SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee Public Session**
Date	**22 January 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**Data Protection Overview**
Item Number	**9.2**
Presented By	**DCO David Page**
Recommendation to Members	**For Noting**
Appendix Attached	**No**

PURPOSE

The purpose of this paper is to provide Members with an overview of Data Protection within Police Scotland.

The paper is presented in line with the Scottish Police Authority Governance Framework.

The paper is submitted For Noting.

1. BACKGROUND

1.1 This paper sets out the current arrangements, roles and responsibilities within Police Scotland, to manage compliance with the Data Protection Act 1998 and associated legislation.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Roles, Responsibilities and Governance

2.1.1 All police officers and staff are bound by the terms of the Data Protection Act 1998 and Computer Misuse Act 1990. In broad terms the following combined roles are responsible for ensuring compliance with relevant legislation and ensuring the security and integrity of personal data.

Chief Constable – Data Controller

The Chief Constable is the data controller for all personal data held by Police Scotland and is ultimately responsible for deciding the purpose for which, and the manner in which, personal data will be processed.

Deputy Chief Constable (Designate) – Accountable Officer through the Public Records (Scotland) Act 2011

The DCC (Designate) is identified to the Keeper of the Records of Scotland as the individual within Police Scotland as being responsible for ensuring compliance with the records management plan. This includes the maintenance of security, archiving, destruction or other disposal of records.

Senior Information Risk Owner (SIRO)

The SIRO is the overall decision maker in respect of information risk.

These responsibilities are managed, discharged and co-ordinated by Information Management (Assurance and Disclosure sections).

Governance

Internal governance and reporting to the Scottish Police Authority is via the Audit and Risk Board, which is chaired by the Deputy Chief Officer. Police Scotland has recently formed an Information Governance Board. This forum will be responsible for providing strengthened oversight and decision making for information governance and data protection compliance.

2.2 Compliance and Assurance

2.2.1 Compliance and assurance is provided through both external and internal audit. A programme of internal audits are detailed on the Information Management business plan.

2.2.2 The results of audit, and management of recommendations, are monitored through the Information Governance Board and reported to the SPA Audit and Risk Committee.

2.3 Information Commissioner's Office (ICO) - Audit activity

2.3.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (DPA).

2.3.2 In August 2017 the ICO completed a consensual audit of Police Scotland's processing of personal data. Recommendations arising from the audit are being progressed.

2.4 Information Commissioner's Office – Ongoing Engagement

2.4.1 Information Management adopts a proactive early engagement policy with the ICO in relation to any known or emerging data protection concerns.

2.4.2 In accordance with other statutory requirements, arrangements are in place to report to the Audit and Risk Committee any relevant 'reported data loss' incidents which have been notified to the ICO. No enforcement activity has been taken by the ICO in respect of any incidents reported.

2.5 Data Weeding, Retention and Information Sharing

2.5.1 Police Scotland, due to its nature as a law enforcement organisation, processes large volumes of personal data. Some of this information may require to be shared with partner agencies, under a lawful framework and in a proportionate manner.

2.5.2 Risks associated with ongoing data retention and information sharing are being mitigated wherever possible. This is achieved through a range of measures including;

- Records Retention SOP and policies in place with ongoing engagement with Information Asset Owners;
- ongoing and early proactive engagement by Information Management with the ICO;
- creation of a national Information Asset Register;
- creation of a national Information Sharing Protocol Register;

3. FINANCIAL IMPLICATIONS

3.1 There are financial implications in this report.

3.2 Where data breaches occur due to lack of management controls, currently the ICO may issue a monetary penalty notice of up to £500,000. In May 2018, following data protection reform, more severe financial penalties ranging from 10 million euros, or 2% of turnover, up to 20 million euros or 4% of annual turnover may be imposed.

4. PERSONNEL IMPLICATIONS

4.1 There are personnel implications associated with this paper. Data Protection legislation relates to all officers and staff.

5. LEGAL IMPLICATIONS

5.1 There are legal implications in this paper where failure to comply with data protection legislation may lead to enforcement action by the ICO. Legal action is more likely if preparation, implementation and ongoing compliance is not undertaken.

6. REPUTATIONAL IMPLICATIONS

6.1 There are reputational implications associated with this paper. Enforcement action by the ICO would lead to obvious reputational damage to Police Scotland.

6.2 Following Data Protection Reform in May 2018, Police Scotland will be required to proactively publish and provide detailed information about our data processing.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There are no community implications associated with this paper.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications associated with this paper.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environment implications associated with this paper.

RECOMMENDATIONS
Members are requested to:

Note the information contained within this report.