Error! Unknown document property name.

SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee**
Date	**18 April 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**General Data Protection Regulation (GDPR) Scottish Police Authority Preparedness**
Item Number	**11.1**
Presented By	**Catherine Topley**
Recommendation to Members	**For Noting.**
Appendix Attached	**Yes – Internal Audit Action Plan**

PURPOSE

The purpose of this paper is to provide an update on the progress by SPA to address the forthcoming measures on Data Protection Reform which are a result of the Data Protection Bill and the General Data Protection Regulation 2016 (GDPR).

The paper is presented in line with the Scottish Police Authority/Police Scotland Scheme of Administration.

The paper is submitted For Noting.

1. BACKGROUND

1.1 The General Data Protection Regulation (GDPR) is European Legislation which, in May 2018, will replace much of the existing Data Protection legislation in the UK. The purpose of the GDPR is to strengthen data protection for all individuals within the European Union. The processing of personal information for national security and law enforcement purposes is covered by a separate Directive known as the Law Enforcement Directive (LED).

1.2 The GDPR does not require national governments to pass enabling Legislation, but the LED does. The UK has introduced the Data Protection Bill, which is will transpose the LED into UK law, address gaps which were left by the GDPR and update existing data protection laws. The Bill was introduced to the House of Lords on 13 September 2017. At the time of submission of this report, the Bill is at the Report Stage in the House of Commons.

2. Information Management as the lead department, will provide the necessary guidance to the changes in process which are required to meet legislative compliance.

3. PROGRESS REPORT

3.1 In December 2017, SPA received an internal audit report from Scott-Moncrieff 'GDPR Readiness, December 2017' which made 6 recommendations. Members of the Audit Committee are provided with fortnightly updates on both the Project status and the progress being made with each of the audit recommendations.

3.2 Following agreement and support from Police Scotland, a procurement tender was issued and a contract successfully awarded to Anderson Strathern, who commenced their work with SPA on the 14th February 2018. A data protection lawyer is co- located with the IM team in Pacific Quay for one day a week.

3.3 Work continues across Police Scotland and SPA ensuring a joined up approach, wherever possible, is being managed for the delivery of GDPR. To further support this a weekly call has been set up between key stakeholders in SPA. This approach includes a standing invite for SPA and Police Scotland to each of the Project Boards and the sharing of reports. Furthermore, a practitioners group will also meet on a regular basis to ensure that information is cascaded down to practitioners.

3.4 Additional resources to support the work required have been identified and are currently progressing through vetting.

3.5 The Project Team have adopted the Information Commissioner's '12 Step Plan' towards achieving compliance with the new legislation. This approach also addresses a number of the areas identified in the ICO Audit in December 2017.

3.6 12 Step Plan Progress

3.6.1 **Awareness** – This step involves raising awareness across the organisation that the law is changing. A process of communication has commenced to make staff aware of the forthcoming changes. Corporate Communications will continue to attend the SPA Project Board to discuss the rollout of communications to SPA/Forensic Staff and other stakeholders as required. SPA IM and Police Scotland IM teams met with Glasgow CC who agreed to share template documents, notice board posters and training tools. Training tools and posters are currently under review.

3.6.2 **Information Held** – Completion of the Information Asset Audit involves documenting the personal data SPA holds, where it came from and who it is shared with. A first draft of the Information Asset Register has been produced and is currently under review and an update will be provided to the SMG mid May 2018.

3.6.3 **Communicating Privacy Information** – This step involves reviewing and making any relevant changes to privacy notices. At present two types of privacy notice will be required, one for law enforcement processing which will be relevant for Forensic Services purposes and another for processing which falls under GDPR which will be relevant for SPA Corporate Services. These will be published on the external website and be made available in other formats as required. Further consultation will be undertaken with business partners to understand responsibilities and ensure notices are in place by May 2018.

3.6.4 **Individuals Rights** – This step involves checking policy and 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. Relevant policies are currently under review

and where necessary, new policies will be drafted, reviewed by the SMG and agreed/published by mid-May 2018.

3.6.5 **Subject Access Requests** – This step involves incorporating the removal of the subject access fee arrangements and the change to processing timescales. The current policy is under review and will be finalised by mid-May 2018.

3.6.6 **Legal Basis for Processing** – This step involves defining the reason we are processing data and is being incorporated into the Information Asset Audit and will be reflected in the appropriate privacy notices. Discussion will be undertaken with business partners and the appropriate documentation will be produced by the end of May 2018.

3.6.7 **Consent** – This step involves reviewing how we seek, record and manage consent and updating practices where required. This is also incorporated within the Information Asset Audit. The information asset audit will act as a discovery exercise for this element of GDPR. Once the audit is complete, any requirements for consent will be identified and actioned accordingly.

3.6.8 **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 is also incorporated within the Information Asset Audit. The information asset audit will act as a discovery exercise for this element of GDPR. Once the audit is complete, any requirements for consent will be identified and actioned accordingly.

3.6.9 **Data Breaches** – This step involves ensuring the right procedures are in place to detect, report and investigate data breaches. A new policy is currently being drafted to ensure compliance with the requirements of the legislation. The draft will be available for consultation in May 2018.

3.6.10 **Data Protection by Design and Privacy Impact Assessments (DPIAs)** – This step makes it an express legal requirement to adopt 'privacy by design' and to carry out Data Privacy Impact Assessments. These were previously desirable but are now mandatory. An assessment of the processing is underway via the information asset audit. Further discussions will also be required with business partners.

3.6.11 **Data Protection Officer** – As a public authority Police Scotland must have a Data Protection Officer (DPO). A review of the structure is currently underway in SPA and this will be considered as part of the review.

3.6.12 **International Transfers** – It will be necessary to establish through the Information Audit whether the SPA processes personal data which affects individuals in EU member states, or whether personal data is ever transferred cross-border. If so, it will be necessary to ensure that appropriate controls are place in order to meet the requirements of the GDPR.

4. Compliance and Assurance

4.1 The Data Protection Reform Project aims to ensure the necessary revisions to internal processes, SOPs and supporting documentation are in place by May 2018. Delivery of these outputs is being monitored through the Project Board. A provisional date of 17 May has been agreed for the outcomes of the 12 step plan
To be presented to the SPA |SMG.

4.2 Relevant risks are recorded, monitored and reported via the SPA risk register.

5. FINANCIAL IMPLICATIONS

There are financial implications in this report. Data protection reform will result in direct and indirect financial implications.

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. It is not anticipated that the loss of fees in relation to subject access requests will have a significant financial impact on the SPA due to small number of requests received.

6. PERSONNEL IMPLICATIONS

There are no personnel implications associated with this paper

7. LEGAL IMPLICATIONS

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.

8. REPUTATIONAL IMPLICATIONS

There are reputational implications associated with this paper. Enforcement action by the ICO would lead to obvious reputational damage to SPA and loss of public trust should the organisation be unable to demonstrate compliance with legislation.

9. SOCIAL IMPLICATIONS

There are no social implications associated with this paper.

10. COMMUNITY IMPACT

There are no community implications associated with this paper.

11. EQUALITIES IMPLICATIONS

There are no equality implications associated with this paper.

12. ENVIRONMENT IMPLICATIONS

There are no equality implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

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

Error! Unknown document property name.

Appendix A - INTERNAL AUDIT ACTION PLAN UPDATE

The following Control Objectives are taken from the Internal Audit report of January 2018.

No	Control Objective	Recommendation	IA Status Assessment (Jan)	Management Action	Due Date	Owner	SPA Status Assessment (Mar)
Formal Gap Analysis and Action Plan							
1	A gap analysis has been conducted and documented to identify where current personal data management policies, practices and procedures are not consistent with the GDPR	We recommend that a formal gap analysis is produced for SPA. This should identify all actions necessary to achieve compliance with the GDPR and LED. In developing this action plan, management should review the current tasks lists to confirm that all relevant recommendations from the ICO and internal assessment are being addressed.	Amber	The first draft of the information asset registers have now been received by the IM team from all departments within SPA Corporate Services. Review of these by the IM team and the DP Lawyer is underway. The first draft of the information asset register has also now been received from	March 2018	Catherine Topley	Amber
2	Action plans have been developed to address all identified gaps.		Amber				Amber

		Once this is completed, SPA should develop a detailed project plan which lists all actions, the timescales for their completion, action owners and people requirements to deliver them.		Forensic Services and is under review. All relevant SPA DP Policies are now under review. Suggested amendments to the ICO Audit Executive Summary are to be submitted to the ICO on Monday 26 March.			
Timescales and Responsibilities							
3	Action plans contain timescales for completion and responsibilities.	We recommend that once an action plan has been developed, management make a formal assessment of the people resources required to deliver it. If there is any	Red	The SPA Project Board met on 12th March to review the Project Initiation Document and the consolidated Action Plan.	March 2018	Catherine Topley	Amber

4	Appropriate resources are assigned to support achievement of action plans.	additional people requirement, this should be escalated as soon as possible to senior management for review and approval. In light of the current high market demand for data protection specialists, SPA management should develop formal contingency arrangements in the event that the additional staff cannot be recruited in line with expected timescales. This should include consideration of partnering with a third party who would be able to provide staffing for a fixed period.	Red	Timescales within the Action Plan are to be completed by the IM team and the DP Lawyer. The IM team has been restored to 100% capacity. Vetting is ongoing regarding the appointment of the SPA GDPR officer.			Amber

Progress Monitoring							
5	There is adequate governance to monitor progress in delivering action plans.	We recommend that GDPR and LED compliance is managed as a project within SPA. This should include the creation of a formal project framework which includes a Project Sponsor (member of the Senior Management Group) being assigned to the project, the creation of a project board as well as the creation and maintenance of risk and issues logs. The Project Board should meet on a regular basis. Given the timescales to implementation this should be at least	Red	The SPA Project Board sat for the first time on Monday 12th March. The Project Initiation Document and Action Plan were reviewed. A Project Board Action Log was produced after the meeting and will continue to be monitored. A project approach is now being established within SPA and the relevant documentation put in place. The new interim Director,	March 2018	Catherine Topley	Amber

		monthly with highlight reports being submitted to the SPA Senior Management Group so that they have a clear understanding of progress and how risks and issue are being managed.		Catherine Topley, has been identified as the SIRO. The project progress, risk and issues will be reported internally to SPA SMG on a monthly basis.			
Training							
6	Plans are in place to ensure all relevant staff are made aware of the impact of GDPR and their role in supporting compliance.	We recommend that training and awareness requirements are included within the GDPR and LED action plan. Training should be provided through face-to-face sessions or through the use of e-learning tools. In addition, there	Amber	A communications plan will be built into the overall consolidated SPA action plan. Corporate Communications will continue to attend the SPA Project Board to discuss the rollout of	March 2018	Catherine Topley	Amber

		should be regular awareness raising campaigns conducted to highlight the importance of the requirements of GDPR and LED. This should include, for example, email communications, notice board posters, features on the intranet etc.		communications to SPA/Forensic Staff and other stakeholders as required. SPA IM and PS IM teams met with Glasgow CC who agreed to share template policy documents, notice board posters and training tools. Training tools and posters are currently under review by the SPA IM team and the DP Lawyer.			