SCOTTISH POLICE AUTHORITY

Data Protection Policy

Version	**V3.0**
Owner	**Head of Information Management**
Review Date	**May 2018**

Version Control

Version	Date	Author	Description/Amendment
V0.1	March 2013	L Davie	Document Creation
V0.2	April 2013	L Davie	Amend area function names
V1.0	April 2013	L Davie	Final Version
V1.1	November 2015	L Davie	Review & Update
V2.0	November 2016	L Davie	Review & Update
V2.1	April 2018	F Blair	GDPR Review
V3.0	May 2018	L Davie	Review changes

Document Review

Role Title	Draft Review (Y/N)	Review (Y/N)	Sign Off Required (Y/N)	Date
Head of Information Mgt	Y	Y	Y	May 2018
Director (CT)	Y	Y	Y	June 2018
SMT		Y	Y	June 2018
Staff Associations		Y		July 2018

Distribution

Version	Date	Name(s)
V0.1	March 2013	SPA Interim Head of Legal, D Yates
V0.2	April 2013	SPA Board
V1.0	April 2013	Staff
V1.1	December 2015	Audit & Risk Committee
V2.0	November 2016	Staff
V2.1	April 2017	SPA Information Management
V3.0	June/July 2018	SPA SMT, Staff associations
	Aug 2018	Staff

Policy Statement

The objective of data protection is to ensure that the rights and freedoms of data subjects are considered in the collection and processing of personal data.

The purpose of the Data Protection Policy of the Scottish Police Authority (SPA) is to ensure that personal data collected and processed by SPA is managed in accordance with Data Protection Law (the General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and any statutes that amend, repeal or replace this legislation).

It is the policy of SPA to ensure that:

- personal data will be collected and processed in accordance with Data Protection Law
- personal data will be protected against unauthorised access
- confidentiality and integrity of personal data will be assured and maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- data protection training will be available to all personnel processing personal data for SPA
- all breaches of Data Protection Law, actual or suspected, will be reported to, and investigated by SPA's Data Protection Officer (DPO), with assistance from the IM Team and SPA Legal & Compliance

All SPA managers are directly responsible for implementing this policy within their business areas, and for seeking to ensure adherence to the policy by SPA staff.

It is the responsibility of each employee of SPA to adhere to the policy.

Table of Contents

1 Introduction

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected.

Processing and transmission of personal data – generally information relating to living individuals who can be identified from the information – is subject to legislative controls.

Data Protection Law requires organisations to be responsible for and able to demonstrate compliance with the data protection principles, as listed below.

The policy will be subject to review annually and additionally in response to any changes affecting the basis of the original document. The policy will also be reviewed to monitor its effectiveness, demonstrated by the nature, number and impact of recorded incidents.

2 Intention

This policy sets out minimum standards for the collection and processing of personal data by the Scottish Police Authority (SPA) and its business partners and contractors, where appropriate. It is intended to provide a common basis for developing organisational standards and effective management practice and to provide confidence in inter-organisational dealings and third party access/supply.

The policy extends to all personal data processed by SPA and in particular that which is processed on behalf of our business partners.

This policy is based on the requirements of Data Protection Law:

- the Data Protection Act 2018,
- the General Data Protection Regulation (EU) 2016/679, and
- any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection

This policy does not apply to processing under the Law Enforcement Directive/Part 3 of the Data Protection Act 2018. All such processing must be in accordance with SPA's Data Protection (Law Enforcement) Policy.

3 Definitions

Definitions in relation to terminology are contained in Appendix A to this policy.

4 The Data Protection Principles

There are six Data Protection Principles set out in the GDPR, with which data controllers are required to comply. The principles apply to the processing of all personal data. SPA is the data controller and SPA's Data Protection Officer is the Head of Information Management (HoIM).

Separate procedures will be required for each data set/operating system where SPA is the data controller. These procedures must include detailed guidance in respect of compliance with each of the six Data Protection Principles

First Principle

'Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject'.–

SPA may only collect, process and share personal data fairly, lawfully, transparently and for specified purposes. The GDPR allows processing for specific purposes, which are set out in Appendices B and C to this Policy.

Method of Compliance

SPA processes personal data in relation to its staff and also on behalf of its business partners, including the Chief Constable of the Police Service of Scotland (PSoS).

SPA must identify and document the legal basis being relied on for each processing activity. Data Protection Law requires SPA to provide detailed, specific information to data subjects about whom it is processing personal data, depending on whether the personal data was collected directly from data subjects or from elsewhere. Such processing information must be provided through appropriate Privacy Notices issued by SPA, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language, so that a data subject can easily understand the processing information. SPA will publish privacy notices on its Intranet and Internet pages.

Whenever SPA collects personal data directly from data subjects, it must provide the data subject with all the information required by Data Protection Law, including the identity of the SPA as the data controller, SPA's DPO, how and why it will use the personal data and how it will share and protect that personal data. The Privacy Notice must be presented when the data subject first provides the personal data to the SPA. When personal data is collected indirectly (for example, from a third party or publically available source), SPA must provide the data subject with all the information required by Data Protection Law as soon as possible after collecting/receiving the data, unless this proves to involve disproportionate effort or impossibility considering the available measures to locate the named individual. SPA must also check that the personal data was collected by the third party in accordance with Data Protection Law and on a basis which accords with SPA's proposed processing of that personal data.

SPA is solely responsible for compliance with Data Protection Law in terms of personal data it processes and in addition has an obligation to ensure that, where personal data is processed on behalf of, or in conjunction with, a business partner, the processing is in accordance with the Data Protection Principles. In respect to this, SPA is under the legal obligation to enter into data sharing agreements that would state the responsibilities of both parties in respect of data processing.

Any new exercise/activity that involves processing personal data which is likely to involve the extensive collection, or certain other forms of processing, of personal data, will be subject to a Data Protection Impact Assessment (DPIA). DPIAs must be conducted in accordance with SPA's Data Protection Impact Assessment Policy.

Second Principle

'Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (with exceptions for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes)'. – these are not incompatible according to GDPR.

SPA cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained, unless SPA has informed the data subjects of the new purposes and they have consented, where necessary, or SPA has identified a legal basis for processing other than consent.

Method of Compliance

Where information has been obtained for a specific purpose, subject to the exemptions, any non-obvious further use must be communicated to the data subject. The data subject must be provided with enough information in order for them to make an informed decision about authorising that further processing. Consent (usually in writing) will usually be required where another legal condition cannot be met (see Appendix B and Appendix C).

Any purpose for processing personal data must be defined in the relevant SPA Privacy Notices.

Third Principle

'Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

Method of Compliance

SPA will identify and collect the minimum amount of information that is necessary for the purpose of processing for which it was collected. If it becomes necessary to hold/obtain additional personal data about certain individuals, such information will only be collected and recorded in relation to those individuals.

Where personal data is no longer needed for specified purposes, it must be deleted, archived or anonymised in accordance with SPA's Records Retention Policy.

Fourth Principle

'Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

Method of Compliance

SPA shall instigate an audit programme to ensure that all personal data that it is processing are kept accurate and up to date.

Where appropriate, an indicator with the last date of review of information is to be added to files.

Where SPA identifies an inaccuracy, or a data subject indicates that personal data held by SPA or supplied to/from a business partner is inaccurate, the inaccuracy must be rectified by the owner of the data. Where SPA is not the owner, the owner must be advised without delay and in any case within two working days from when SPA became aware of the inaccuracy.

Where SPA has shared any inaccurate data with a 3rd party, notification of the inaccuracy must be sent to the 3rd party within two working days from when SPA became aware of the inaccuracy.

Fifth Principle

'Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.

Method of Compliance

SPA shall follow a documented procedure in relation to the retention of personal data. Personal data may not be retained on the basis that it 'might possibly' be useful in the future and a reasonable, legal use cannot be identified. The SPA's Records Retention policy must be followed at all times.

SPA will take all reasonable steps to destroy or erase from its systems all personal data that it no longer required, in accordance with SPA's Records Retention Policy. This also includes requiring third parties to delete such data where applicable. SPA will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Personal data can be stored for a longer period for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes given that the individual cannot be directly identified and suitable security measures are put in place. However any such storage must be approved by SPA Information Management.

Sixth Principle

'Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

Method of Compliance

SPA has produced a separate Information Security SOP to address the requirements of this principle. All SPA personnel and contractors are required to comply with the Information Security SOP.

SPA has put procedures in place to deal with any suspected Personal Data Incident and will notify any applicable regulator/Information Commissioner's Office or the data subjects where legally required to do so in respect of any information incident. SPA has produced a Data Incident Procedure Policy which will be adhered to in the event of a Personal Data Incident.

5 Training

It shall be mandatory for all SPA personnel and contractors to undertake a data protection induction prior to accessing SPA systems or information.

Line Managers will be responsible for advising SPA's IM Team of 'new starts' and arranging an induction on the first day at SPA. The induction training shall cover both data protection and information security. A record of training shall be maintained on personnel records.

Personnel shall receive refresher training annually.

6 Audit

In order to ensure the continued compliance with the Data Protection Principles, SPA will develop an audit plan based on a risk assessment and will audit personal data in accordance with the outcome of the assessment.

The overriding objective of auditing is to ensure that data held on computer systems is obtained, held, used and disclosed in accordance with Data Protection Law.

The results of audits shall be communicated to the relevant SPA Executive Meetings.

7 Relevant Offences Under the Data Protection Act 2018

It is an offence to knowingly or recklessly:

- handle personal data without the consent of the controller;
- procure or disclose the personal data of another person without the consent of the controller; or
- retain personal data, after it has been obtained, without the consent of the person who was the controller when it was obtained.
- knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.
- Alteration, deletion, etc of personal data to prevent disclosure to data subject

Where an access or data portability request has been received, it is an offence for a controller or related persons, including a processor, to obstruct the provision of information which an individual would be entitled to receive. It is a defence if the obstruction would have occurred regardless of the request. In addition, it is a defence if the person charged acted in the reasonable belief that the individual was not entitled to receive the information.

Defences include where the:

- action was necessary for the purposes of preventing or detecting crime;
- action was required or authorised by an enactment, rule of law or court order;
- action was justified in the public interest;
- person holds the reasonable belief that their action was lawful or that the controller would have consented, had they known what has happening;
- person acted for the special purposes, with a view to the publication by a person of any journalistic, academic, artistic or literary material, and in the reasonable belief that in the particular circumstances the action was justified as being in the public interest.

SPA staff are only permitted to access personal data for SPA's lawful business purposes. Access for any other reasons may be an offence under Data Protection Law. SPA will report all breaches to the PSoS for onward transmission to the Procurator Fiscal.

SPA operates a zero tolerance policy in respect of breaches of Data Protection Law. Any staff suspected of breaching Data Protection Law will be suspended with immediate effect pending the outcome of an investigation and disciplinary/court hearing.

SPA will audit access to personal information on systems it owns or manages. Validations may be issued to staff. Validations require the employee who accessed data to provide a reason, verified by their line manager, for any access to personal data. As such, staff should ensure that any field requiring 'enquirer' or 'reasons' are properly completed on computer systems.

8 Compliance

Diversity

There is no adverse impact on any group in terms of race, religion, gender, sexuality, disability or age in relation to this procedure. The application of this policy/procedure will be monitored to ensure compliance with the organisation's Equality and Diversity Strategy.

Health & Safety

There are no specific additional issues in relation to health and safety relating to this procedure.

Administration

Heads of Business Areas are responsible for ensuring compliance with Data Protection Law in their business area.

The Head of Information Management is responsible for ensuring that a valid notification is maintained with the Office of the Information Commissioner in respect of SPA's processing.

All staff will receive appropriate training/briefings in accordance with the information handled within their role.

Communication

These arrangements will be communicated to staff via Heads of Business Areas and will be accessible via the SPA Intranet.

Relevant sections of the procedure will form part of SPA's Induction Pack and all staff, whether permanent or temporary, joining SPA will require to be made aware of this.

This policy/procedure is available to all SPA staff via the Intranet.

Monitoring and Review

This policy/procedure will be reviewed annually by the document owner.

9 Appendix A – Definitions

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Law. SPA are the Data Controller of all Personal Data relating to personnel and Personal Data used in for business purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under Data Protection Law.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that SPA can identify (directly or indirectly) from that data alone or in combination with other identifiers SPA possess or can reasonably access. Personal Data includes Special Category Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that SPA or third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when SPA collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Category Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

10 Appendix B – Lawful Basis for processing personal data

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

11 Appendix **C** – Lawful Basis for processing special category personal data

Processing shall be lawful only if and to the extent that at least one of the following applies.

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject Schedule 1 to the Data Protection Act 2018 establishes conditions that may assist data controllers with their assessment of whether they have lawful grounds to process the special categories of personal data and criminal convictions data as identified in paragraphs (b), (g), (h), (i) or (j) above.

Some of those which are likely to be of particular relevance to SPA are where:

Under paragraphs (b), (h), (i) or (j)

- Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection. In order to meet this condition the controller must have an appropriate policy document in place, as required under Part 4 of Schedule 1

- Processing necessary for health or social care purposes.

- Processing necessary for reasons of public interest in the area of public health, and carried out under the responsibility of a health professional or another person who owes a duty of confidentiality.

Under paragraph (g)

- Processing necessary for the exercise of a function conferred on a person by enactment or the exercise of a function of the Crown, a Minister or a government department.

— Processing necessary for the administration of justice or the exercise of a function of Parliament.

- Processing necessary to prevent or detect an unlawful act (including an unlawful failure to act).

- Processing necessary to protect the public against: dishonesty, malpractice or other serious improper conduct; unfitness or incompetence; mismanagement in the administration of a body or association; or failures in services provided by a body or association.

- Processing necessary for certain disclosures made under the Terrorism Act 2000 and Proceeds of Crime Act 2002.