SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee**
Date	**18 April 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**General Data Protection Regulation (GDPR) Police Scotland Preparedness**
Item Number	**11.2**
Presented By	**ACC Alan Speirs**
Recommendation to Members	**For Noting.**
Appendix Attached	**Yes – Progress report on Scott Moncrieff 'GDPR Readiness, December 2017' recommendations.**

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 which will implement the General Data Protection Regulation 2016 (GDPR) and Law Enforcement Directive.

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 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) and the latest information from the Home Office is both LED and GDPR will commence on the same date, 25 May 2018. At the time of submission of this report, the Bill awaits its third reading in the UK parliament.

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

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 The Police Scotland Data Protection Reform Project was established in November 2017, following recruitment and appointment of the Project Team, with the final member of staff taking up post in February 2018. Following a change in Executive portfolios, the Project SRO is Assistant Chief Constable Alan Speirs (Professionalism and Assurance) and Chief Superintendent John Paterson is the Deputy SRO.

2.2 The multi-disciplinary Project Board comprises senior officers and members of police staff from both operational and corporate functions to ensure appropriate governance and coordination of the required changes in internal processes and policy.

2.3 In December 2017, Police Scotland 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. The most recent update in respect of the progress made against the Scott-Moncrieff recommendations is provided in Appendix ‘A’ to this report.

2.4 The Project Team have adopted the Information Commissioner's '12 Step Plan' towards achieving compliance with the new legislation, whilst at the same time engaging with the wider policing community through the National Police Chief's Council Data Protection Portfolio to ensure Police Scotland adopts consistent practices and approaches towards data protection reform. Due to the different legislative frameworks in relation to law enforcement processing, Police Scotland may, in certain circumstances, require to assess the impact of, and develop bespoke practices, which meet the requirements of both the Bill and Scottish law, particularly around sharing of wellbeing concerns with partner agencies.

2.5 **Preparation and Progress**

Using the ICO's 12 Step Plan as the project baseline, the following progress has been made to date.

2.5.1 **Awareness** – This step involves raising awareness across the organisation that the law is changing. The Project Team have completed seven communication and engagement events across the country with an attendance of circa **600** officers and staff across from all divisions and departments. This has been supported by a programme of local support meetings, and a robust communications strategy, which has seen revisions made to the main Information Management Intranet site and the creation of a dedicated Data Protection Reform Intranet page which contains news releases and FAQs. From the end of November 2017 to date, the Intranet site has been visited on over **13,000** occasions; news articles read almost **5,000** times and line manager / staff briefing packs downloaded a little under **6,000** times.

2.5.2 In addition the Project Team is currently finalising three bespoke on-line packages (General Awareness, Behaviours and Consent) which will be delivered across Police Scotland via the Moodle on-line training platform.

2.5.3 **Information Held** – Completion of the Information Asset Audit involves documenting the personal data Police Scotland holds, where it came from and who it is shared with. The task of populating the Information Asset Register is nearing completion and will be followed by a Quality Assurance Process which will track and record any remedial actions required by Information Asset Owners.

2.5.4 **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 and another for all other processing which falls under GDPR. Following review of the Information Asset Register, the Project Team are currently engaging with 10 business areas to allow for development of appropriate privacy notices. These will initially be published on the external website and be made available in other formats as required.

2.5.5 **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. Policy Support is currently undertaking a review of all Standard Operating Procedures (SOPs) to identify those that will need updated either substantially or in part.

2.5.6 **Subject Access Requests** – This step involves incorporating the removal of the subject access fee arrangements and the change to processing timescales. A review of the SAR process has been completed with the revised Standard Operating Procedure sent for mandatory consultation. The changes to the SAR process will be subject of a future communications bulletin to all officers and staff.

2.5.7 **Legal Basis for Processing** – This step involves defining the reason we are processing data and is being incorporated into the Information Asset Audit.

2.5.8 **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. This is likely to have a significant impact on operational officers i.e. how consent for processing personal information (out with law enforcement) is obtained and recorded. The Project Team has supported the Risk & Concern Project in developing appropriate guidance for front line officers and Risk & Concern Hubs. This guidance will be incorporated in the Moodle training package 'Consent' which will be rolled out prior to 25 May.

2.5.9 **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 is also incorporated within the Information Asset Audit. Under GDPR, children can consent to data processing at 16 years. The UK has decided to set the age of 13 as the minimum age by which a child can consent to data processing. Again this guidance will be incorporated in the Moodle training package 'Consent' which will be rolled out prior to 25 May.

2.5.10 **Data Breaches** – This step involves ensuring the right procedures are in place to detect, report and investigate data breaches. Whilst Police Scotland currently reports certain breaches to ICO, the new legislation will require the organisation to report a lower threshold of breach, with all breaches being reported within 72 hours. The 'Information Security Incident Reporting' Standard Operating Procedure is being updated and internal processes are being revised accordingly.

2.5.11 **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. The Project Team has developed DPIA templates and guidance which are currently subject of mandatory consultation.

2.5.12 **Data Protection Officer** – As a public authority Police Scotland must have a Data Protection Officer (DPO). In this regard, the organisation has created a new DPO post, which is the subject of a ongoing recruitment process.

2.5.13 **International Transfers** – The Project Team met with the International Assistance Unit and International Development & Innovation Unit to gain an understanding of their work and to provide any advice on the implications of data protection reform for those respective areas of business.

2.6 Compliance and Assurance

2.6.1 The Data Protection Reform Project aims to meet compliance by ensuring the necessary revisions to internal processes, SOPs and supporting documentation are in place by 1 May 2018. Delivery of

these outputs is being monitored through the Project Board chaired by the Deputy SRO.

2.6.2 External assurance to the Project has been provided by a variety of means. This includes internal audits carried out by Scott-Moncrieff, regular updates to the Audit Committee, and through ICO inspections. The ICO has recently confirmed it will undertake a follow up assurance review of progress made by Police Scotland in respect of its previous audits.

2.6.3 Excessive retention of personal data, including failure to weed police systems, either due to a lack of functionality on existing systems or application of the Records Retention Policy, remain the same under the new legislation and is a continuing risk to the Force.

2.6.4 To mitigate this risk, Police Scotland will form a Data Retention & Review Design Authority which will provide a multi-disciplinary forum to prioritise and manage the work required by Strategic Information Asset Owners and ICT to meet legislative compliance. This forum will provide for a coordinated approach between the Board, the Digitally Enabled Policing and Data Governance and Insight Programmes.

3. FINANCIAL IMPLICATIONS

3.1 There are 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. Public protection and sharing of information is an area considered particularly high risk as it may wholly or in part fall under GDPR, thereby giving data subjects substantially increased rights. This will require operational officers to be fully aware of these rights and be able to articulate these as required.

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 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.

Scott-Moncrieff GDPR Audit - Progress Updates Utilising BRAG Status Key							Appendix 'A'
Ref	**Subject**	**Recommendation**	**Rating**	**Management Action**	**Due Date**	**Allocated To**	**Update**
1	Gap Analysis - Info Asset Register	We recommend that management monitor outputs from information audits so that any additional project tasks and activities are identified and assessed as soon as possible. If any changes are necessary the impact of these should be formally assessed to establish whether they affect delivery timescales and staffing needs.		The Project Team will establish a methodology to assess the outcome of each audit to ensure any additional project tasks and activities which are required are addressed. These will be captured in 'issue logs' for progression. The methodology will be established by due date.	~~February 2018~~ March 2018	Project Lead	28/03 – Quality Assurance work is underway in respect of the Information Asset Audit returns received. Any additional project tasks / resourcing issues will be highlighted to the Project Board.
2	Legacy Systems	There is a risk that, without formal opinion being sought on the applicability of the derogation, Police Scotland's interpretation of the derogation may be incorrect. If this is		The systems will be identified as part of the audit schedule. The assessment methodology mentioned in paragraph above should identify these. Police Scotland will seek legal opinion and	May 2018	Head of Information Management	28/02 – Following an enquiry with the Home Office, correspondence was received on 28 February 2018 which confirms it is intending to implement the derogation under Article 63(2) to allow

		the case, this will have significant negative impact on the overall GDPR/LED project.		if upheld we will develop a plan to address the systems. If the position is not upheld a risk and impact assessment will be conducted to allow for appropriate action.			competent authorities until 6 May 2023 to make systems for automated processing set up before 6 May 2016 compliant with the Law Enforcement Directive (LED). This is covered by note 221 in the Explanatory Notes which states: 'Article 63(2) of the LED provides for a transitional period in respect of the logging requirements for automated processing systems set up before 6 May 2016; in such cases the requirements of Article 25(1), as transposed by clause 62, must apply by 6 May 2023'.

							Such a change would be made by regulation under clause 206 which allows for the Home Secretary to make transitional provisions concerning the coming into force of any provision of the Bill. This would include in relation to Articles 63(2) and (3) of the LED.
3	Compliance by May 2018	We recommend that, where possible, areas of the Data Protection Reform project related to personal data are prioritised over operational data areas in order to increase the level of compliance by May 2018.		Business areas which process the highest volumes of personal data are being prioritised over operational areas where appropriate. This has already been reflected in the Information Asset scheduling. Areas which will not be	May 2018	Project Lead	28/03 – Linked to recommendation 1; the self-assessment process has been completed and work is under-way to highlight any gaps / prioritise activity.

				complaint will be subject to a Risk Assessment and required to detail their plans to move towards compliance.			
4	Staffing Requirements	We recommend that an exercise is undertaken to populate the project plan with all tasks and activities that are necessary to achieve compliance by May 2018. This should include an assessment of the people resource needed to deliver each task and, where appropriate, any specialist skills needed to undertake the task activity. Once this exercise is		In early January 2018 further work will be undertaken to review and populate the existing detailed project plan which will take into account the resources required to deliver each activity.	~~February 2018~~ Ongoing	Project Manager	28/02 - Work continues to populate and develop the Project Document Set, including a full review of identified tasks, risks (inc cross referencing with organisational and strategic risks); additional contingencies and dependencies have been identified and the lessons learned section updated. In addition, membership of the

		complete, a review should be performed to confirm whether there is sufficient people and skills available to address requirements.					Project Board has been extended with Subject Matter Experts and the SPA now forming part of the core membership.
5	Project Governance	Project Meetings are in place and the outcomes are recorded by means of an Action and Decision Log. Significant risks and updates will be escalated via the SRO and Deputy SRO to the Force Executive via existing governance structures.		Project Meetings are in place and the outcomes are recorded by means of an Action and Decision Log. Significant risks and updates will be escalated via the SRO and Deputy SRO to the Force Executive via existing governance structures.	February 2018	Project Lead	28/02 - Already implemented. Process is ongoing as part of Project Board.

6	Comms Plan	We recommend management develop and implement the proposed communications plan for GDPR and LED as soon as is practical. The success of the communications plan should be subject to monitoring by the project team and any remedial action taken to address any instances where clarity is required in relation to roles and responsibilities.		Communication plan in place and subject to continual review via Project Board to ensure understanding across the organisation.	February 2018	Project Lead	28/02 - Already implemented. Comms plan agreed and in place and updated content added to the intranet site. Content will be staged in the coming months leading to implementation and afterwards to ensure the changes are visible.