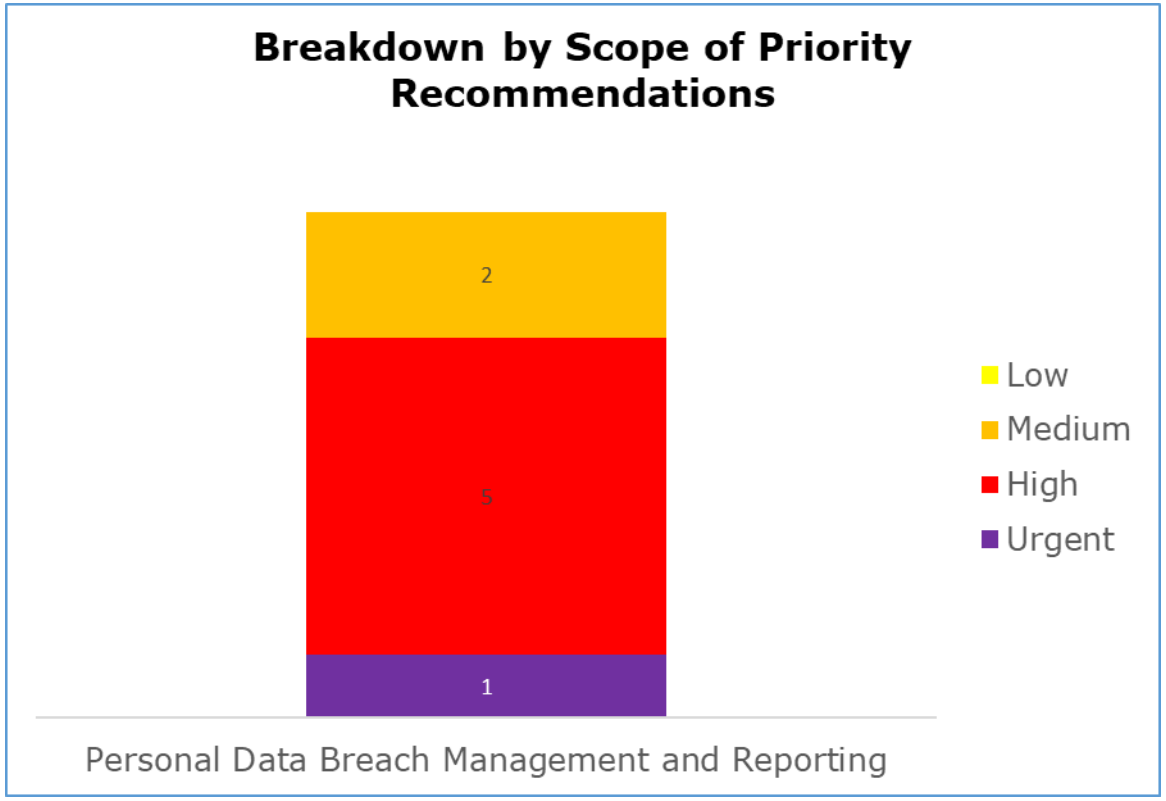
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist BCHP in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Personal Data Breach Management and Reporting	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance

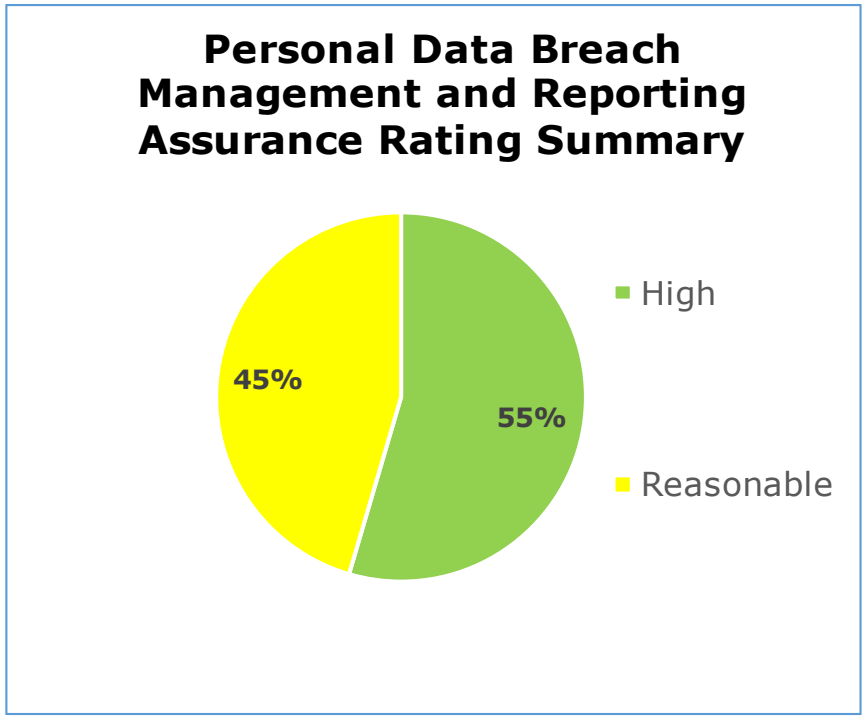
Priority Recommendations



The bar chart above shows a breakdown of the priorities assigned to our recommendations made:

- One urgent, five high and two medium priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 55% high assurance and 45% reasonable assurance.

Areas for Improvement

- Take action to ensure that all staff have completed the required mandatory refresher training packages that cover personal data breach reporting requirements and supplement this with additional training on how to complete the internal reporting form.
- Complete a training needs analysis for all staff that may be involved in making decisions about security incidents and personal data breaches, including Information Asset Owners (IAOs). The training should be completed and refreshed at an appropriate frequency.
- Conduct regular checks on the security measures of data processors, including their compliance with security incident and data breach contractual requirements. These checks should be taking place at a risk based frequency.
- Review the threshold for reporting data breaches to the ICO. Currently BCHP are not reporting all incidents or breaches that are likely to result in a risk to an individual's rights and freedoms, and the numbers of breaches they have reported are particularly low considering the sensitivity of data that may be involved. Assessments of the likely harm to individuals should be more detailed and documented, particularly when it is decided not to report them.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance, and internal control arrangements in place rest with the management of Bedfordshire, Cambridgeshire, and Hertfordshire Police.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting, or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Bedfordshire, Cambridgeshire, and Hertfordshire Police. The scope areas and controls covered by the audit have been tailored to Bedfordshire, Cambridgeshire, and Hertfordshire Police and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.