Devon and Cornwall Police and Dorset Police

Data protection audit report

October 2020

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.

Devon and Cornwall Police and Dorset Police (DCP & DP) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 23 June 2020 with representatives of DCP & DP to discuss the scope of the audit.

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

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.

Requests for Access to Personal Data	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.
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 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 DCP & DP 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 24 August to 11 September 2020. The ICO would like to thank DCP & DP for its flexibility and commitment to the audit during difficult and challenging circumstances.

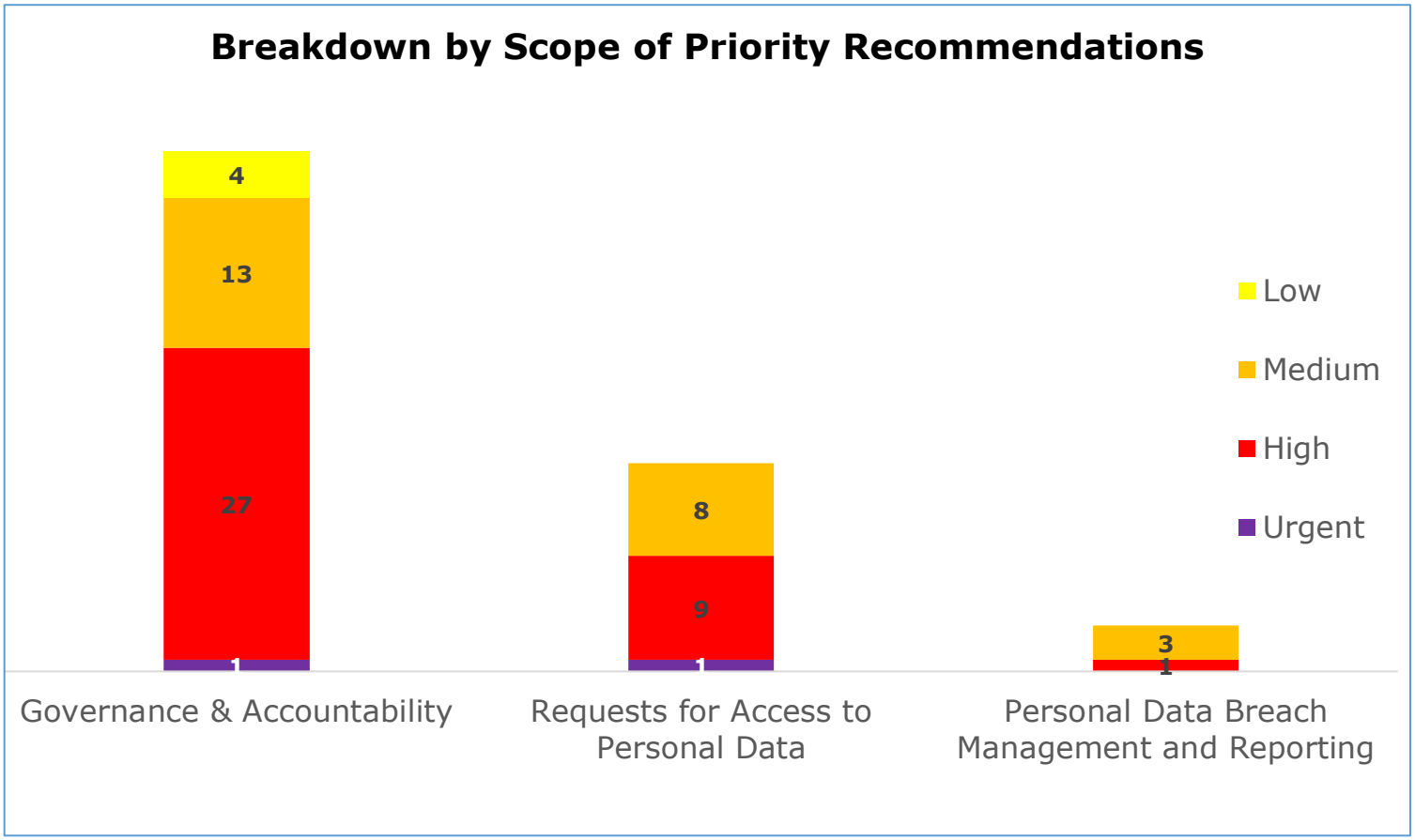
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist DCP & DP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. DCP & DPs 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.
Requests for Access to Personal Data	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.
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.

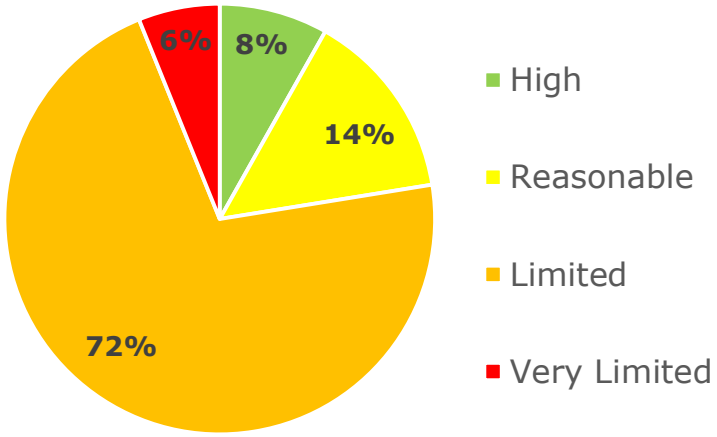
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

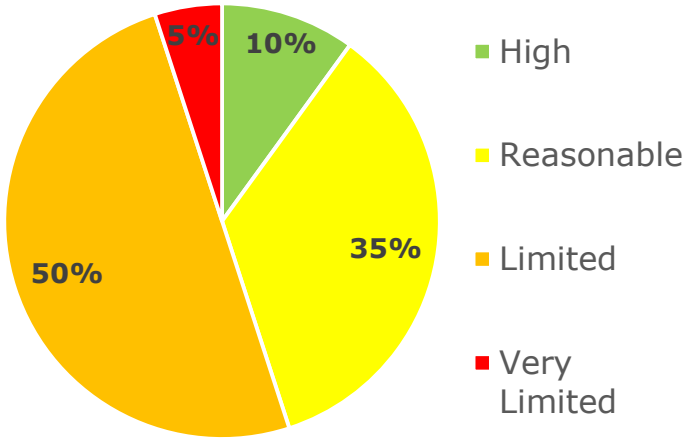


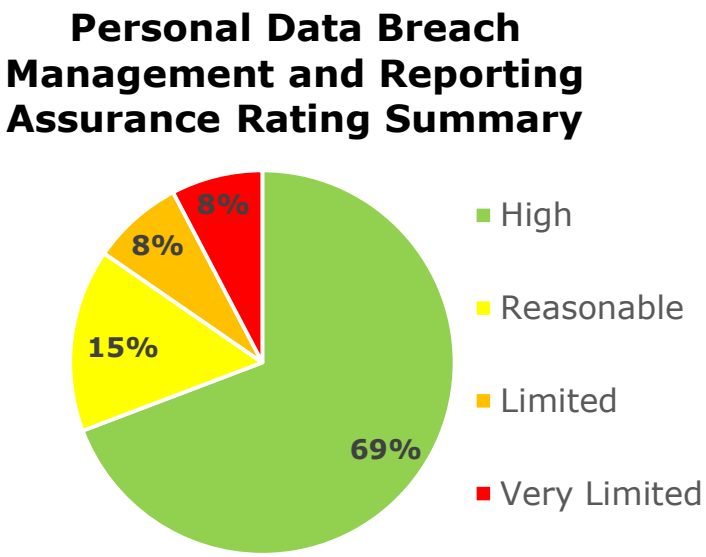
Graphs and Charts

Governance & Accountability Assurance rating summary



Requests for Access Assurance Rating Summary




Personal Data Breach Management and Reporting Assurance Rating Summary
8%
8%
15%
69%
High
Reasonable
Limited
Very Limited

Areas for Improvement

The completion of an information audit/data mapping exercise would ensure that all data processors are clearly identified and create both a Record of Processing Activities and Information Asset Registers , to incorporate all business areas across the whole organisation. The exercise is key to comply with Article 30 GDPR and Section 61 DPA18 legislation and establishing the lawful basis for processing personal data/special categories of data. In addition, the IARs should be reviewed on a regular basis to ensure that the lawful basis is still appropriate.

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 Information Asset Registers above will contribute to this) and what rights they have in relation to that processing, including the right to withdraw consent. The privacy information should be available in other languages and formats to meet the needs of all sections of society.

DCP & DP should continue to monitor resource levels within the Data Protection Team to ensure that the Data Protection Officers can carry out their key functions, including monitoring internal compliance, informing and advising on data protection obligations, in accordance with Articles 37, 38 and 39 of the GDPR.

Continue to develop working practices and procedures to support Information Governance/Data Protection policies to provide practical guidance and increase awareness for staff of their data protection responsibilities in all business areas across DCP & DP. Develop and implement a formal sign off process to gain assurance that staff have read new and amended Data Protection policies and understood current IG related guidance and procedures.

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. The Data Protection Officers need to have complete oversight of all the training areas and all training content delivered across DCP & DP, which include elements of Information Governance/Data Protection to ensure the programme is delivered consistently.

Routinely monitor the compliance, with Information Governance policies, of any processor acting on behalf of DCP & DP. This should cover the processor's procedures, Data Protection training and data security arrangements to ensure they are effective and comply with contractual agreements. In addition, to identify and manage information risks, a programme of risk based Information Governance audits should be initiated as part of an external audit plan.

Key Performance Indicators should have set targets in all key areas in Information Governance, including Subject Access Requests, Training, Incident Management and Records Management. Once targets are set, performance against those targets should continue to be monitored and discussed at the Joint Information Board to drive improvements. The use of more meaningful data as part of a new dashboard will help DCP & DP achieve this. In addition, DCP & DP should continue to monitor the number of staff in place, to ensure the level of resource is sufficient to be able to handle incoming requests for access whilst also working through the existing backlog.

Review all consent mechanisms to ensure they meet GDPR requirements. There should be clear, publicised information on how individuals can withdraw their consent and when such requests are received they are acted upon promptly. In addition, review consent on a regular basis to ensure that it remains the correct lawful basis for processing personal data.

When responding to a request for personal data the required supplementary information must be provided alongside copies of the personal data requested. This must be sufficiently granular and specific to the data subject that made the request to ensure compliance with Article 15 of the GDPR and Section 45 of the DPA18.

The implementation of a formal approval process would help to ensure that proper consideration is given and documented to the removal of personal and third party data that is exempt from disclosure. Furthermore, the creation of a quality assurance process would ensure a consistent approach to the application of exemptions and the removal of personal and third party data, is taken across the Data Protection Team.

Producing guidance would assist staff in recognising a valid request for access to personal data. This should explain that requests can be made verbally and in writing, and that an individual can request supplementary information as well as copies of their personal data.

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 DCP & DP.

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