SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee Public Session**
Date	**22 January 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**General Data Protection Regulation (GDPR) Police Scotland Preparedness**
Item Number	**9.3**
Presented By	**DCO David Page**
Recommendation to Members	**For Noting.**
Appendix Attached	**No**

PURPOSE

The purpose of this paper is to provide an update on the progress by Police Scotland to address the forthcoming measures on Data Protection Reform which are a result of the Data Protection Bill. This will see the implementation of the General Data Protection Regulation 2016 (GDPR) and Law Enforcement Directive.

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

The paper is submitted For Noting.

1. BACKGROUND

1.1 The GDPR is a regulation by which the European Parliament and its associated bodies intend to strengthen and unify data protection for individuals within the European Union (EU). Once enacted the new Data Protection Bill, which incorporates GDPR, will replace the current Data Protection Act 1998.

1.2 As part of the Bill, the UK will implement the Law Enforcement Directive (LED).

1.3 Many of the GDPR's main concepts and principles are similar to those in the current Data Protection Act, however, there are new elements and significant enhancements which require consideration. The target date for completion of this work is 1 May 2018.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Summary

2.1.1 The GDPR will not apply to personal information processed for national security or law enforcement purposes, however it will apply to some personal information processed during operational policing activities and support activities.

Reform will require a culture of data privacy to pervade the organisation and create new obligations including;

- Proactively informing individuals how their data is being used;
- Obtaining clear and unequivocal consent before an individual's data is processed in certain circumstances;
- Deleting data following a request (where there is no compelling reason to keep it).

2.2 Preparation and Progress

2.2.1 A project team has been appointed to introduce the requirements of GDPR. The team have a detailed project plan which covers the significant actions required to be carried out by 1 May 2018. The areas are as follows;

2.2.2 **Awareness** –This step involves raising awareness across the organisation. A series of workshops, intranet messages and SPOC awareness sessions are being carried out.

2.2.3 **Information Held** – This step involves documenting the personal data we hold, where it came from and who we share it with. This work is being collated through an information audit. The information audit is a key milestone for producing an Information Asset Register. The Information Asset Register will provide a record of all information assets held, along with owners and risks including weeding dates.

2.2.4 **Communicating Privacy Information** –This step involves reviewing and making any relevant changes to privacy notices.

2.2.5 **Individuals' Rights** – This step involves checking procedures to ensure they cover all the rights of individuals, including how we would delete data or provide data electronically in a commonly used format. Policy Support are currently reviewing all Standard Operating Procedures (SOPs).

2.2.6 **Subject Access Requests** – This step involves reviewing the SAR process. This is ongoing and additional training is in progress.

2.2.7 **Legal Basis for Processing** – This step involves defining the reason we are processing data. This has been incorporated into the Information Asset Audit.

2.2.8 **Consent** – This step involves reviewing how we seek, record and manage consent and updating practices where required. This has been incorporated into the Information Asset Audit.

2.2.9 **Consent of Children** – This step involves consideration of how consent is obtained for processing data relating to children and whether parental consent is required. This has been incorporated into the Information Asset Audit.

2.2.10 **Data Breaches** – This step involves ensuring the right procedures are in place to detect, report and investigate data breaches. The new legislation will require us to report a lower threshold of breach with all breaches being reported within 72 hours.

2.2.11 **Data Protection by Design and Privacy Impact Assessments (PIAs)** – This step involves the use of PIAs. A draft PIA template has been produced.

2.2.12 **Data Protection Officer** – This step involves designating a Data Protection Officer. As a public authority this is mandatory.

2.3.13 **International Transfers** –This step involves determining our lead data protection supervisory authority. Our lead authority will be ICO.

2.4 **Resourcing**

2.4.1 Due to market competition, challenges were encountered finding suitable candidates to implement the GDPR project. This led to a slight delay however additional data protection reform posts are now in place.

2.4.2 The Force Executive have been briefed in relation to the project and have agreed that any future resource requests required for the project will be approved.

2.5 **Compliance and Assurance**

2.5.1 Police Scotland will not be fully compliant on 25 May 2018. This is predominately due to the retention of personal data on legacy systems. Work is ongoing, with ICO support, to enhance processes to facilitate full compliance. Assurance around this activity will be discharged as detailed at 2.5.2.

2.5.2 The Data Protection Reform Project will meet the compliance standard on internal processes including amendments to policy and practice. SOPs and supporting documentation will be updated by 1 May. Delivery of these outputs will be monitored through the Project Board chaired by the Senior Responsible Officer.

2.5.2 External assurance to the project will be provided by a variety of means. This includes internal audits carried out by Scott Moncrieff, regular updates to the SPA Audit and Risk Committee, and through ICO inspections. A Scott Moncrieff assessment of preparedness will be available in Draft by late December. Further to this, ICO is scheduled to carry out follow up activity from their previous audits in early 2018.

3. FINANCIAL IMPLICATIONS

3.1 There <u>are</u> financial implications in this report. Data protection reform will result in direct and indirect financial implications.

3.2 Fees for subject access requests will no longer be charged. This will result in lost annual revenue of circa £50,000. Where data breaches occur due to lack of management controls, the regulator may impose severe financial penalties ranging from 10 million euros, or 2% of turnover, up to 20 million euros or 4% of annual turnover.

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 and loss of public trust should the organisation be unable to demonstrate compliance with legislation.

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 environmental implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

Note the contents of this report and the preparations made towards data protection reform.