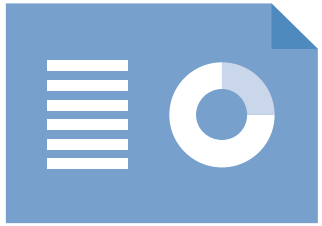
Bedfordshire, Cambridgeshire and Hertfordshire Police

Data protection audit report

January 2021

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) 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.

Bedfordshire, Cambridgeshire and Hertfordshire Police (BCHP) have a collaboration agreement in place for their shared Information Governance functions. BCHP agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 1 September 2020 with representatives of BCHP to discuss the scope of the audit.

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, and/or any data protection issues or risks which affect their 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, and to avoid duplication across scope areas. 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
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore BCHP agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 20 November 2020 to 10 December 2020. The ICO would like to thank BCHP for its flexibility and commitment to the audit during difficult and challenging circumstances.

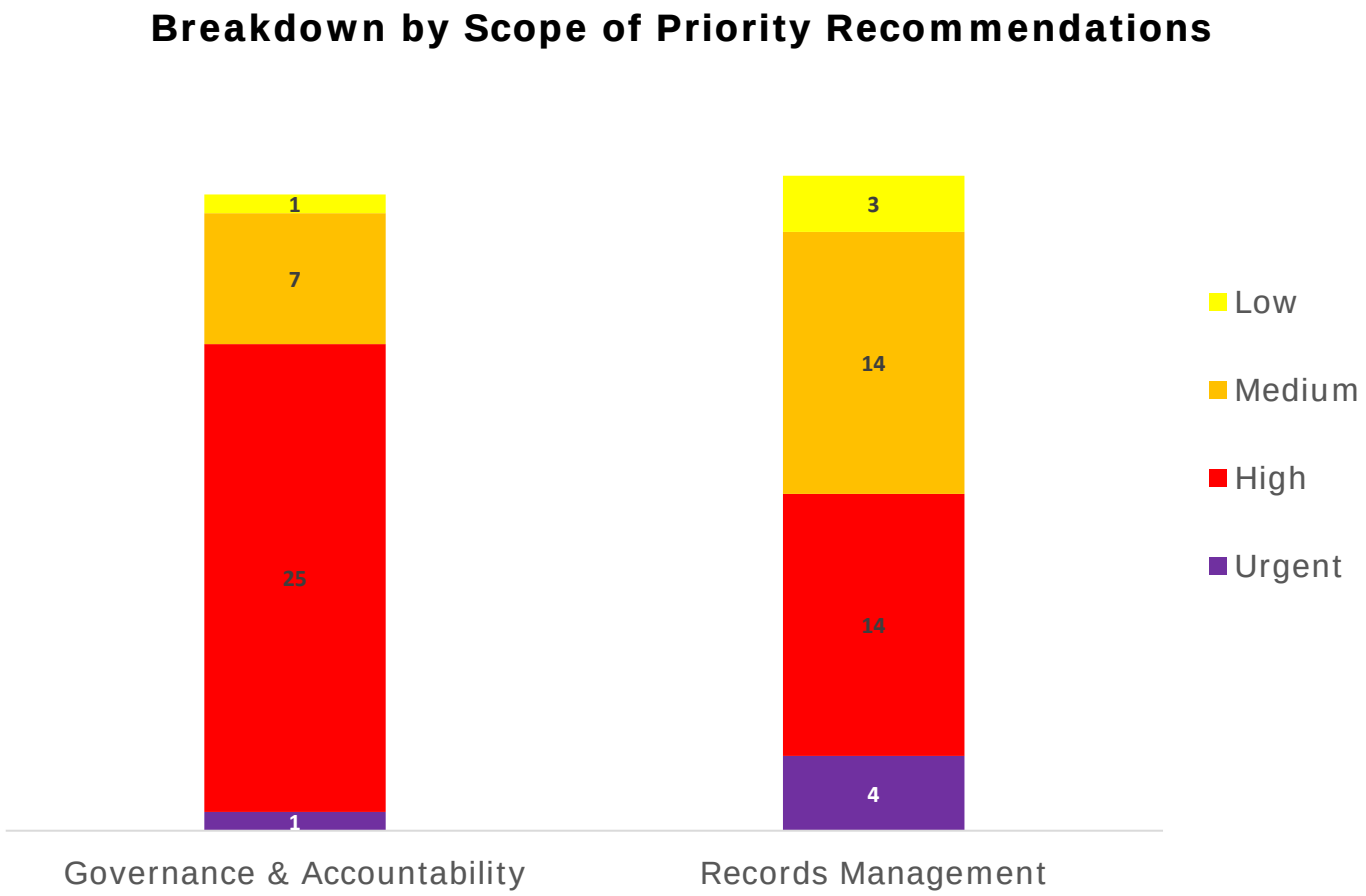
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist BCHP in implementing the recommendations each has been assigned a priority rating based upon the risks that they 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
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	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.

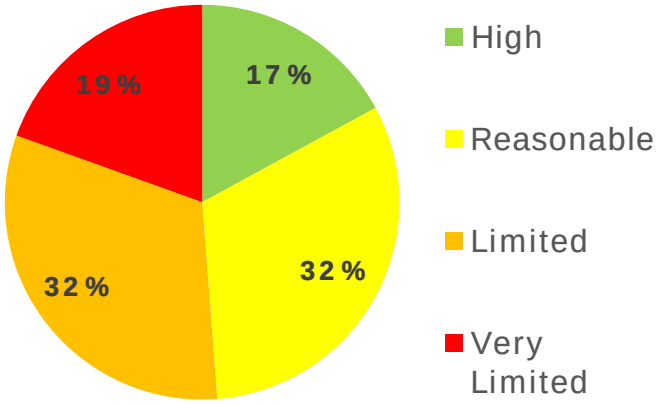
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

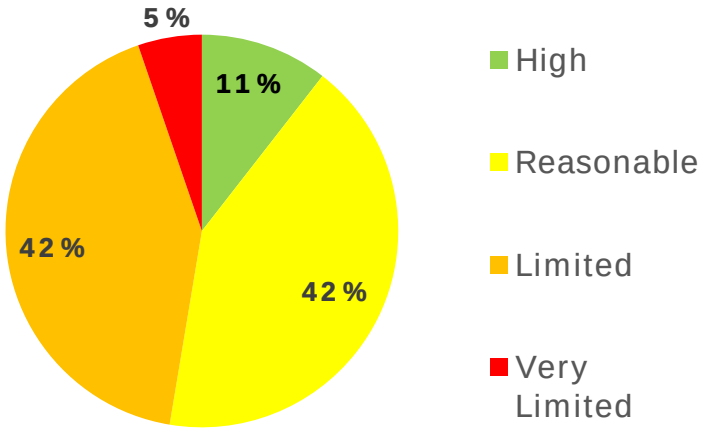


Graphs and Charts

Governance & Accountability Assurance rating summary



Records Management Assurance Rating Summary



Areas for Improvement

The Logging of automated processing systems (any IT database) needs to be completed for all BCHP systems to meet s.62 DPA18 requirements. The effectiveness of any processors logging systems should also be routinely checked.

The completion of an information audit/data mapping exercise would ensure that all data processors are clearly identified and create both a complete Record of Processing Activities (ROPA) and Information Asset Register (IAR), to incorporate all business areas across BCHP. The exercise is key to comply with Article 30 GDPR and s.61 DPA18 legislation and establishing the lawful basis for processing personal data/special categories/sensitive processing of data.

The Appropriate Policy Document should be reviewed to reflect BCHPs own retention schedule and should accurately reflect the conditions for processing used to process sensitive data.

Producing comprehensive and clear privacy notices will ensure individuals are aware why their personal data is being processed, under what lawful basis (the review of ROPA and IARs above will contribute to this) and what rights they have in relation to that processing. The privacy information should be available in other languages and formats to meet the needs of all sections of society. Where restrictions to privacy information are applied, ensure there is a documented process to ensure restrictions are applied appropriately and consistently.

Develop a Training Needs Analysis and an accompanying training plan which tailors training to individual job role requirements, and provide specialist training to staff responsible for Records Management, Information Security, Data Protection, disclosures, data sharing and Data Protection Impact Assessments (DPIAs).

Identify and document all data processors acting on behalf of BCHP, ensuring that appropriate written contracts are in place. Contracts should contain all the terms and clauses required under DPA18. Due diligence checks should be conducted before entering into and during the contract to gain assurance that the requirements of DPA18 are met.

A programme of risk-based Information Governance (IG) audits and compliance checks should be initiated as part of an internal audit plan, which should include routine monitoring of records management functions and storage facilities and any processor acting on behalf of BCHP. Risk identification and management can be augmented by a regular programme of independent external audits.

Conduct DPIAs for processing activities that commenced before 25 May 2018 (prior to the introduction of the GDPR and DPA18) and ensure that all outcomes from DPIAs are integrated into relevant work plans, project action plans and risk registers to effectively mitigate or manage any risks identified.

Establish a process to notify affected individuals where a breach is likely to result in a high risk to their rights and freedoms.

To ensure that manual and electronic records containing personal data are appropriately accessed, classified, stored and disposed of, document formal records management policies and procedures including sharing personal data with third parties across all areas of BCHP.

Physical records are not adequately tracked. Without robust tracking procedures in place the risk that the documents could be unlawfully accessed, compromised, or lost is greatly increased. Also, should there be a breach of special category/sensitive data the harm to the data subject is substantially higher.

Conducting regular weeding and reviews of manual and electronic records across all areas will ensure they remain appropriate to be retained, or disposed of accordingly.

Producing guidance would assist staff in handling requests for rectification and erasure of personal data in certain circumstances. It will also help BCHP inform third parties to which that data was shared.

Best Practice

BCHP have established a robust process for ensuring that policies and procedures across all three forces are reviewed in accordance with their scheduled review dates. This is particularly significant given the size of the three forces and their collaborated functions. This process is overseen by the Head of Information Rights and Assurance. Adherence to the review date is monitored quarterly by the Information Management Board via a Key Performance Indicator (KPI) which records the total number of policies and the number and percentage of those which are up to date. BCHP have also established an escalation process via the Deputy Chief Constable where non-compliance occurs. The ICO has noted a marked improvement in compliance from February 2020 to August 2020 with some areas of the Force now over 90% compliant. This process has allowed BCHP to gain assurance that policies and procedures are up to date and fit for purpose as documents that contain outdated information could cause personal data breaches.

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 BCHP.

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 BCHP. The scope areas and controls covered by the audit have been tailored to BCHP and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.