Derbyshire Constabulary



March 2019

Data protection audit report

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.

The purpose of the audit is to provide the Information Commissioner and Derbyshire Constabulary (DC) with an independent assurance of the extent to which DC, 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. |
| Security of Personal Data | There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data. |
| Data Sharing | The design and operation of controls to ensure the sharing of personal data complies with the principles of all 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, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist DC 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. DC’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 | 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. |
| Security of Personal Data  | High | There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation. |
| Data Sharing | 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. |

Priority Recommendations

Graphs and Charts

Areas for Improvement

DC have a newly formed Strategic Information Management Board (SIMB) which is yet to define how key enabling boards effectively communicate information risks to the SIMB.

The corporate risk register contains generic risks around data protection reform and needs to be fully populated with details of the information risks discussed and agreed via the SIMB. This will enable the information risks identified to be managed appropriately.

DC are in the process of updating their Information Asset Register (IAR). The information flow mapping currently being undertaken needs to be finalised to ensure that they have an accurate record of all data processing activities as required by GDPR/DPA18.

The completion records for data protection training are inaccurate and there is no assurance for DC that all staff have understood and are aware of their data protection responsibilities.

Specialist training should be mandatory for Information Asset Owners (IAOs) who have additional data protection responsibilities. This will ensure that IAOs are aware of the requirements of their roles and that their information assets are handled and managed appropriately.

DC carry out risk assessments on new systems or when there is a change to the system. Risk assessments for all hardware and software assets are not regularly conducted. A log of the devices that have not connected to the network are kept; however physical checks to ensure the accuracy of the hardware asset inventory are not conducted.

It was reported that line managers are responsible for ensuring that staff changing roles only have access to systems/drives/ folders relevant to their new role. Regular reviews, or checks of user access rights are not undertaken to ensure that the access rights are appropriately updated. There is therefore a risk that employees could retain access to information that they no longer need.

Line managers are also responsible for completing regular clear desk sweeps or checks and regular compliance reviews of systems and processes within their area of responsibility. However there are no assurances that this takes place across the Force.

DC should review and update the Information Sharing and DP Policies to ensure that they comply with current legislation and are fit for purpose. The policies should contain more high level guidance on how to deal with one-off personal data disclosures.

Information sharing agreements reflect the fact that DC will retain shared data in accordance with the national Guidance on the Management of Police Information and the retention periods to be applied by partners refers to their individual records management policies. Steps should be taken to ensure that retention periods are actively discussed and agreed with all partners to agreements. This will help to ensure that personal data is being retained appropriately and not excessively.

DC should ensure that information sharing agreements contain prescriptive requirements for the reporting of both suspected and actual security incidents. Effective reporting mechanisms should be detailed to ensure that partners are aware of how to report incidents promptly.

Good Practice

The Head of the Information Management Department who is also the Force Data Protection Officer (DPO) attends the regular "Heads of Business Meetings", chaired by the Senior Information Risk Officer (SIRO). This enables the DPO greater oversight of force activities involving personal data and ensures a higher profile for both data protection and the Information Management Department.

The 'Connect' intranet has a means to flag and enforce a policy/guidance to be read by way of a mandatory read receipt. If the item remains unread it is sent to the users email inbox. This is an excellent way to enforce users read key documents.

The programme of data quality checks completed by the Data Quality and RRD Team is comprehensive and enables DC to identify and rectify data quality issues efficiently and proactively.

**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 Derbyshire Constabulary.

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