SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee Public Session**
Date and Time	**22 January 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**General Data Protection Regulation (GDPR) SPA Preparedness**
Item Number	**9.4**
Presented By	**Catherine Topley**
Recommendation to Members	**For Noting**
Appendix Attached:	**No**

PURPOSE

To provide Board Members with an awareness of the changes being made to Data Protection legislation in the UK and the action which requires to be taken by the SPA to implement those changes.

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; however, the UK has introduced the Data Protection Bill, which is based on GDPR and the LED requirements, to update existing data protection laws. The Bill was introduced to the House of Lords on 13 September 2017.

1.3 One of the most significant changes to the legislation is to the enforcement regime. Under GDPR, the Information Commissioner's Office (ICO) will have the power to impose fines for non-compliance of up to £17 million or 4% of annual gross turnover.

1.4 The SPA's preparations for implementing the GDPR are currently being audited by the internal auditors. It is expected that the internal auditors will produce draft findings in December 2017 and a final report in January 2018.

1.5 The Information Management team within the SPA is small (two staff) and to date progress in implementing the required changes has been limited. Following discussions with the Chief Officer (and previously the Chief Executive Officer) plans are underway to appoint three staff on a temporary basis (one solicitor and two data protection staff) to assist the SPA meet the requirements of the new legislation as well as the implementation of recommendations made recently by the ICO.

1.6 There are 12 key steps to GDPR compliance. The steps and the action which requires to be taken by the SPA to implement the new obligations are as set out below.

1. Awareness – ensure key staff and decision makers are aware of the change in the law

Staff need to be aware of the provisions of the new legislation and the changes which it makes to existing legislation.

Action required

- Provide information to the Senior Management Group of the SPA on an ongoing basis and use the intranet to communicate relevant updates. Work is underway to produce a bulletin via the intranet explain the GDPR and the changes it will introduce.
- Scope an electronic solution to deliver training to staff, ensuring that specific staff have appropriate training with more general training given to all staff.

2. *Document the personal data which the SPA holds, where it came from and who it is shared with*

ICO guidance provides that organisations should document the personal data which they hold, the source from which the data originates and who, if anyone, the data is shared with. The guidance is intended to ensure compliance with the GDPR's "accountability principle" which requires organisations to show how they comply with the data protection principles.

Action required

In order to satisfy these requirements, the SPA will conduct an Information Audit. The purpose of the audit is to create a log of processing activities and to establish with information asset owners what personal data is held; the legal basis for processing it; who has access to it; who it is shared with; its protective marking; and how weeding and retention is managed.

The Information Management team has produced a template for completion by heads of service documenting the personal data processed in their respective areas. The template will be circulated in December 2017.

3. *Communicate Privacy Information to subjects of the personal data – Review privacy notices and ensure changes are in effect for implementation dates*

Organisations which collect personal data have to give the subjects of that data certain information, such as to how it intends to use the information: this is normally done by way of a "privacy notice". Under GDPR, privacy notices need to contain additional information including an explanation of the legal basis for processing the personal data, the period in which the data

will be retained and the right of data subjects to complain to the ICO if they have an issue with how their personal data is being handled.

Action required

In order to satisfy these provisions, the SPA requires to establish – through the Information Audit - the information in respect of which the SPA is the data controller. Where the SPA is the data controller, it must ensure that at the point at which the personal data is collected, data subjects are provided with "fair processing information" (e.g. the purpose for which the data is processed, the period in which it will be retained and the rights of data subjects to have access to the data).

The SPA's policies and procedures will require to be amended to reflect these new requirements. A review of all policies and procedures relating to data protection will be undertaken by April 2018.

4. *Individual Rights – Check procedures to ensure they cover all the rights which individuals have under the GDPR*

The guidance issued by the ICO suggests that organisations should check their procedures to ensure that they cover all the rights which data subjects have e.g. the right to be informed of the processing of their personal data, the right of access to the data and the right to rectification or erasure of the data.

Action required

As noted above, all data protection policies and procedures will be subject to a full review by April 2018.

5. *Subject Access – Ensure policy and procedures reflect new timescales and requirements for disclosure*

The GDPR introduces new provisions for the handling of subject access requests (i.e. requests from individuals for the personal data which an organisation holds). At present, organisations may charge for complying with such requests; however, under GDPR in most cases charging will not be permissible. The GDPR also requires responses to subject access requests to be provided within one month, rather than the current 40 day period.

Action required

The SPA's data protection procedures require to be updated to reflect the new timescale and the fact that in most cases it will no longer be permissible to charge individuals for complying with subject access requests. This will be undertaken by April 2018 as part of the full review of data protection policies and procedures.

6. Lawful Basis for Processing – Identify the lawful basis for processing, document it and update privacy notices

Under the GDPR, organisations will require to explain the legal basis for their processing of personal data, in privacy notices or when responding to subject access requests.

Action required

Establish through the Information Audit the legal basis for processing the personal data which the SPA holds. This will allow data subjects to be informed in privacy notices of the basis for processing the data.

7. Consent – Review how the SPA seeks the consent of data subjects for the processing of personal data and ensure that the approach is consistent with the new requirements under GDPR

In order to prepare for the GDPR, organisations require to review how they seek, record and manage consent to the processing of personal data. The GDPR imposes new standards in relation to consent. Consent to the processing of personal data must be freely given, specific, informed and unambiguous: consent must involve a positive "opt-in" and cannot be inferred from silence.

Action required

The new requirements for consent may have only limited impact on the SPA since in many cases personal data will be held lawfully on grounds other than consent. However, given that Police Scotland processes personal data on behalf of the SPA (for example, HR data concerning staff) it will be necessary to ensure that Police Scotland complies with the requirements of the GDPR. This can be achieved by means of a data processing agreement between the two organisations.

8. *Children – Establish procedures to verify the ages of data subjects and if necessary obtain parental consent for the processing of the data*

The GDPR introduces special protection for children's personal data.

Action required

The SPA will establish – through the Information Audit - if the SPA processes the personal data of children and ensure that the consent of parents or guardians is obtained if necessary.

9. *Data Breaches – Establish procedures to detect, report and investigate personal data breaches*

The ICO requires to be notified of data protection breaches where these are likely to result in a risk to the rights and freedoms of data subjects e.g. financial loss or damage to reputation. Under the GDPR, all data breaches must be reported to the ICO within 72 hours.

Action required

In order to meet the requirements of GDPR, the SPA will develop an "incident response plan" setting out how data breaches will be identified and reported to the Information Management team, how any threat to the rights of data subjects will be eradicated or mitigated and how breaches will be reported to the ICO.

10. *Privacy "by Design" and data protection impact assessments*

Privacy by design is an approach to projects which embeds privacy and data protection compliance from the start. Privacy Impact Assessments (PIAs - i.e. assessments designed to identify and reduce privacy risks) are the means by which privacy by design is achieved. Under the GDPR, privacy by design is made an express legal requirement.

Action required

PIAs will be required where the processing of personal data is likely to result in high risk to data subjects e.g. where a new technology is employed which affects the rights of data subjects.

A PIA policy for the SPA is currently in draft form.

11. Appointment of Data Protection Officer to take responsibility for data protection compliance

Under GDPR, public bodies must designate an individual to act as Data Protection Officer who will have responsibility for compliance with data protection legislation. Data Protection Officers must have appropriate support and resources to carry out their role effectively.

Action required

The SPA already has a qualified Data Protection Officer who will be supported by existing staff as well as the temporary appointments referred to above.

12. *Requirements in relation to processing personal data across borders within the European Union*

Under GDPR, there are various requirements upon organisations which operate in more than one EU member state, or which operate in one member state but carry out processing which substantially affects individuals in other member states.

Action required

Although these requirements are less likely than others to affect the SPA, 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.

2. FINANCIAL IMPLICATIONS

2.1 There are financial implications in terms of the additional resources required to satisfy the new requirements. In addition, the ICO may impose significant fines for non-compliance. 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.

3. PERSONNEL IMPLICATIONS

3.1 There are personnel implications in that the intention is to appoint additional staff on a temporary basis to assist with GDPR compliance.

4. LEGAL IMPLICATIONS

4.1 There are legal implications in relation to this paper. The GDPR imposes a range of legal requirements on the SPA and it is essential that sufficient steps are taken to ensure compliance.

5. REPUTATIONAL IMPLICATIONS

5.1 There would be reputational implications in the event that the SPA fails to comply with the new legislation.

6. SOCIAL IMPLICATIONS

6.1 There are no social implications associated with this paper.

7. COMMUNITY IMPACT

7.1 There are no community impact implications associated with this paper.

8. EQUALITIES IMPLICATIONS

8.1 There are no equalities implications associated with this paper.

9. ENVIRONMENTAL IMPLICATIONS

9.1 There are no environmental implications associated with this paper.

RECOMMENDATION

It is recommended that Members note the information presented.