SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee**
Date	**24 July 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**GDPR Update**
Item Number	**6.1**
Presented By	**Lindsey McNeill**
Recommendation to Members	**For Information**
Appendix Attached	**A. Internal Audit Action Plan Update** **B. GDPR End of Project Report**

PURPOSE

To provide SPA Audit Committee Members with a progress update on the General Data Protection Regulations (GDPR) Project and future arrangements within SPA.

1. BACKGROUND

1.1 The General Data Protection Regulation (GDPR) is European legislation which, along with the Data Protection Act 2018, came in to effect on 25 May 2018. 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 SPA's preparations for implementing the GDPR were audited by the internal auditors who reported their findings to the Audit committee in January 2018. Since then, follow up work has been completed to ensure that all actions have been discharged appropriately.

1.3 The initial project to deliver GDPR compliance has now come to an end, with an 'End of Project' Report being signed off by the outgoing Director. This signified a transfer of responsibilities to the new Information Governance Forum, chaired by the SPA Senior Information Risk Owner (SIRO).

1.4 Going forwards, the Information Governance Forum will report progress on relevant action plans and ongoing compliance to the SPA Audit Committee on a six-monthly basis.

2. GENERAL PROGRESS UPDATE

2.1 A review of SPA's Information Assets has been concluded and will now be reviewed periodically to ensure any new or missed IA are captured. Stage one represents the collation of the data from each business area. This data has informed the contents of all policies, notices and agreements. A formal Gap Analysis document has now been produced and adopted by SPA.

2.2 In parallel, all SPA's core Information Management Policies have now been reviewed and are currently out for review by the Senior Management Team, the Board and the Staff Associations.
It is expected this process will be concluded by mid-August and all policies will, thereafter, be published on the Intranet and, where relevant, the Internet.

2.3 Privacy Notices were published on SPA's Intranet and Internet sites in time for go-live on 25 May.

2.4 Anderson Strathern are working alongside PSoS to formalise an agreement as joint data controller of information between SPA and PSoS.

It is anticipated that 2 agreements will be required. One for general GDPR processing and one for the LED processing primarily undertaken by Forensic Services.

2.5 Work will be undertaken in Phase 2 of the project to produce service agreements between SPA and PSoS in relation to services back.

2.6 A separate sub-project plan has been developed by Forensic Services to manage the IT element of compliance required for GDPR. This involves cataloguing all tranche 2 ICT systems being used by Forensic Services, identifying information asset owners, training information asset owners and liaising with suppliers in terms of GDPR requirements and current 'state of play' for their products.

2.7 Over 230 Forensic Services staff have received face to face training and across the whole of SPA, 442 people out of 542 have completed the mandatory Moodle training. (81.5% completion rate.)

2.8 The SPA GDPR Project Board have now prepared a hand-over to the new SPA Information Governance Forum. The IGF will be responsible for ensuring any areas in phase 1 of the plan not already delivered are actioned timeously and for setting a project plan for phase 2 and thereafter moving in to 'business as usual'. The IGF will be chaired by the SPA SIRO and will meet monthly with all business areas being represented.

2.8 The review of the SPA structure has identified the need for an additional, permanent, resource within SPA Information Management. This addresses the risk identified by the independent auditors in respect of the resources required to manage the function within SPA.

3. FINANCIAL IMPLICATIONS

3.1 There are no additional financial implications in this report beyond those previously reported.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications associated with this paper.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications associated with this paper.

5.2 While not directly associated with the content of this paper, the non-compliance of SPA with the ICO audit recommendations and the GDPR legislation may result in penalties for SPA.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no direct reputational implications associated with this paper. However, failure to comply with the legislation and any resulting publicity may have reputational implications in the current climate.

6.2 The report that was concluded by the ICO in October 2017, identifying the areas for improvement that SPA need to consider, was published in full by the ICO on 25 May 2018 in response to an FOI request.

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:

1. Note the progress to date in preparing SPA for compliance with the new GDPR legislation; and,

2. Note that the Information Governance Forum will now report progress of activities to the Audit Committee on a 6-monthly basis.

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 (Apr)	Management Action	Due Date	Owner	SPA Status Assessment (Apr)
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. Once this is completed, SPA should develop a detailed project plan which lists all actions,	Amber	The ~~i~~nformation asset registers from all departments within SPA Corporate Services are now being analysed by the IM team and the DP Lawyer. A further draft of the information asset register has also now been received from Forensic Services and is under review. A Gap Analysis document has been produced	April 2018	Catherine Topley	Green
2	Action plans have been developed to address all identified gaps.		Amber				Green

		the timescales for their completion, action owners and people requirements to deliver them.		and approved. Relevant SPA DP Policies are now drafted for internal review.			
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 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	Amber	The SPA Project Board met on 14th May and reviewed the Gap Analysis, Risks Log, Communications Plan, PID, Action Plan. Timescales have been completed by the DP Lawyer and the Action Plan will stay under review. The IM team continues at 100% capacity and an additional member of staff joined the team on 2 May.	April 2018	Catherine Topley	Green
4	Appropriate resources are assigned to support achievement of action plans.		Amber				Green

		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.		04/06 The structure review has identified the need for an additional, permanent, resource in IM			
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	Amber	The SPA Project Board sat again on Monday 14th May and reviewed the Gap Analysis, Risks Log, Communications Plan, PID, and Action Plan. A Project Board Action Log was produced after the meeting and will continue to be monitored. The Board will	April 2018	Catherine Topley	Green

		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 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.		continue to meet on a fortnightly basis until mid-June. A project approach is now established within SPA and the relevant documentation put in place. The interim Director, Catherine Topley, has been identified as the SIRO. Regular update is being provided to SPA SMG Preparations are now being made for post 25 May: Planning for areas where work will be ongoing, e.g. ICT systems; Identifying and establishing the			

				appropriate governance group to take SPA/FS forward to full compliance. 04/06 TOR's for the IGF have been presented to the SMT. The GDPR Project Board will hand-over to the IGF. The IGF will be chaired by the SPA SIRO and will deliver any outstanding areas for phase 1 of the project and develop/manage phase 2 whilst moving into 'business as usual'. The IGF will meet monthly with business reps from all areas.			

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 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.	Amber	A communications plan has been developed. This will continue to be monitored by the SPA Project Board to discuss the rollout of communications to SPA/Forensic Staff and other stakeholders as required. Two of Police Scotland's Moodle packages have now been rolled out across SPA/FS. Poster have now be displayed in SPA/FS buildings. 04/06 Over 230 staff now trained face to face and last of 3 Moodle	April 2018	Catherine Topley	Green

				modules, entitled 'consent' now available for staff. Posters swapped out w/c 28/5			

Appendix B - GDPR END OF PROJECT

SCOTTISH POLICE AUTHORITY

END PROJECT REPORT

General Data Protection Regulations (GDPR)

Date: 2nd July 2018

Author: Lynne Clark

Owner: Catherine Topley

Version Number: V 1.0

VERSION CONTROL

Author	Role	Version Number	Date Issued	Comments
Lynne Clark	Programme Development Manager	v 0.1	12/06/18	initial draft for team comment
Lynne Clark	Programme Development Manager	v 0.2	21/06/18	Draft for Project Board
Lynne Clark	Programme Development Manager	V1.0	02/07/18	Incorporating Project Board feedback

DOCUMENT REVIEWERS

Name	Role	Draft Review (Y/N)	Review (Y/N)	Sign-off Required(Y/N)
Catherine Topley	Project SRO	Y	Y	Y
Kenneth Hogg	SPA Chief Officer	N	N	Y
Lindsey McNeil	Director of Governance & Assurance	Y	Y	Y
John McCroskie	Director of Communications & Engagement	N	Y	N
Lindsey Davie	Information Management Team	Y	Y	N
Carol-Anne Hilley	Information Management Team	Y	Y	N
Rodica Cararus	Information Management Team	Y	Y	N
Graham Stickle	Risk and Policy Manager	N	Y	N
Fiona Killen	Anderson Strathern	N	Y	N
Fionnlagh Blair	Anderson Strathern	N	Y	N

AMENDMENT INFORMATION

Amended By	Project Role	Version Amended	Date	Comments
Lynne Clark	Programme Development Manager	0.2	02/07/18	Amended with feedback from Project Board

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1.0 INTRODUCTION

1.1 PROJECT BACKGROUND

1.2.1 The General Data Protection Regulation (GDPR) is an EU Regulation which, in May 2018, replaced 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).

1.2.2 The Data Protection Bill was announced in the Queens speech of 21 June 2017 and received Royal Assent on 24 May 2018. The Act updates data protection laws in the UK, supplementing the GDPR, implementing the Law Enforcement Directive, as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data.

1.2.3 One of the most significant changes to the legislation is to the enforcement regime. Under the legislation, 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 global turnover

1.2.4 The SPA's preparations for implementing the GDPR were audited by the internal auditors who reported their findings to the Audit committee in January 2018(http://www.spa.police.uk/assets/126884/415820/441176/441449/item9.1)

This included a number of recommendations to improve the approach.

1.2.5 The Information Commissioner's Office also undertook an audit of SPA in 2017 and a number of the resulting improvement recommendations were linked to the GDPR work so this was taken into consideration within the GDPR planning.

1.2 PURPOSE OF END PROJECT REPORT

The End Project Report is the Project Director's report to the SPA Chief Officer and the Project Board documenting how the project has performed against the objectives outlined in the Project Initiation Document (PID). This report effectively confirms hand-over of all completed products and informs the decision to proceed with the next phase of work to becoming fully compliant with the GDPR and to complete any outstanding recommendations from the Information Commissioner's Office (ICO) Audit.

The Internal Auditors (IA) undertook a GDPR preparedness review of SPA (date) and a number of recommendations were made around the best approach to ensuring SPA reaches compliance with the new legislation. A 2-weekly report on these recommendations has been issued to the Audit Committee Members for assurance that progress is made. This report gives a final status on these recommendations and will be shared with IA to validate that the project approach achieved the recommended control objectives.

Information for the End Project Report has been derived from the Project Initiation Document, the Project Plan the Project Risk Register, Progress Reporting to Project Board and Audit Committee and the project team members.

2.0 ACHIEVEMENT OF PROJECT DELIVERABLES

It was identified early on in the year that working towards compliance with the new regulations would require more resource than was available within the SPA Information Management team. A temporary Director came into post in January and an early piece of work was recruiting temporary resources with GDPR knowledge and capability to build resilience within the team and ensure minimal impact on business as usual. This included an Information Assurance Officer post for a period of 9 months (starting end April) and legal assistance (starting mid-February) over the same period. The associated costs are detailed further within section 3.

Due to recruitment and vetting procedures, the Information Assurance Officer role was slow in being in place. This impacted the timescales for the project but the majority of the key deliverables were able to be put in place as the regulations came into force.

The following project deliverables were outlined within the Project Initiation Document (PID) which was signed off by the Project Board on 16th April '18.

2.1 Staff awareness and education sessions and communications

Police Scotland (PS) have a separate project running in parallel to SPA's which reflects the differences in the scale and scope of the changes they require to implement to be compliant with the new regulations. At the outset of the project a collaboration with PS was established. This meant that the sharing of project information and joint development of policies and training materials was of benefit to SPA and open invitations to each other Project Boards was mutually beneficial.

A poster campaign was implemented to inform staff of the changes they could expect as the date of the new regulations coming into force approached. This was coupled with Moodle training packages which gave staff a general awareness of what the regulations were and how they would be impacted in their day-to-day work. GDPR was discussed at a number of the staff huddles at Pacific Quay to keep a focus on the changes.

A series of roadshows took place in the run up to the 25th of May, with the Information Management team at all the Forensic Service (FS) locations to give a broad outline of the impact on the FS areas of work. These roadshows were well attended with 241 at each of the Forensic Services locations, Glasgow, Dundee, Edinburgh and Aberdeen.

In addition all staff were directed to the links on the PS Intranet where a comprehensive section on GDPR is available.

Evidence: Posters - N:\SPA Team\Governance & Assurance\INFORMATION MANAGEMENT TEAM\GDPR\Phase 1 Posters N:\SPA Team\Governance & Assurance\INFORMATION MANAGEMENT TEAM\GDPR\Phase 2 Posters, Communications Plan; Intranet Information https://spi.spnet.local/spa/Information%20Management/Policies,%20procedures,%20guidance%20and%20forms/Pages/default.aspx; Training Log

Further work required: Training on Data Protection (1)[1] will be an ongoing business as usual requirement which will be monitored and managed by the Information Management team. Further training packages will be developed (2) that keep staff up to date on what is required of them and informed of any ongoing changes to policy, processes and procedures within SPA/FS. Some of this

[1] The numbers in brackets link to the draft GDPR Action Plan for Phase 2 **(Appendix B)**

training will be specific for example for the Information Management team or for Information Asset owners (3).

Work is also underway to develop a comprehensive induction module specifically on Data Protection for any new starts or secondees to SPA (4). This includes Board Members induction and specific training and awareness sessions will also be scheduled for their benefit (5). Sessions carried out; 06/06/2018, 22/06/2018 – Final session: 13/06/2018

2.2 Staff training sessions/materials (initial and ongoing) including update to the staff induction process

Staff training and awareness activities to date are detailed in section 2.1 above.

Staff induction is currently run centrally by PS for all staff across PS, FS and SPA. Some elements of this need to be specifically tailored for SPA/FS staff to ensure the correct policies are adhered to and the processes and procedures relevant to SPA are highlighted. The work on this has begun but full development and implementation will form part of phase 2.

Evidence: Moodle training: https://spi.spnet.local/policescotland/news/Pages/Data-Protection-Reform---GDPR-Now-Live.aspx, Forensic Services Training Needs Analysis

Further work required: The full roll out of the SPA staff induction process with particular emphasis on Data Protection, has now to be put in place (4).

Any additional specific training for IM staff is outlined in section 2.8 (3). However an annual refresh programme for general staff training to include information asset owners and Board Members has to be developed (6).

2.3 Information audit / Information Asset Register

One of the early deliverables for this project was the development of an Information Asset Register. This required every member of staff within SPA and Forensic Services to complete a schedule of all the information held or shared that had personal details or implications. Staff were asked to input to this information audit by the end of April. This register then formed the basis of a number of other deliverables, the related data protection and security policies, the data sharing agreements and the privacy impact notices.

It is now 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.

Evidence: Information Asset Register, Gap Analysis, Data Protection Policy (SPA specific), Information Security Policy (SPA specific), Information Governance forum Terms of Reference.

Further work required: The Information Asset Register is a living document and from now on will be a record of compliance (7). This will be managed by the Information Management team and will be overseen by the SPA Information Governance Forum (see section 2.7)

The Information Asset Register can be found: N:\SPA Team\Governance & Assurance\INFORMATION MANAGEMENT TEAM\GDPR\Information Asset Register\REP 180523 Corporate Master.xlsx

2.4 Data Protection Impact Assessment (DPIA)

There was work to do in defining the reason we are processing data and this was incorporated into the Information Asset Audit and can be seen reflected in the relevant privacy notices.

Evidence: Data Impact Assessment process, DPIA Policy, Privacy Notices:

https://spi.spnet.local/spa/news-and-events/latest-news/Pages/Privacy-Notices.-For-the-attention-of-all-personnel.aspx

Further work required: The information asset register is a live document and will require ongoing management to ensure it is kept up to date and any issues arising can be dealt with through the appropriate governance and processes (7). Training will need to be maintained on an ongoing basis (6).

2.5 Data Sharing Agreements / Data Controller Agreements

In preparation for compliance, legal advice concluded that the relationship between SPA and PS was a controller to controller one.

Broadly three strands of sharing on a controller to controller basis are as follows:

1. For the purposes of SPA's supervisory function of PS
2. Sharing between parties in the provision of forensic services
3. Service-back arrangements (for some services) from PS to SPA

One strand of processing by PS on behalf of SPA:

1. Service back arrangements (for other services)

In addition, correspondence was issued to 3rd parties where data sharing has been identified. This is to establish what arrangements these 3rd parties have in place in relation to GDPR compliance.

Evidence: Draft Data Sharing Agreements x 3, 3rd Party Data Sharing Register

Further work required: To better understand the relationship in each of the services back, a schedule of services will need to be developed and agreed by both parties, PS and SPA (8).

Once a response is received from all 3rd parties with whom SPA/FS shares data, then agreements can be drawn up for sign-off (9).

The finalisation of the data sharing agreements will need to be approved and signed off by all parties.

2.6 Privacy/Fair Processing notices

Work was undertaken to review privacy notices and make any relevant changes. There are two types of privacy notice, one for law enforcement processing which is relevant for Forensic Services purposes and another for processing which falls under GDPR which is relevant for SPA Corporate Services.

A suite of privacy notices were created and published on the SPA/PS websites. These include

- Privacy Notice - Scottish Police Authority staff
- Privacy Notice - Police Scotland officers and staff
- Privacy Notice - For all external contact

Evidence: Privacy Notices:https://spi.spnet.local/spa/news-and-events/latest-news/Pages/Privacy-Notices.-For-the-attention-of-all-personnel.aspx

Further work required: Further consultation will be undertaken with business partners to understand responsibilities and ensure notices are in place as soon as possible. This includes notices with 3rd party suppliers (10) for procurement, HR, recruitment, vetting and occupational health etc. This will require ongoing assurance provided to SPA by Police Scotland.

2.7 Data incident/Breach Management process

This work involves ensuring the right procedures are in place to detect, report and investigate data breaches. A new policy has been drafted to ensure compliance with the requirements of the legislation.

Evidence: Data Incident Management Policy, Terms of Reference for the Information Governance Forum

Further work required: A staff workflow is still required, complete with timescales for compliance, which links directly into the Information Governance Forum and any escalation of issues from there to the Information Commissioner (11).

2.8 The role descriptions and accountabilities across SPA and SPA Forensic Services

As public bodies and as data controllers, Police Scotland and SPA must have Data Protection Officers (DPO). An officer has now been recruited into PS and the existing role strengthened within SPA.

In addition an Information Governance Forum is being established within SPA as a standing forum accountable to the Audit Committee. The forum is chaired by the Senior Information risk Owner (SIRO[2]) and is set up to promote the effective management of SPA information in all formats throughout its lifecycle, to meet operational, legal and evidential requirements; to support the SPA in identifying and managing its information needs, risks and responsibilities, and; to review policies, procedures, and recommending action where appropriate to strengthen information security controls.

Evidence: Role profile for SPA DPO (currently under review as part of the executive review); Terms of Reference for the IGF.

Further work required: While the role of DPO exists within SPA, it will be into the next phase of GDPR compliance before all the role consultations have completed as part of the new SPA structure implementation (3). This will better establish the accountabilities of this role and will provide an additional presence within Forensic Services. The scale and capacity of this resource will be reviewed at regular intervals.

[2] A Senior Information Risk Owner (SIRO) is an Executive Director within an organisation with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation.

Any specific formal training to carry out these roles has yet to be scoped and will form part of a wider training needs analysis (1). However further informal training and mentoring will be ongoing.

2.9 Policies and process maps as defined in the ICO information audit

A number of Information Management / Security policies were reviewed in line with the GDPR regulations. Some of the policies were specific to SPA and some were joint with PS. All the policies were reviewed and refreshed and made available on the SPA Intranet. The refresh of the Intranet with regard to data Protection policies remains the responsibility of the IM team.

Evidence: Suite of policies available on the SPA/PS Intranet:

- Information Security Policy v 4.0
- Data Protection Policy v3.0
- Electronic communications Policy v 2.0
- Data Incident Management Policy v 1.0
- Subject Requests SOP v1.0
- SPA CCTV v1.0
- Access Control Policy v 1.0
- Remote Working Policy v 2.0
- Data Protection Impact Assessments v 2.0
- Freedom of Information V2.0

Link to policies:
https://spi.spnet.local/spa/Information%20Management/Policies,%20procedures,%20guidance%20and%20forms/Pages/default.aspx

Further work required: Due to the tight timescales for implementing the updated policies and making them available to all staff there is still a requirement to ensure these are filtered through the JNCC Policy Working Group (12). Any feedback or amendments from this forum will then be made to the policies.

There are outstanding policies from this first phase of the project and these include: Data Sharing (13), Use of PEDs (drafted, awaiting sign-off) (20) and Information Security in Third Party Suppliers (14).

There are outstanding processes for development and these include: compliance programme spot checks (15), dip sampling (16), access control audits and induction process (4). Some of this work is reliant on services back from Police Scotland and Project Adel

2.10 ICT Compliance

As part of the original PID the ICT system compliance was not scoped as a standalone requirement. It has become clear through the ongoing discussion and review around GDPR that this is a much broader piece of work and will require considerable resource input and a more detailed plan of action.

The systems across SPA/FS have been identified but only 2 of the key systems has been agreed as compliant, Evidence Management System (EMS) and Image Management System (IMS).

Evidence: List of key systems across SPA/FS, FS GDPR Action Plan

Further work required: A full review of all the ICT systems within SPA corporate and SPA Forensic Services has now commenced and will delivered as part of the service back arrangement by Police Scotland (17). A work plan needs to be developed, in conjunction with ICT and any 3rd party suppliers (18), so that expectations can be set both within the SPA and also with the ICO around the timescales to meet compliance and the costs involved.

2.11 Information Commissioner's Office Audit

As identified within the SPA GDPR Project plan, a number of the ICO recommendations from the August 2017 audit were linked to the activity and are now considered to be complete (at the time of writing this was estimated to be 45). The evidence for this can be provided to the ICO in line with their process for any follow up review that might take place. This progress will be reported to the SPA Audit Committee as part of the regular reporting cycle.

Evidence: GDPR Project Plan

Further work required: A number of recommendations made by the ICO were not fully covered within the GDPR project and these will be incorporated into next phase of delivery (19). These actions will now be progressed as part of the work plan for the IGF.

3.0 PERFORMANCE AGAINST PLANNED TIMESCALES AND BUDGET

Expectations were set at the outset of the Project that SPA/FS would not be fully compliant with GDPR by the 25th May. This was reported at both the SPA Audit Committee and the SPA Board. Fortnightly reports were also provided to Audit Committee Members which provided the status against the internal audit control objectives. The key deliverables outlined at section 2 were met by the end of May. Activity timescales slipped within the overall timeframe but the final target date was met for these key deliverables.

As information has been analysed and reviewed through the development of the information asset register and through the course of the project, the scope has expanded and this means that a clear focussed delivery plan will be needed to continue towards full compliance during a second phase, overseen by the IGF.

The costs to date have included the additional support from Anderson Strathern and up to 31/3/18 was a total of £11,772.70. An additional salary cost for the Information Assurance Officer over a period of 9 months is forecast to be £29, 961.

4.0 LESSONS LEARNED

Project Start up - Control Objectives resulting from the Internal Audit January '18 review of GDPR readiness proposed a formal project structure being set up to deliver GDPR compliance. This was a proposal accepted by SPA, however it would have been beneficial to have put this structure in place at an earlier date to allow more time for scoping, planning and resource estimation and management **(see Appendix C)**

Project Management - It would have been helpful to have had a full-time project manager engaged in this work. During the course of the project the IM Team were diverted on to key business as usual

issues which impacted on the project progress. This is consistently an issue when managing projects as well as business as usual.

Collaboration - Working in collaboration with Police Scotland was of benefit to SPA in key areas allowing a flow of information and access to products developed under the PS Project such as the training packages.

In addition materials were shared by Glasgow City Council which assisted the SPA in developing some of their staff awareness communications.

Communications/staff engagement - given the interdependencies with communications from PS and SPA - an improved joined up approach to ensure timeliness and consistency of messaging to staff (this did align at Moodle 3 stage). It was useful to have the opportunities to communicate with staff through the huddles and the roadshows.

The information gathering for the information asset register opened up communications between staff and the IM team. Staff were more open to asking questions around information management and the team gained insight into current practices and procedures. This was true across both the SPA executive team and Forensic Services. This will make it easier in the future to develop training and guidance for staff on matters of information management and security.

Information Gathering – The time for gathering information for the IAR was truncated which meant that additional requests for information had to be issued. Upfront briefings would have helped to be clear on the information requirements.

While the establishment of the Information Governance Forum will give a focus to information issues and management it would help in the delivery of the work, still to be undertaken, if there was more feedback on the products being developed from the senior management team.

5.0 POST PROJECT REVIEW/WORKPLAN FOR INFORMATION GOVERNANCE FORUM

It will be an early requirement for the Information Governance Forum to review the outstanding work plan, assess the resourcing commitment required and plan the timescale for reaching full compliance. This will include an assessment of any further external advice and guidance necessary to complete this work.

It will be at that point that a post implementation review can be factored in to the plan and the methodology for review agreed.

Internal audit will also be carrying out a follow up assurance review on the SPA's preparedness for GDPR and will submit this to the SPA Audit Committee.

A high level list of the expected activity in phase 2 is attached at **Appendix B**. This will need to be assessed fully to identify the skills required to deliver phase 2 and the timescales to complete.

The project risk register is also attached at **Appendix D**.

6.0 SIGN OFF

GDPR Project Board

Senior Responsible Owner

Name (Block Capitals): Catherine Topley

Signature: _____

Date: _____

SPA SIRO

Name (Block Capitals): Lindsey McNeill

Signature: _____

Date: _____

SPA Chief Officer

Name (Block Capitals): Kenneth Hogg

Signature: _____

Date: _____

Appendix A – Terms of Reference for the Information Governance Forum

Information Governance Forum
Terms of Reference

Owner: Director of Governance & Assurance (SIRO)

Version: 1.0

1. Introduction

1.1 The Information Governance (IG) Forum (the forum) is established as a standing forum accountable to the Audit Committee. The purpose of the forum is to promote the effective management of SPA information in all formats throughout its lifecycle, to meet operational, legal and evidential requirements; to support the SPA in identifying and managing its information needs, risks and responsibilities, and; to review policies, procedures, and recommending action where appropriate to strengthen information security controls.

1.2 Meetings will initially occur on a regular basis as detailed at paragraph 4 below but this will be reviewed as appropriate.

2. Membership

2.1 The membership of the forum shall include:

- Senior Information Risk Owner (SIRO) (Chair)
- Data Protection Officer (DPO)
- Legal Services Officer
- Risk Manager
- Financial Services Officer
- Communications Officer
- Forensic Services Business Services Manager
- PSOS ICT Officer
- Governance Support Officer (Secretariat)

2.2 In the event of the Chair of the forum being unable to attend all or part of the meeting, the DPO will deputise for that meeting.

3. Quorum

3.1 Four members of the forum, including either the chair or deputy chair, must be present for the quorum to be established.

3.2 No formal business shall be transacted where a quorum is not reached.

4. Frequency of meetings and attendance

4.1 Meetings shall be held on a fortnightly basis.

4.2 Members of the forum should make every effort to attend all meetings of the forum. The Secretary to the forum will monitor attendance and will report on this annually.

5. Authority

The forum is authorised by the Audit Committee to approve the arrangements for ensuring appropriate and safekeeping and confidentiality of records and for the storage, management and transfer of information, including personal data.

6. Emergency powers

6.1 Where an urgent decision needs to be made in between scheduled meetings, members of the forum can convene an extra-ordinary meeting to discuss a particular issue. Quorum rules in section 3 above will still apply at such a meeting.

6.2 If it is not practicable for forum members to meet in person, matters can be dealt with through telephone or the exchange of emails. The exercise of such powers shall be reported and minuted at the next forum meeting.

7. Duties

7.1 The duties of the forum are to:

- develop and implement a framework for IG across the SPA and to reinforce a strong ethos of IG;
- oversee the annual review of compliance against the IG Standard, to identify priority areas, develop and oversee the implementation of an action plan to ensure compliance;
- inform the review of SPA's management and accountability arrangements for IG;
- review and develop SPA's Freedom of Information publication scheme and review performance;
- develop SPA's IG work programme;
- oversee the ongoing implementation of the new EU General Data Protection Regulations (GDPR) and Data Protection Act 2018;
- ensure that SPA's approach to information handling is communicated to all staff and where appropriate made available to the public;
- co-ordinate the activities of staff given data protection, confidentiality, security, information quality, records management and freedom of information responsibilities;
- monitor SPA's information handling activities to ensure compliance with the law and guidance;
- consider serious breaches of confidentiality and security and where appropriate undertake or recommend remedial action;
- monitor SPA's Information Asset Register/Record of Processing, to ensure that it is fully up-to-date
- review SPA's Data Sharing Register and protocols to ensure that all of SPA's sharing activities are in compliance with the law
- review and inform IG activity reports as defined by the internal and external auditors;
- ensure training made available by SPA is taken up by SPA personnel, as necessary to support their role;
- provide a focal point for the resolution and/or discussion of SPA IG issues;

8. Reporting arrangements to the Audit Committee

8.1 The forum will report to the Audit Committee on at least a six monthly basis and the following documents will be presented:

- minutes of the forum's meetings;
- six monthly report against the Information Governance Strategy and Management Framework and annual work plan.

9. Annual review of the Forum

9.1 The forum will undertake an annual self-assessment to:

- review that these Terms of Reference have been complied with and whether they remain fit for purpose, such as with new national requirements;
- determine whether the forum's planned activities and responsibilities for the previous year have been sufficiently discharged; and,
- recommend any changes and / or actions it considers necessary, in respect of the above.
- provide the Audit Committee with an annual report, which details the outcome of the annual review.

10. Forum servicing

10.1 The forum shall be supported administratively by the DPO, whose duties in this respect will include:

- agreement of the Agenda with the Chair and collation of papers in-line with the forum's Annual Cycle of Business;
- providing written notice of meetings to forum members, and the papers, not less than 5 working days before the meeting;
- taking the minutes and keeping a record of matters arising and issues to be carried forward;
- producing a single document to track the forum's agreed actions and report progress to the forum;
- producing draft minutes for approval within 5 working days of the meeting.

Appendix B – Draft GDPR Compliance Action Plan – Phase 2

Activity Required*	Link to ICO Recommendations	Link to Further Work in Section 2
Data Sharing		
Develop a Data Sharing / Processing Register (to complete once agreements are signed off)		
Develop Data Sharing Policy	D4, D7, D21, D23	
Schedule of Services to be agreed		8
Data Sharing Agreement (with PS) to be signed off	D10, D11, D12, D13, D14, D16, D18, D19, D21	
Data Sharing Agreements (with other bodies) to be signed off	D3	9
FS identify key external bodies with whom information shared		
Data controller agreement	S8, S84	
Data Sharing Review process (map key international data flows)	D14	
check the data sharing status with HO (UK DNA DB)		
Privacy/Fair Processing		
Put in place notices with third parties (contractor/supplier compliance)	Service back from PS	10
HR/recruitment/vetting forms/Occupational Health	Service back from PS	
Confirm requirements for data collected indirectly e.g. surveys		
Clear responsibility when working with partners who collect data on our behalf (build into procurement contracts)		
Ongoing Process Development		
Compliance Programme - Spot Checks - secure storage (S71)	S72	15
Compliance Programme - Dip Samples - access rights (S58), data sharing (D1)	S59	16
Compliance Programme - Access Control Audits - physical access (S68), info security audits (S105)	S68, S103	
Induction process - policy/SOPS to be read, assets req'd, USB log (S46), outline responsibilities of users (S36)	S27, S57, S36, S46 T15, T16, T19, T20, T23	4
SPA leavers process - responsibilities across the organisation; de-commissioning process (SD cards) (S49)	S49, S55, S57, S74, S75, S80, S83	
Ongoing review of Information Asset Register		7
Staff workflow diagram – for date incident/breach management		11

Activity Required*	Link to ICO Recommendations	Link to Further Work in Section 2
Training & Awareness		
Develop a programme for ongoing Staff and Board awareness (changes or updates to policy /Procedure and new staff/Members)	T12, T21, T22 and D6	5
Issue updates to staff on changes to policies including annual refresh		6
Develop a strategy, staff training needs analysis (TNA) (for SMG to agree requirements)	T3,T4, T9, T10, T11, T24, T25, T26, T28, T31, T39	
Develop and deliver training for information asset owners. Specific training for IM team. DPO role confirmation.		3
Take the training plan through unions and staff associations		
Intranet refresh	T32	
Develop further Moodle training packages		2
Policies		
Establish dates for policies to go through JNCC (Policy Working Group)		12
Develop a policy review/refresh schedule		
Data Sharing		13
Use of PEDs		20
Information Security in Third Party Suppliers	S82, S85, S87, S88, S89, S90, S91	14
CCTV		
review for all SPA sites: who owns the CCTV; who is processing the data: who can access it		
Ensure suitable notifications/signage		
Put in place third party access agreements		
ICT Compliance		
Assess all systems identified for compliance		17
Identify the supplier and systems costs to become compliant		
Liaise with PS ICT to identify the plan to work towards compliance		18
Provide an update report to the Audit Committee (July)		
LED		
Take forward any additional activity for compliance		
ICO Recommendations		
Take forward delivery on all outstanding ICO recommendations		19

Skill requirement and Timescales will be determined by the Information Governance Forum

Appendix C – Internal Audit - Control Objectives

The Control Objectives are taken from the Internal Audit report of January 2018. The following is final position, in June, as assessed by SPA)

No	Control Objective	Recommendation	IA Status Assessment (Apr)	Management Action	Due Date	Owner	SPA Status Assessment (Jun)
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. 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.	Amber	The information asset registers from all departments within SPA Corporate Services are now being analysed by the IM team and the DP Lawyer. A further draft of the information asset register has also now been received from Forensic Services and is under review. A Gap Analysis document has been produced and approved. Relevant SPA DP Policies are now drafted for	April 2018	Catherine Topley	Green
2	Action plans have been developed to address all identified gaps.		Amber				Green

				internal review.			
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 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.	Amber	The SPA Project Board met on 28th May and reviewed the Gap Analysis, Risks Log, Communications Plan, PID, Action Plan. Timescales have been completed by the DP Lawyer and the Action Plan will stay under review. The IM team continues at 100% capacity and an additional member of staff joined the team on 2 May. 04/06 The structure review has identified the need for an additional, permanent, resource in IM	April 2018	Catherine Topley	Green
4	Appropriate resources are assigned to support achievement of action plans.		Amber				Green
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	Amber	The SPA Project Board sat again on Monday 28th May and reviewed the Gap Analysis, Risks Log, Communications Plan, PID,	April 2018	Catherine Topley	Green

		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 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.		and Action Plan. A Project Board Action Log was produced after the meeting and will continue to be monitored. The Board will continue to meet on a fortnightly basis until mid-June. A project approach is now established within SPA and the relevant documentation put in place. The interim Director, Catherine Topley, has been identified as the SIRO. Regular update is being provided to SPA SMG Preparations are now being made for post 25 May: Planning for areas where work will be ongoing, e.g. ICT systems; Identifying and establishing the appropriate governance group to take SPA/FS forward to full compliance. 04/06 TOR's for the IGF have been presented to			

				the SMT. The GDPR Project Board will hand-over to the IGF. The IGF will be chaired by the SPA SIRO and will deliver any outstanding areas for phase 1 of the project and develop/manage phase 2 whilst moving into 'business as usual'. The IGF will meet monthly with business reps from all areas.			
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 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	Amber	A communications plan has been developed. This will continue to be monitored by the SPA Project Board to discuss the rollout of communications to SPA/Forensic Staff and other stakeholders as required. Two of Police Scotland's Moodle packages have now been rolled out across SPA/FS. Poster have now be	April 2018	Catherine Topley	Green

		intranet etc.		displayed in SPA/FS buildings. 04/06 Over 230 staff now trained face to face and last of 3 Moodle modules, entitled 'consent' now available for staff. Posters swapped out w/c 28/5			

Appendix D – GDPR Risk Register

SPA GDPR RISK REGISTER														
Risk ID	**Date Risk Identified**	**Date of last review**	**Date of next review**	**Risk Description**	**Untreated Score**	**Risk Mitigation/Controls in Place**	**Current Score**	**Planned Risk Mitigation**	**Target Score**	**Target Date**	**Risk Movement**	**Risk Owner**	**Risk Lead**	**Comments (Including Closure Date)**
GDPR 001	01/03/2018	22/05/18		There is a risk that SPA does not make information on data protection and management widely accessible Impact This would result in reputational issues around SPA's openness and transparency.	20	~~1. ensure all policies, process and structures are widely available and understood by all~~ 1 . Regular updates via staff huddles 2. Moodle training packages	4	1. Review and update all related SPA Policies and Process 2. Communicate publication of policies/processes to staff 3. Give easy access to policies/process on SPA Intranet	4	25/05/2018	↔	Catherine Topley (GDPR Project SRO)	SPA Head of Information Management	
GDPR 004	19/03/18	22/05/18		There is a risk that the current network set up between Police Scotland and SPA means that SPA will not be fully compliant. Impact Failure to meet the privacy requirements of GDPR	20	1. SPA to determine the requirements to separate the SPA and PS domains (link to the ICO audit)	12	1. Plan required on how all ICT systems will be made compliant and by when	4	End of 2018	↔	Catherine Topley (GDPR Project SRO)	SPA Head of Information Management	
GDPR 005	19/03/18	22/05/2018		There is a risk that the required privacy statements with 3rd parties will not be in place by the 25th of May. Note:- this work should be completed by Police Scotland on behalf of SPA. SPA are the signatories on contracts so any potential risk sits with SPA	9	1. SPA to consider the process to ensure all requirements are met	9		0	Timescale to be confirmed as risk will not be mitigated by 25th May	↔	Catherine Topley (GDPR Project SRO)	SPA Head of Information Management	Prev risk wording:- Notices with 3rd parties – suppliers, contracts. While this is a service delegated to PS contracts go out under SPA signature. SPA to

SPA GDPR RISK REGISTER													
				Impact:- Failure to adhere to GDPR legislation, potential fines and reputational damage									decide if this is a risk they wish to accept. (ICO security rec 8) Impact Any action for breaches would be against SPA as the signatory
GDPR 006	19/03/18	22/05/2018		There is a risk that SPA will not be able to respond to subject access requests within regulatory timescales caused by reduced timescales under GDPR and potential for increased requests being dealt with by SPA as the data controller Impact:- Reputational damage Increased resources required Failure to adhere to legislation	8	1. Ensure policies and procedures fully cover the individual rights including the retention/deletion of data & SAR process	8		0	?	↔	Catherine Topley (GDPR Project SRO)	SPA Head of Information Management	Prev risk wording:- There is a risk associated with data subject access requests, if we don't meet GDPR requirements Impact Data subjects may complain to ICO or litigate against SPA for 'harm' caused
GDPR 009	20/4/18	22/05/18		There is a risk that the full impact of GDPR has not been scoped within SPA and/or F/S caused by failure to fully understand the legislation and/or failure to identify all systems/data Impact This may result in potential fines and reputational damage	8	Resources from Anderson Strathern - gap analysis	4	1. continued review of GDPR legislation requirement in comparison to actions being taken by SPA	3		↔	Catherine Topley (GDPR Project SRO)		Note:- Impact of Law Enforcement Directive for SPA Corporate and F/S not known (legislation still a bill). This could have a significant impact on this risk

SPA GDPR RISK REGISTER													
GDPR 010	07/05/18	22/05/2018		There is a risk that SPA retains out of date information without legal basis caused by the failure to weed paper files in accordance with policy resulting in potential fine and reputational damage	8	A process of weeding files to commence	8	Manual review of all files to be completed with weeding in line with current policies	1	?	↔	Lindsey McNeil	SPA Records Manager	Prev risk wording:- Legacy files are being stored securely within Pacific Quay. These require to be weeded as per current policy. Impact Risk of retaining out of date information with no legal basis.
GDPR 11	22/05/2018			There is a risk of SPA receiving fines for failure to comply fully with GDPR legislation caused primarily by delays in ICT resulting in:- Potential financial impact dependent on size of fine Reputational damage	15		15	1. Liaison with ICO regarding progress to full compliance 2. Robust plan in place to achieve full compliance 3. Appropriate governance structure within SPA (including F/S)	1		New risk	Catherine Topley (GDPR Project SRO)		
GDPR 12	22/05/2018			There is a risk that SPA will not receive the required support from Police Scotland ICT to facilitate full GDPR compliance by the end of 2018	9		9		1		New risk	Catherine Topley (GDPR Project SRO)		
GDPR 013	22/5/18			There is a risk that SPA and/or F/S will not have sufficient resources (capacity/capability) to facilitate compliance with GDPR legislation by the end of 2018	12	1. Resources from Anderson Strathern 2. Additional IM resource 3. Wider SPA/FS support	12		1	End of 2018	New risk	Catherine Topley (GDPR Project SRO)	SPA Head of Information Management	

SPA GDPR RISK REGISTER														
				Impact This may result in potential fines and reputational damage										