Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI0518
Policy Ownership	Operational Support Department
Issue Date	24/05/2018
Review Date	5 years from issue date
Last Updated	11/02/2019
Governing Service Policy	Information Management
Cancellation of	PSNI Data Protection Policy 06/08
Classification	**OFFICIAL [PUBLIC]**

SI0518

Data Protection

This Service Instruction clearly defines the responsibilities placed on the Police Service of Northern Ireland to ensure compliance with the Data Protection Act 2018 and the General Data Protection Regulation. Adherence to this Service Instruction will assist in meeting the objectives of the overall Information Management Service Policy.

Keeping People Safe

Table of Contents

Table of Appendices

1. Aims

This document is aimed at providing an overview of roles, responsibilities and obligations to enable all in the Police Service of Northern Ireland (PSNI) to comply with the legislative requirements set out in the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR) ('the Data Protection legislation'). The PSNI will follow guidance outlined in the College of Policing's Authorised Professional Practice (APP) for Data Protection which is still in the process of being updated and will supplement the information contained here.

This Service Instruction will serve to highlight the key features of the new legislation and set out the practices to be followed in the PSNI. It is not intended to be an exhaustive replication of the contents of the Data Protection legislation but a guide to be followed and adhered to.

This Service Instruction also references the guidance published by the Information Commissioner's Office (ICO). This Service Instruction will also be updated as and when further relevant guidance becomes available at www.ico.org.uk. The PSNI's Data Protection Officer will also have responsibility for review of this Service Instruction.

2. Introduction

On the 25th May 2018, the General Data Protection Regulation ('GDPR') and the Data Protection Act came into effect. GDPR is a European Regulation which is directly effective and covers the general processing of personal data. The Data Protection Act covers those areas of data protection outside of EU competence which are covered in the GDPR including law enforcement.

3. Governance and Responsibility

Legal Obligations

Each Chief Officer is a "Data Controller" and has a legal obligation to ensure that all processing of personal data, by or on behalf of their police service is in accordance with changes to the Data Protection legislation. Every police officer and police staff member, as well as those contractors working for the police, is therefore required to comply with the Data Protection legislation. When the PSNI are involved in partnership working, where both partners determine the purpose for, and the manner in which the data is processed, both partners will be responsible as Data Controllers and are referred to as 'joint data controllers'.

Roles and Responsibilities

The Chief Constable is responsible for ensuring a number of roles and responsibilities are carried out:

- Senior Information Risk Owner (SIRO) – This role at Assistant Chief Constable (ACC) rank provides strategic decision making at a senior level responsible for promoting information governance and ensuring mitigation of information risks, including those linked to personal data;

- Data Protection Officer (DPO) –This role is responsible for ensuring that the PSNI is compliant with the Data Protection legislation. They will inform and advise the PSNI with regards to its obligations under the legislation whilst monitoring and auditing to check for compliance. The Data Protection Officer will be the primary point of contact for the Information Commissioner's Office for matters of data protection and will liaise with PSNI business areas as required;

- Information Asset Owner – Individual with responsibility for information assets in their business areas. They are identified on PSNI's Information Asset register maintained by Records Management Unit.

Record Keeping

GDPR Article 30 and the Data Protection Act Section 61 contain provisions requiring the PSNI to maintain records of their processing activities, and for similar records to be maintained by any other joint controller, or processor processing personal data on the organisation's behalf. The PSNI comply with these requirements through the PSNI's Information Asset Register, maintained by the Records Management Unit. This register assists the PSNI in knowing what personal data is held, where it is held, where it came from and who we share it with.

Privacy Notices

The public have a right to know how the PSNI handles personal data, for example what our retention and disposal policies contain. The PSNI has included a new privacy notice on its website which provides this. There is also a privacy notice for children.

4. Personal Data and Key Definitions

The Data Protection legislation sets out a range of definitions relating to general processing and law enforcement processing. Some of the principle definitions include:

Personal data: any information relating to an identified or identifiable living person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Certain categories of personal data are referred to as "Special Category Data" under GDPR and as "sensitive processing" when the processing is for a law enforcement purpose. These categories relate to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data or biometric data used to uniquely identify a person;
- Health; and
- A person's sex life or sexual orientation.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Law enforcement purposes: the purposes for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security.

Processor: any person who processes personal data on behalf of the data controller (other than a person who is an employee of the controller).

Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to themselves.

5. Overview of Data Protection Legislation

Structure

The Data Protection Act 2018 is structured into seven main parts:

a) Part 1 contains preliminary matters.

b) Part 2 contains provision extending the GDPR standards to areas outside EU competence (the "Applied GDPR" scheme), with the exception of law enforcement and processing by the intelligence services. The DPA 2018 and the GDPR apply substantively the same standards to the majority of data processing in the UK, in order to create a clear and coherent data protection regime. It also sets out certain derogations that provide exemptions from the GDPR.

c) Part 3 contains provision for law enforcement data processing and any interpretation of the provisions of Part 3 should consider the relevant recitals of the Law Enforcement Directive which it is intended to implement.

d) Part 4 provides for data processing by the intelligence services.

e) The remaining parts provide for the continuance of the office of the Information Commissioner (the "Commissioner"), enforcement and offences, and supplementary provisions.

General Processing

The GDPR encompasses 'general processing', which may be defined from a policing perspective as any processing of personal data that does not fall under the scope of Law Enforcement processing (DPA 2018 Part 3) or Intelligence Services Processing (DPA Part 4).

Although an item of personal data may be concurrently subject to both general processing and law enforcement processing, any individual processing operation by the PSNI has to be either general processing or law enforcement processing – both cannot apply at the same time to a particular processing operation. Therefore it is important to determine what type of processing is taking place and apply the correct part of Data Protection legislation.

Examples of general processing for policing can include:

- Training;
- Vehicle and Transport management;
- Human Resources;
- Health management; and
- Payroll.

The Principles

The Data Protection legislation contains six principles or standards of good information handling practice which outline how personal data should be processed. These are legally enforceable standards which the PSNI must comply with unless an

exemption within the Data Protection legislation applies. There is also an additional requirement that the Chief Constable as Data Controller is able to demonstrate compliance with these principles, which is referred to as the 'accountability principle'. Whilst largely similar there are slight differences between general processing and law-enforcement processing so reference should be made to the specific part of the legislation when considering each part.

General Processing Principles

These Principles, in Article 5 of the GDPR, state personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

Law Enforcement Processing Principles

These Principles are available in Part 3, Chapter 2 of the DPA.

a) The first data protection principle - Processing of personal data for any law enforcement purposes must be lawful and fair. Law enforcement processing does not require the processing to be transparent due to the potential to prejudice an ongoing investigation.

b) The second data protection principle - The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

c) The third data protection principle- Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

d) The fourth data protection principle- Personal data processed for any of the law enforcement purposes must be accurate and where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

e) The fifth data protection principle - Personal data processed for any of the law enforcement purposes must be kept for no longer that is necessary for the purposes for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

f) The sixth data protection principle – Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

The Lawful Basis

Article 5 (a) of the GDPR and the first principle of the DPA 2018 requires personal data to be processed ‘lawfully’. For general processing the lawful basis can be satisfied by one of the available lawful bases for processing set out in Article 6 of the GDPR. Further guidance on each lawful condition can be accessed on the Information Commissioner’s Office ‘Guide to the Data Protection Regulation’.

Special Category Data and Sensitive Processing

If the general processing involves Special Category Data there is an additional requirement for at least one of the ten special processing conditions in Article 9 (1) of GDPR to be met; the Data Protection Bill at Schedule 1 also contains additional conditions which may be relied upon.

Sensitive processing is defined in the law enforcement provisions as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

In the context of law enforcement, the personal data being processed will often be sensitive. When it is, the PSNI must be able to demonstrate that the processing is strictly necessary and satisfy one of the conditions in Schedule 8 of the Data Protection Act 2018 or is based on consent. 'Strictly necessary' in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through a less intrusive means.

Where the PSNI carries out processing in relation to special category data in reliance of a Schedule 1 condition or sensitive processing based on the consent of the data subject, or based on another specific condition in Schedule 8 of the Data Protection Act 2018 the PSNI must put in place additional safeguards these include how we record such reliance. The PSNI have developed additional guidance on how records/additional safeguards should be kept.

6. Data Protection by Design and Data Protection Impact Assessments (DPIAs)

The PSNI have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection and privacy considerations into processing activities.

One of the main ways in which this can be achieved is through the completion of Data Protection Impact Assessments (DPIAs).

DPIAs are mandatory for certain types of projects or initiatives going forward that result in a high degree of risk to the rights and freedoms of individuals. This includes projects which intend to use large scale processing of special categories of data.

This approach promotes data protection compliance from the start (i.e. by design). The DPO will provide advice to the PSNI in relation to the completion of DPIAs.

DPIA's ensure that technical measures are adopted as far as is practical/proportionate during the development of major IT systems to reduce the instances of poor quality data. Such measures may be informed by identification/reporting and rectification activities resulting from individuals exercising their right.

Where a DPIA indicates that processing would be of high risk the DPO will liaise with the ICO in relation to this processing.

7. Rights of individuals under the Data Protection Legislation

The Data Protection legislation contains enhanced rights for individuals over how the PSNI processes their personal information. The rights that individuals have over their data differ depending on whether the information falls under the remit of "general processing" (GDPR) or processing for law enforcement purposes (DPA Part 3).

General Processing Rights

Chapter 3 of the GDPR (Articles 12-23) sets out the rights for individuals. These include:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making including profiling.

Law – Enforcement Processing Rights

Part 3, Chapter 3 of the Data Protection Act 2018 includes the following individual rights:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure or restrict processing; and
- The right not to be subject to automated decision making.

Certain rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the law-enforcement provisions. Further, there are

exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights. Further detail on other rights can be found in Appendix A and in the section entitled 'individual rights' in the Guide to the GDPR and the Guide to Law Enforcement Processing (Part 3 of the Bill) on the Information Commissioner's Office website.

Enacting Individual Rights

When individuals enact their rights, the PSNI must respond within one month to that request. This can be extended by a further two months if the request is complex or the PSNI receives a large number of requests (general processing only). The response provided by the PSNI which includes any reasoning for why a right may or may not be enacted must be provided in a clear and transparent manner. Under the Data Protection legislation the PSNI will not charge an individual for enacting their rights. Where a request is to be deemed manifestly unfounded or excessive, the request will be progressed; however, clarification will be sought from the requester with regards decreasing the parameters of the search.

When an individual requests their rights are enacted, the PSNI will be required to further process their personal information in order to keep a record of what amendments, if any, have been made and the justification for any decisions made.

The PSNI's Corporate Information team will assist individuals wishing to enact their rights under GDPR and Data Protection Act 2018 as well as liaise with the Information Commissioner's Office in respect of these if required. The process for dealing with subject access requests is set out at Appendix B and the process for dealing with all other rights is set out at Appendix C.

Requests linked to enacting individual rights should be directed to:
Corporate Information Branch
Police Service of Northern Ireland
Police Headquarters
65 Knock Road
Belfast
BT6 5LE
Telephone: 02890700164
Email: DataProtection@psni.pnn.police.uk

All data protection rights requests or queries should be sent to these addresses rather than to individual staff members, as staff absence could result in a delay of the process and non-compliance with legislative timeframes.

Where a subject request relates to Information held within Occupational Health Department (OHW), that request will be forwarded by the Corporate Information Branch to OHW. OHW will process that request.

There is no provision in the legislation with regards to, in what format a requester should enact their rights; however, if the request is not in writing the PSNI will ask that it be put in writing and proof of identification will be sought before beginning to process the request. It should be noted a request can be made verbally. Whilst officers/staff should direct members of the public to put their request in writing as the PSNI is under an obligation to verify an individual's identity, if this is not possible (e.g. an individual is in custody and the PSNI is assured of their identity), then the officer or staff member should send this request in writing to the Corporate Information Branch, confirming, if it is reasonable to do so, those details with the requester. The Corporate Information Branch will respond to the officer or staff member and to the requester if an address is provided.

The Corporate Information Branch will be the liaison between the requester and other areas of the PSNI. It will be this Branch who will ascertain the business area/s' position on the processing of the data to be reviewed; they will then advise the requester if their request has been successful or not. Where a request involves information held by OHW, this request will be processed by OHW. Where necessary and appropriate the PSNI will make all reasonable steps to amend, delete or rectify personal data, and information held by third parties with whom we have shared the data. This is in line with advice and guidance from the ICO.

Where information is deemed to be suitable for rectification, restrictions or erasure, however, is required for evidential purposes the controller must restrict it's processing.

Where the PSNI need to enact the rights of rectification, erasure and restriction, we will do so as far as is reasonably practicable. This rectification must be done within one month, or three months in complex cases (this extension is available for general processing only). Where no action is taken individuals have the right to be informed of how to seek a judicial remedy.

The response letter to the requester will, where possible, and not subject to any relevant exemptions, provide justification around why the PSNI have decided to accept their request or whether processing

of their personal data will continue. It will also include reference to the relevant sections of the PSNI's Retention and Disposal Schedule. The data subject will be provided with the ICO's contact details to enable them to make a request to, or complain to the Commissioner, if they feel it necessary to do so. A requester will also be reminded of their right to apply to a court.

Right to Access – Subject Access (SARs)

This right is applicable to both general and law enforcement processing.

Under Article 15 of GDPR and section 45 of the Data Protection Act 2018, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the following information:

- The purposes of and the legal basis for the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer:
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the rights which individuals have with regards to how their data is processed;
- The right to lodge a complaint with a supervisory authority – the PSNI will provide the details of the ICO when sending out a SARs response:
- Where the personal data are not collected from the data subject, any available information as to their source; and
- The existence of automated decision-making, including profiling.

A data subject can request a copy of any personal data which is held by the PSNI in electronic and manual format. More common requests include, CRV, personnel files, and incident reports.

Two forms are used when applying for this information ("DAT 1" and "DAT 2"); these detail the supporting identification documents, if any, which are required alongside any request. The "DAT1" form is for use by members of the public and non-serving/retired members and is contained on the external PSNI website. The "DAT2"

form is to be used by internal staff members; this is available on the intranet. These forms can be submitted to the Branch either in hard copy or electronically via the email: DataProtection@psni.pnn.police.uk

The PSNI can only provide personal data to the requester. To apply on behalf of another person (the requester), a letter of authorisation or form of authority must be included which indicates the data subject's consent, which must be explicit and concise. An external requester will still be required to sign the form and submit relevant identification documents and ID regardless if they are submitting their request in hard copy or electronically. Details of suitable identification are included in the form.

The PSNI will not charge for processing SARs. Where a request is to be deemed manifestly unfounded or excessive, the request will be progressed where possible; however, clarification will be sought from the requester to assess what can reasonably be provided to them.
Article 15 of GDPR and Section 45 of the Act provides a right for data subjects to have access to their personal data, unless an exemption applies. Staff in the Corporate Information Branch, in consultation with business areas, will apply these exemptions where relevant. It is imperative that the business area highlight any harm/risk that may be associated in releasing this information to the data subject to the Corporate Information Branch in order for the branch to apply any relevant exemptions. All rationale in relation to the disclosure/non-disclosure of personal data to an individual will be documented on the Corporate Information case management system. This may be required to be made available to the ICO.

Appendix B provides an overview of processing a SAR within PSNI. To enable a request to be answered, information is then requested from relevant business areas via a case tracker form (a copy can be obtained from the branch). The PSNI have a one calendar month legislative timeframe to comply with in relation to SARs; therefore, it is imperative that requests are processed as time efficiently as possible by each business area involved.
When personal data is supplied to a requester, an explanation will be provided to account for any information which may have been withheld under exceptions, unless there is harm/risk in revealing these details to that person; i.e. disclosure would undermine an ongoing investigation.

It is the responsibility of the PSNI to provide information held on their own system and the Police National Computer (PNC); however, currently a request for personal data held on PNC will be forwarded by the PSNI to National Police Chiefs Council (NPCC) and subsequently responded to by them.

There is no requirement for the PSNI to review a decision made regarding what has been supplied in response to a SAR. The data subject will however be provided with the ICO's contact details to enable them to make a request to, or complain to the commissioner, if they feel it necessary to do so, or to apply to a court for a compliance order.

8. Exemptions

There will be occasions when the PSNI is required to restrict the rights offered to individuals under the new data protection legislation and occasions where the PSNI are able to lawfully disclose personal data in prescribed circumstances. These restrictions or exclusions are known as exemptions and are only applicable where necessary and proportionate.

The exemptions are found in Part 3 and Schedules 2-4 of the Data Protection Act 2018 and the most commonly used exemptions by the PSNI will include:

- Crime and taxation; including the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- Protect national security;
- Avoid obstructing an official or legal inquiry, investigation or procedure;
- Information required to be disclosed by law etc. or in connection with legal proceedings and legal advice;
- Functions designed to protect the public – linked to dishonesty, malpractice, other seriously improper conduct or the unfitness or incompetence of persons;
- Protection of the rights of others – withholding third party information;
- Legal Professional Privilege;
- Confidential references; and
- Management forecasts.

Exemptions will apply to specific provisions of data protection legislation. Corporate Information Branch will be able to advise around relevant exemptions in relation to data subject rights.

9. Further processing of information

Information Sharing

The police have an absolute and unconditional obligation to take all steps

necessary for the prevention of crime and disorder. For the PSNI this is both a statutory and common law duty. In order to fulfil its policing purposes, the PSNI are required to share personal data with a variety of external organisations.
The sharing of information should be done so in full compliance with the Data Protection legislation. The disclosure should be limited to the minimum amount of information required to achieve that purpose.

Many third party data users will have informed the police that they are an organisation with whom they will share data and an Information Sharing Agreement (ISA) may be in operation. If they have not, data can still be shared with the PSNI under the Act in order to: prevent and detect crime, apprehend and prosecute offenders, and if non -disclosure would be likely to prejudice either of these. A "Form 81" should be used to request the information.

If information is to be shared between the PSNI and other organisations on a regular basis, an information sharing agreement should be created setting out the expectations for processing personal data in line with the data protection principles.
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. There needs to be a clear agreement between the parties as to who is responsible for what and hence who is liable for what.

Where an organisation is provided with information by the PSNI and determines how the processing will be conducted, both are data controllers. Whilst both parties are responsible for the security and means of processing it would be advisable that the PSNI provide guidance around the safeguards and procedures used when they are to process the data.

When somebody else conducts processing on behalf of and under strict instruction from the PSNI they are known as data processors and must:

- Provide guarantees to implement appropriate technical and organisational measures sufficient to secure the protection of the rights of the data subject.
- Be governed by a contract in writing, setting out clearly what they should do.
- Only do as instructed by the Controller, or to comply with a legal obligation.
- Give special consideration and safeguards in relation to the processing of special category data.

The Corporate Information Branch will provide an advisory function to the PSNI on the review of Information Sharing Agreements. At the time of writing of this Service Instruction an external recruitment is ongoing and this function has not yet transferred to Corporate Information.

Procurement and Contractual Agreements

When entering into contractual agreements with external contractors, both public authorities and non-public authorities as well as with Data Processors, the PSNI will ensure compliance with Data Protection legislation. Significant review has taken place of the PSNI's procurement policies and guidance in relation to compliance with new data protection legislation.

Transfers to Third Countries or International Organisations

Personal data should only be transferred outside the European Union if appropriate safeguards are in place or the country has been deemed as offering an adequate level of protection.

The PSNI must closely adhere to provisions set out in Chapter 5 of the GDPR and DPA. Article 49 of GDPR highlights derogation for the transfer of data in the absence of an adequacy decision or appropriate safeguards. These include explicit consent of the data subject, public interest, vital interests of the data subject, in relation to legal claims, and prevention of an immediate or serious threat to security of persons and countries.

Further information on safeguards can be accessed via the ICO's website.

10. Contravention of Data Protection Legislation

Report of a Data Protection Breach

The PSNI is under an obligation to ensure that it or any of its data processors implements appropriate technical and organisational measures to ensure level of security appropriate to the risks arising from the processing of personal data.

The PSNI have clear policies and procedures in place setting out the information security standards required of all officers, staff and contractors. These are set out in Service Instruction SI0516 'Information Security' and underpinned by specific security standards; this includes the requirement to report information incidents in line with those standards. An information incident is defined as an event that has compromised or has the potential to compromise the confidentially, integrity and/or availability of any PSNI information asset. Where this involves personal data

there are additional obligations on PSNI to report serious breaches within 72 hours to the Information Commissioner's Office and potentially to individuals affected by the breach. PSNI's Information Security Standards 1.05 - Incident Identification and Reporting and 2.04 - Information Incident Management have been updated to reflect these new requirements.

Offences under the legislation

There are a number of offences linked to the mis-use of personal data:

- Data obtained unlawfully;
- Re-identification of de-identified personal data without the consent of the data controller;
- Altering, defacing, blocking, erasing or destroying data to prevent disclosure:
- Retaining data against the wishes of the Data Controller, even where the data was originally obtained lawfully.

If a police officer or member of police staff is found to breach the data protection legislation, and/or are believed to have committed one of the above offences, any allegations of criminality and/or misconduct will be thoroughly investigated. When appropriate, these staff will be subject to misconduct proceedings.

11. Training

All police officers and police staff are required to carry out mandatory Data Protection training when they join the PSNI, and every three years thereafter.

PSNI's Data Protection training package is being updated and will be relaunched to highlight changes to the legislation. This will be mandatory for all officers and staff to complete. Further details will be made available. An interim training package is available and provides an overview of the new data protection legislation and key changes. It is imperative that mandatory training is kept up to date and training refreshed, as compliance is audited.

12. The Information Commissioner's Office

Regulation of the Data Protection legislation is the function of the Information Commissioner's Office. That office has a range of powers which allow it to investigate a public authorities handling of personal data. If the PSNI are found to be in breach of the legislation the ICO have a number of enforcement powers they can engage. Depending on the type and extent of the contravention the PSNI could face fines of up to £18,000,000 for non-compliance.

If dissatisfied with the PSNI's handling of personal data, the data subject may complain to the ICO directly.

The ICO have a Belfast Office situated at:
Information Commissioner's Office
3rd Floor
14 Cromac Place
Belfast
BT7 2JB
Tel: 028 9027 8757 or 0303 123 1114
Email: ni@ico.org.uk

The PSNI will co-operate fully with the ICO in relation to requests regarding how PSNI process personal data. This includes making available, to the ICO, any relevant data required to perform its tasks. The PSNI will also make available the contact details of the DPO to the ICO.

Appendix A Rights in relation to General Processing and Law Enforcement Processing

1. Right to Rectification (Article 16 of GDPR) and Section 46 DPA 2018

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate or incomplete personal data concerning them. Also included in this right is to have a supplementary statement added to their personal information.

2. Right to Erasure or restriction of processing (Article 17 and Article 18 of GDPR) and Section 47 of the DPA 2018

2.1 General Processing

In certain instances individuals can ask that their personal data is erased or restricted. Those which may be relevant to PSNI are noted below:

- When personal data is no longer necessary for the original purpose;
- Consent is withdrawn and there is no other basis for processing;
- The data subject objects under Article 21 and there is no overriding legitimate interest;
- Personal data has been unlawfully processed;
- The data needs to be erased to comply with a legal obligation.

Any deletion of personal data by PSNI will be carefully considered. Where there is an underlying business requirement PSNI may reject this request and continue to process the data for the following reasons:

- A legal obligation;
- A task carried out in the public interest/exercise of official authority;
- The establishment, exercise or defence of legal rights;
- Archiving purposes.

Where it is claimed that data is inaccurate or the right to object (Article 21) has been exercised individuals can require the controller to restrict processing until verification checks have been completed. Individuals may also require controllers to restrict processing where there is no legal basis however the data subject opposes erasure, or if it is only needed for legal claims.

In certain circumstances, the data subject shall have the right to obtain from the controller restriction of processing. "Restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future. Where it has been restricted, processing other than storage should only occur for a number of specific reasons, namely – the consent of the data subject, legal claims of the data subject, to protect rights of others or in the public interest.

Article 19 of GDPR places a responsibility on the PSNI, where possible, to communicate any rectification, erasure or restriction of processing to anyone with whom the data has been shared.

2.2 Law Enforcement Processing Individuals have a right to have personal data erased or to restrict its processing. PSNI must erase personal data without undue delay if:

- the processing of the personal data will infringe the data protection principles;
- It does not meet safeguards for archiving and processing of sensitive personal data; or
- PSNI have a legal obligation to erase the data.

The Information Commissioner's Office recognise that complete deletion of personal data in electronic systems can often be problematic, but you should ensure that you have adequate systems and storage media in place to comply with an individual's request for erasure. If deletion is not technically possible, you should at least take steps to put the personal data 'beyond use'.

PSNI must tell an individual if we are not going to erase or rectify the personal data they have requested that you amend. We must also inform them of their right to raise a complaint with the Information Commissioner or take the matter to court. PSNI may limit the provision of such information however, where a request for rectification is received it is necessary and proportionate to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

3. Right to Data Portability:

This right is applicable to only general processing.

Under Article 20 of the GDPR, the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The personal data must be provided in a structured, commonly used and machine readable form. The information must be provided free of charge.

The right to portability does not apply to all data. The data must have been obtained through consent or contract and the processing of such needs to be automated. Data applicable to this right must have been knowingly and actively provided by the data subject only.

This right will not apply to the data if 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 Data Controller. It is unlikely this right will apply to the PSNI.

4. Right to Object:

This right is applicable to only general processing.

Individuals have the right to object to the processing, by the PSNI, of their personal data where processing is necessary for the performance of a tasked carried out in the public interest or in the exercise of official authority vested in the controller, or when processing is based on legitimate interests.

To continue processing, PSNI must be able to demonstrate compelling legitimate grounds, which override the interests, rights and freedoms of the data subject. Or it must be necessary for the establishment, exercise or defence of legal claims.

5. Right to not be subject to automated decision-making:

This right is applicable to both general and law enforcement processing.

Article 22 of the GDPR and Section 49 DPA gives individuals the right to object to decisions made about them solely on the basis of automated processing, where those decisions have legal or other significant effects. This includes processing where there is no human intervention. The PSNI does not ordinarily use automated decision making or profiling. Where a significant decision has been taken

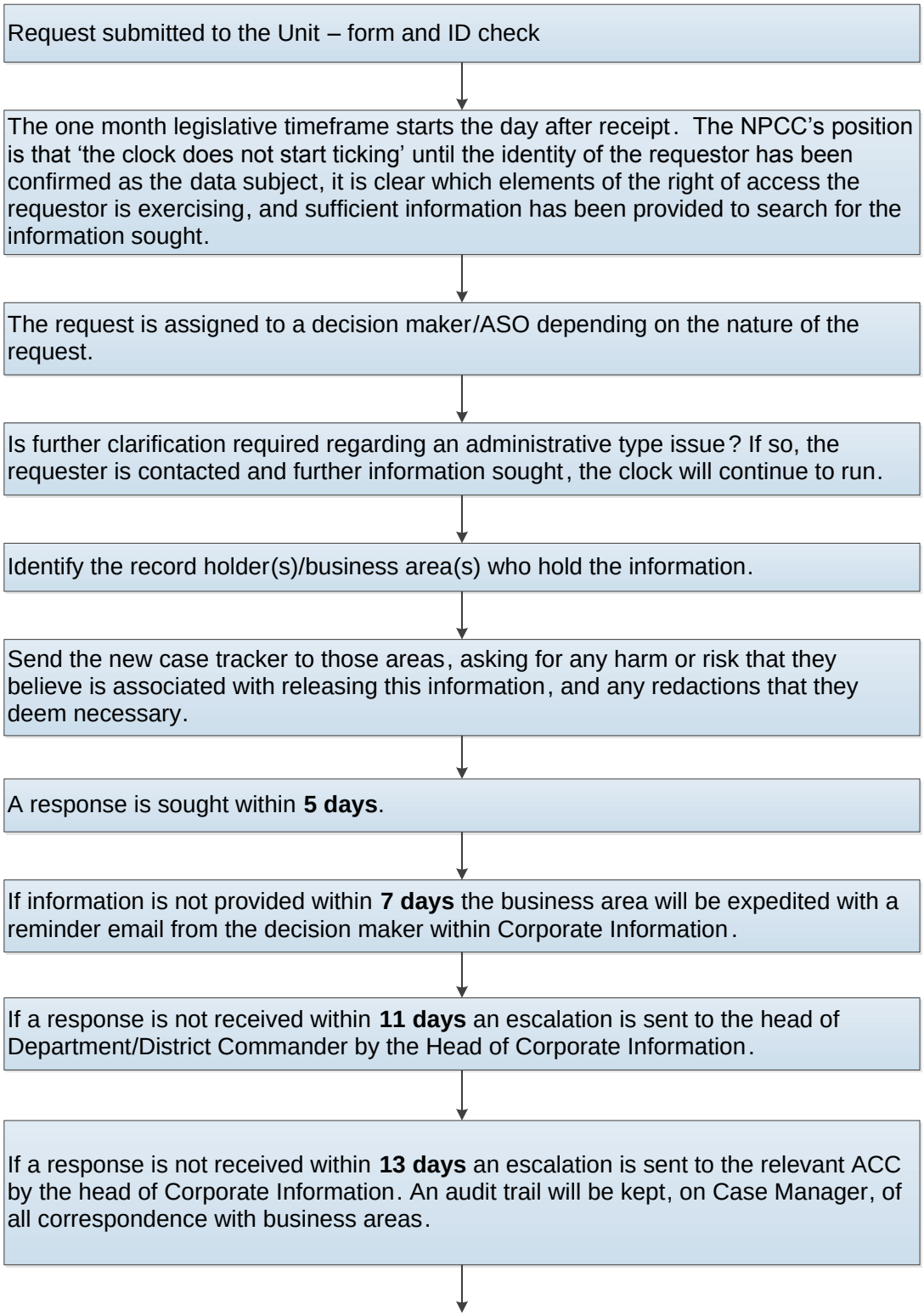
based solely on automated processing the PSNI must, as soon as practicable, advise the data subject in regards to this. One occasion where it may be used is as part of Human Resources recruitment techniques.

Processing by these means can continue if it is:

- Necessary for entering into, or the performance of a contract between the data subject and the data controller;
- Authorised by UK law;
- Based on the data subjects explicit consent.

However, the PSNI must have measures in place to safeguard the process, for example, possibility of human intervention.

Appendix B Processing a Subject Access Request (SAR)



Once the information is retrieved it should be scanned on to Case Manager, and any comments from the business area noted also.

The material should be revised in line with business area comments and redactions made. Consent should be sought, from third parties, if necessary. If the request is deemed to be manifestly unfounded or excessive the requester will be contacted to assess if information can be provided.

Before the decision maker has completed the case it should be discussed with the manager (EO1) as part of a quality assurance process checklist by decision maker

Once quality assured, the response should be issued to the requester by the specified means. This will include the information set out in the document "response letter to requester". If CDs are being sent to the requester, these should be encrypted and sent on a different date to the encryption password.

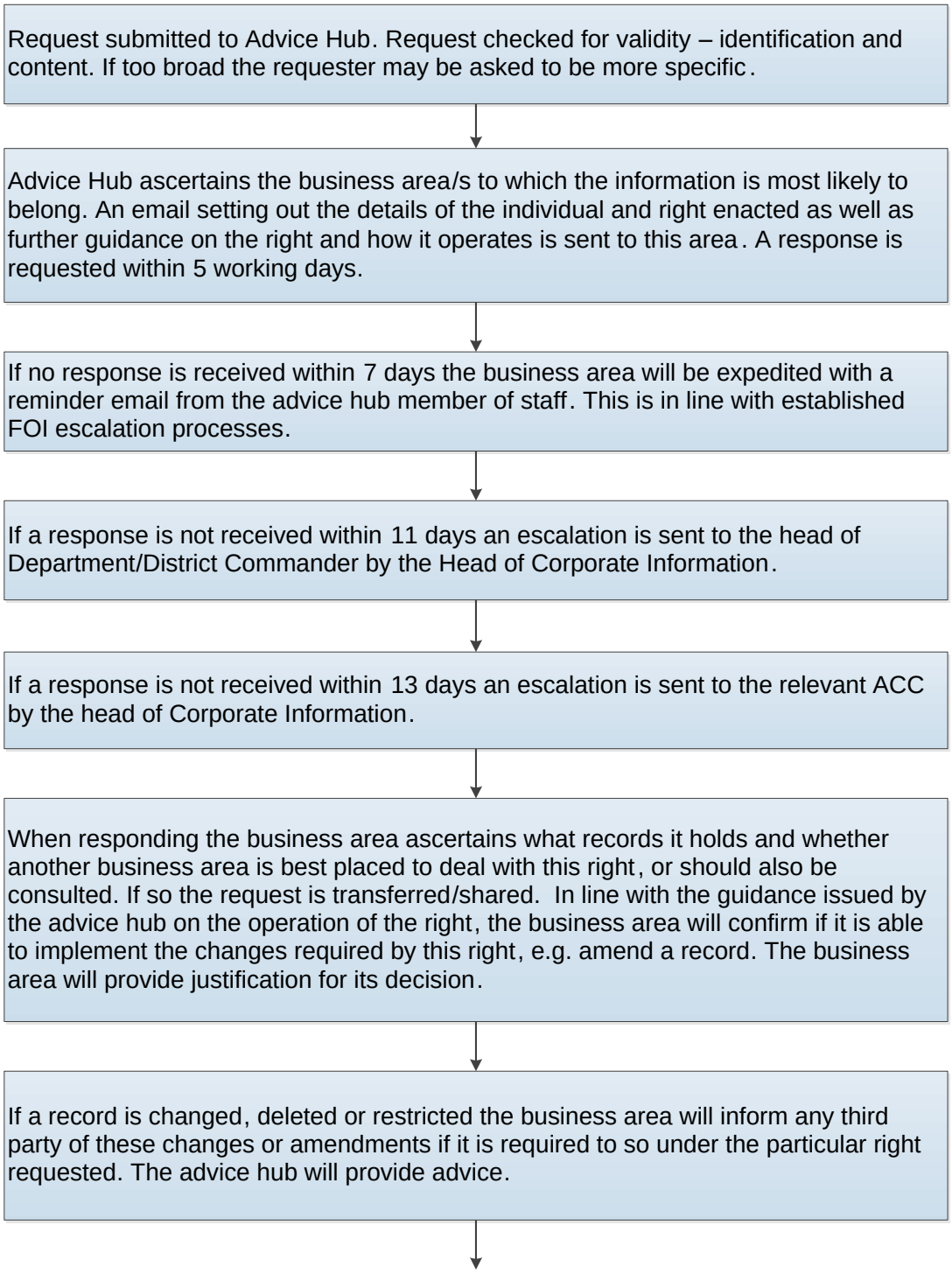
Before or on the day of the one month deadline, if no response is being issued, a letter should be issued to the requester to both apologise for and explain the reason for the delay. If the request has been deemed complex and the additional time extension allowed for under the legislation (a further 2 months – only for general processing) is relevant the requester should be advised of such.

A requester may contact the unit once they have received their information or whilst they are waiting on their response. These will be classified on Case Manager under three headings:

- DPA Internal - SAR - **Complaint from Requester** - complaints about our SAR responses should be attached to this action. Whilst the Unit can assist with short queries, no formal internal review will be conducted of the information. The requester will have already been provided with the contact details of the ICO when issued with their original response.
- DPA Internal - SAR - **Follow on query received** - further queries should be attached to this action – for example, explanation of terms.
- DPA Internal - SAR - **Time Delay Enquiry** - any emails about time delays should be attached to this action.

If the ICO are contacted by the requester and PSNI are issued with a "Request for Assessment" (RFA) the case should be reviewed by the office manager (SO) and the ICO responded to by the date requested.

Appendix C Processing a request for individual rights to be reviewed (including rectification, erasure and objection)



In a complex case where it is not clear if the PSNI can enact the right, advice will be sought from the business area with most expertise e.g. records management or ICS as to how best to proceed. This will likely involve discussions with managers within Corporate Information branch and relevant business areas.

For some individual rights the legislation advises that any changes/deletions should be made without undue delay. In line with ICO advice, the PSNI will have one month to respond to requests, except in complex circumstances, where this can be extended by a further two months. The necessity for extension will be assessed on a case by case basis and applies to general processing only. These requirements will be detailed on the advice document to be prepared for business areas.

The advice hub will issue a final response to the requester setting out the action it has taken. If not enacting the right the advice hub will provide the requester with reasons in line with the Data Protection legislation as to why it is not enacting the right.

As with subject access requests, if the requestor is dissatisfied with their response, they have a right of recourse to the ICO. Whilst the Unit will endeavour to deal with any minor issues at a local level, they will not offer a complaint review of the decision. If the requestor is unhappy and reports their issue to the ICO a Unit Supervisor will deal with the complaint submitted, by the ICO, to the Unit.

Appendix D Contact Details

Service Instruction Author

Deputy Principal Corporate Information Branch

Branch Email

zDataProtection and zFOI