SIS Bulk Personal Data Handling Arrangements

*All gists in the following extract are underlined

Contents

1.0 INTRODUCTION

1.0.1 These Handling Arrangements are made under section 2(2)(a) of the Intelligence Services Act 1994 ("the ISA 1994"). They come into force on 4 November 2015.

1.0.2 The Arrangements apply to the Secret Intelligence Service (SIS) management (acquisition, use, disclosure and retention) and oversight of the category of information identified in 1.1.5 below, namely "bulk personal datasets" (BPD).

1.0.3 **The rules set out in these Arrangements are mandatory and are required to be followed by all staff.** Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal.

1.0.4 These Arrangements have three functions. First, they describe the processes that SIS applies in relation to BPD. Second, they refer to specific published guidance to staff in SIS with respect to the acquisition, use, disclosure and retention of BPD. Third, they set out a list of requirements and considerations that must be followed and applied by SIS staff when handling BPD. Some of the detail underpinning those requirements is contained in documents annexed to these handling arrangements. In particular, staff must ensure that no BPD are acquired, used, retained or disclosed except in accordance with these Arrangements, (including the underlying documents referred to therein), and the legal framework set out in paragraph 2.0. Compliance with these Arrangements, in conjunction with the paragraph 2.0 legal framework, is designed to ensure that the acquiring, use, retention and disclosure of BPD by SIS continues to be lawful, justified and tightly controlled, and is subject to robust and effective safeguards against abuse.

1.0.5 The Arrangements satisfy the duty of the Head of the Secret Intelligence Service to ensure that arrangements are in place to secure that no BPD is acquired by SIS except so far as necessary for the proper discharge of its functions, and that no information is disclosed except so far as necessary for the proper discharge of their functions or for the additional limited purposes set out in sections 2(2)(a) of the ISA 1994.

1.1 The information covered by these Arrangements

1.1.1 SIS needs to collect a range of information from a variety of sources to meet the requirements of its statutory functions, and it does this in accordance with its legal obligations (in particular, the information gateway provisions in the ISA 1994).

1.1.2 BPD are obtained from a wide range of sources including SIA partners and other HMG departments. Some of this data is publicly available, some of it is purchased, and some of it is acquired covertly in accordance with SIS statutory functions. These datasets may relate to a variety of areas of potential intelligence interest to SIS.

1.1.3 Such datasets provide information about subjects of intelligence interest ("subjects of interest"), but inevitably also include information about those who are of no direct relevance to SIS operations. It is not possible to acquire the information that will be of direct value to these operations without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.

1.1.4 SIS draws on this data and uses it in conjunction with other data in order to perform its statutory functions; for example, to identify subjects of interest, to validate intelligence or to ensure the security of operations or staff. It may also be used to facilitate the exclusion of individuals from an operation or other pursuit of intelligence requirements. This ensures that the activities of SIS are correctly and solely focused on those individuals or organisations that are relevant to the performance of their statutory functions.

1.1.5 The Secret Intelligence Agencies ('SIA') have an agreed definition of "Bulk Personal Datasets" ('BPD'):

"*any collection of information which:*

- *Comprises personal data as defined in by section 1(1) of the Data Protection Act 1998*[1]*;*
- *Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;*
- *Is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies.*

1.1.6 BPD are also too large to be manually processed (particularly given benefit is derived by using them in conjunction with other datasets);

1.1.7 The definition of 'Sensitive Personal Data' has the meaning given to it in the DPA (1998), and so covers the following:

- Religion
- Political
- Racial/Ethnic Origin

[1] Whilst DPA refers only to 'a living individual', many BPD will contain details about individuals who are dead. SIA policy and processes in relation to BPD are the same for both the living and the dead.

- Disability/Medical condition
- Sexual orientation
- Criminal Activity
- Medical information
- Journalistic information

1.1.8 Any BPD which contains 'Sensitive Personal Data', or which contains data falling within certain additional categories that SIS considers to be worthy of more detailed consideration (e.g. financial, legal protected privilege and spiritual counselling), is deemed to be a BPD containing 'particularly intrusive' data. BPD which contains 'particularly intrusive' categories of data is subject to greater scrutiny prior to authorisation for exploitation.

1.1.9 SIS's relevant directorate is responsible for the governance arrangements for BPD. It works in consultation with the operational, legal and policy directorates to understand operational requirements for BPD and ensure that BPD are subject to appropriate handling and protection throughout their lifecycle.

1.1.10 For the avoidance of doubt, these Arrangements apply to BPD under section 1(1) of ISA 1994 itself by agreement with third-party voluntary suppliers and by other non-covert access methods, and apply also to bulk personal datasets acquired by the exercise of other statutory powers.

1.1.11 These other statutory powers include, but are not limited to, those exercisable under warrants issued under section 5 of the ISA in respect of property and equipment interference; intrusive surveillance warrants issued under section 32 of the Regulation of Investigatory Powers Act 2000) ('RIPA'); directed surveillance authorisations issued under section 28 of RIPA; covert human intelligence source authorisations issued under section 29 of RIPA; warrants issued under section 8(1) or section 8(4)] of Part 1 Chapter 1 of RIPA for the interception of communications; and communications data notices or authorisations issued under Part 1 Chapter 2 of RIPA. The application of these Arrangements to bulk personal datasets acquired by exercise of these other statutory powers is without prejudice to the additional statutory requirements specified in the relevant legislation (whether section 5 of the ISA or RIPA).

1.1.12 Where the BPD in question has been obtained via a statutory regime which itself requires a particular procedure or safeguards, those procedures or safeguards will be applied in parallel to the safeguards set out in these Arrangements.

1.1.13 Oversight of the obtaining, use, retention and disclosure by the SIA of BPD is provided by the Intelligence Services Commissioner ('the IS Commissioner') pursuant to the direction given by the Prime Minister on 12 March 2015, except where the oversight of such datasets already falls within the statutory remit of the Interception of Communications Commissioner.

2.0 THE LAW

2.0.1 The ISA 1994 sets out the statutory functions of the Secret Intelligence Service. These are: obtaining and providing information relating to the actions or intentions of persons outside the British Islands; and performing other tasks relating to the actions or intentions of such persons. The ISA 1994 goes on to provide that SIS's respective statutory functions may only be exercisable (a) in the interests of national security, with particular reference to the defence and foreign policies of the UK Government, (b) in the interests of the economic well-being of the UK, or (c) in support of the prevention or detection of serious crime.

2.0.2 The information gateway provisions in sections 2(2)(a) and 4(2)(a) of the ISA 1994 impose a duty on the Head of SIS to ensure that there are arrangements for securing (i) that no information is obtained by SIS except so far as necessary for the proper discharge of its statutory functions; and (ii) that no information is disclosed except so far as necessary for those statutory functions and purposes or for the additional limited purposes set out in section 2(2)(a) of the ISA 1994 (in the interests of national security, for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings).

2.0.3 The ISA 1994 accordingly imposes specific statutory limits on the information that SIS can obtain, and on the information that SIS can disclose. These statutory limits do not simply apply to the obtaining and disclosing of information from or to other persons in the United Kingdom: they apply equally to obtaining and disclosing information from or to persons abroad.

2.0.4 Section 19 of the Counter Terrorism Act (2008) confirms that information obtained by SIS in connection with the exercise of any of its statutory functions may be used, and disclosed, by SIS in connection with the exercise of any of its other statutory functions. This means that information that is obtained by SIS for national security purposes can be disclosed to the Security Service, who may use it to support the activities of the police in the prevention and detection of serious crime.

2.1 The Human Rights Act 1998 ("the HRA")

2.1.0 SIS is a public authority for the purposes of the HRA. When acquiring, processing, retaining and disclosing BPD, SIS must therefore ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. In practice, this means that any interference with privacy must be in accordance with the law, necessary for the performance of a statutory function of SIS and proportionate to the achievement of that objective.

2.2 The Data Protection Act 2008 ("DPA")

2.2.1 SIS is a data controller in relation to all the personal data that it holds. Accordingly, when SIS processes any bulk datasets that contain personal data, it must ensure that it complies with the DPA (subject only to cases where the exemption set out under Section 28 is relied upon for the purpose of safeguarding national security).

3.0 ACQUISITION

3.0.1 [Redacted]

3.0.2 In determining whether to seek BPD, SIS is guided by the National Security Council (NSC) priorities, which in turn guide its intelligence collection priorities for the coming year.

3.0.3 [Redacted]

3.1 Before acquiring

3.1.1 SIS acquires BPD from a wide range of sources, such as SIA partners and other HMG departments.

3.1.2 The type of BPD SIS acquires varies, but broadly falls in the following categories;

- Population – these datasets provide population data or other information which could be used to help identify individuals [redacted] e.g passport details.
- Travel – these datasets contain information which enable the identification of individuals' travel activity.
- Financial – these datasets allow the identification of finance related activity of individuals.
- Communications – these datasets allow the identification of individuals where the basis of information held is primarily related to communications data e.g a telephone directory.

3.1.3 There are essentially two scenarios in which SIS acquires BPD:

- Solicited BPD: this is where a decision has been taken prior to acquisition to seek BPD of a particular type or description. [Redacted]
- Unsolicited BPD: this is where BPD are passed to SIS [redacted] without a prior request [redacted].

In either case, prior to acquisition, SIS is not in a position to know exactly what is within the BPD. At this stage, SIS must rely on the description of the data given by the source to make an assessment that it is in fact BPD and that it is likely to be necessary and proportionate for SIS to hold and/or use the BPD.

3.1.4 Whenever SIS considers acquiring a dataset the officers responsible for acquiring the BPD must consider the necessity and proportionality of doing so at the earliest possible stage.

3.1.5 What is necessary in a particular acquisition case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the necessity requirement in relation to acquisition, staff must consider why obtaining the BPD is really needed for the purpose of discharging one or more of SIS's statutory functions. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.

3.1.6 The acquiring of the BPD must also be proportionate to the purpose in question. In order to meet the 'proportionality' requirement, staff must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the data and who may be of no intelligence interest,

against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative, which involves less intrusion, that will still meet the proposed objective.

3.1.7 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or the legal advisers for guidance, or may seek guidance or a decision from the Secretary of State for Foreign & Commonwealth Affairs (SOSFCA).

3.2 [Redacted]

3.3 [Redacted]

3.4 [Redacted]

4.0 AUTHORISATION

4.1 Upon acquisition: the Authorisation process

4.1.1 Before a dataset is ingested for use by SIS, the dataset is subjected to an authorisation process. This is a means by which officers with relevant expertise and seniority are asked to consider and record the operational, policy and legal implications of holding and using the dataset. It culminates in a final decision being taken, having regard to all of those factors, by a senior SIS official.

4.1.2 The considerations are formally recorded on a proforma and circulated around a pre-determined distribution to ensure that the appropriate breadth and level of scrutiny is applied. A copy of the Authorisation Form can be found in Annex A

The stages of the Authorisation process are:

4.2 Assessment

4.2.1 A member of the appropriate team carries out an assessment of the BPD. No exploitation for operational purposes takes place at the assessment stage. In deciding whether to authorise its use consideration is given to necessity, risk assessment, data intrusiveness, actual and collateral intrusion, justification and legal considerations.

4.3 Authorisation

- Necessity Case: To be completed by the Acquiring Officer

  - Which NSC strategic intelligence priorities does this acquisition meet?
  - What results or benefits do you expect it to provide?

- Risk Assessment: To be completed by the Acquiring Officer

  - What are the risks of holding this dataset that might have potential to cause political embarrassment?

- What is the reputational damage to HMG or to SIS' operational equities should possession of this dataset become known?

- Data Intrusiveness Assessment: To be completed by the Transformation Officer

- Does the data contain UK Nationals?
- Does the dataset contain personal information or information that is particularly sensitive?
- Does the data contain minors (under 16)?

- Exploitation case: To be completed by the relevant SIS official

- Actual Intrusion: the intrusion (or interference with) privacy caused by accessing personal data as a result of analysis to identify and investigate intelligence targets;
- Collateral Intrusion: the intrusion (or interference with) privacy of individuals who are not of intelligence interest, which happens as a consequence of the analytical process.

- Justification: To be completed by the relevant SIS official

- What intelligence benefits are to be derived from the exploitation of the data?
- If it is being retained for other purposes (in particular legal or technical (see Paragraph 4.3.5))
- How will SIS make use of the data?
- Consideration of whether the continued retention and/or exploitation of the data is proportionate and necessary.
- Explanation of the analytical platforms onto which the data will be loaded and used, and an explanation of why the use of those tools is justified in necessity and proportionality terms.

- Legal consideration: To be completed by an SIS Legal Officer

- To ensure that holding the data complies with the Intelligence Services Act 1994 (ISA 1994), Data Protection Act 1998 (DPA 1998) and Human Rights Act 1998 (HRA 1998)

- [redacted]

4.3.2 No BPD can be exploited on an SIS system without a completed authorisation being in place. [Redacted]

4.3.3 The Bulk Data management team ([redacted]) are responsible for co-ordinating the authorisation process to ensure officers are aware of their responsibilities in the process.

4.3.4 SIS must ensure that all BPD are authorised for retention or use within 6 months of acquisition, save in exceptional circumstances. This period of time is necessary to ensure that the steps detailed in paragraph 4.3 can be undertaken by the Assessment Team in London. If no adequate case can be made for BPD retention or use it will be deleted immediately.

4.3.5 [Redacted]

When assessing and authorising a BPD, SIS officers must:

- **Accurately assess the contents of the dataset and start the authorisation process at the earliest possible opportunity.**
- **Consider the necessity and proportionality case for SIS to hold and exploit the data during the authorisation process.**
- **Consider the levels of collateral and actual intrusion, in SIS holding and using the data.**
- **Ensure that the authorisation process is adhered to in a compliant and efficient manner.**
- **Complete the authorisation process within 6 months of acquisition of the BPD, save in exceptional circumstances.**

5.0 USE

5.1 Access

5.1.1 The SIS database

5.1.1.1. Staff can only apply for a user account to use the SIS database if, as a result of their role, there is appropriate business need to use the tool. As part of the application process, the officer must obtain approval from their line manager and must then undertake mandatory training. Applications must be submitted with signed copies of the Security Operating Procedures (SecOps) and the Code of Practice which outlines the appropriate use of the BPD in SIS. A copy of the Code of Practice, the SecOps and the Application form are annexed (B, C and D) to this document.

5.1.1.2 [Redacted]

5.1.1.3 Access to analytical tools in SIS is linked to the post held and not the individual. If an individual moves to a new post, their access to analytical tools ceases at the time of that move. If their new post requires access, a new application will have to be submitted and the Codes of Practice and SecOps would have to be re-signed. [Redacted]

5.2 [Redacted]

5.3 [Redacted]

5.4 [Redacted]

5.5 [Redacted]

5.6 [Redacted]

6.0 TRAINING

6.0.1 Staff are required to complete mandatory training as part of the application process to access analytical tools. This training covers the requirement for providing a justification for the necessity and proportionality of conducting a search.

6.0.2 Advanced analysts complete not only mandatory training but also supplementary training which includes guidance to support them in their authorisation, transformation and analysis tasks.

6.0.3 In addition to specific mandatory training for all users of BPD analytical tools, the following courses are available (or in some cases mandatory) for SIS officers generally:

- Operational Management and Compliance courses - there is the relevant team and Legal Adviser input to ensure data and the law are fully covered.
- Legal Compliance with Data Course - online at desk course which is compulsory for SIS middle managers and above. This course reinforces the importance of necessity and proportionality and how our acquisition and exploitation works within the law.
- Legal Adviser briefings – auditorium sessions to educate and reinforce aspects of data and the law.
- The intranet provides supporting advice and guidance surrounding the acquisition, authorisation, and exploitation of bulk data. There are also policies that set out SIS's general approach to information handling and management.
- The relevant team brief SIS officers on the use and acquisition of BPD on [redacted] SIS courses [redacted]. In some cases, lawyers will also provide a brief. In addition to this all SIS staff posted overseas are briefed as part of the pre-posting process.

Before gaining access to SIS analytics officers must:

- **Be in a role that requires access to analytics and have their Line Manager's support.**
- **Have signed and understood the Code of Practice and relevant SecOps**
- **Have provided a business justification and necessity case for having access.**
- **Complete mandatory training**

7.0 DISCLOSURE

7.1 The sharing of BPD is carefully managed to ensure that disclosure only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside SIS rests with a senior SIS official.

7.2 Sharing within the SIA

7.2.1 The SIA all have a common interest in acquiring information for national security purposes, and it is both necessary and lawful for the agencies to share BPD providing certain conditions are met. Information in BPD held by SIS can only be disclosed to persons outside SIS (including to SIA partners) if the following conditions are met:

7.2.2 Disclosure must be 'necessary'. In order to meet this requirement, staff must be satisfied that disclosure of the BPD is 'really needed' for the purpose of discharging a statutory function of that Agency.

7.2.3 The disclosure of the BPD must also be proportionate to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of SIS's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal data.

7.2.4 These conditions apply equally to the disclosure of an entire BPD, a subset of the dataset, or an individual piece of data from the dataset.

7.2.5 Where these conditions are met, the BPD is formally requested from SIS through agreed sharing procedure using an applicable form. The relevant data sponsor is then responsible for submitting an applicable form (attached in Annex E) that will seek authorisation within SIS. Disclosure of the whole (or a subset) of a BPD is only permitted once this is completed. Once approved, arrangements will be made for the data to be shared with the relevant Agency.

7.3 Sharing with liaison services

7.3.1 In the event that SIS deemed it was necessary and proportionate to disclose BPD to a liaison service, the same legal disclosure tests would need to be applied as when sharing with SIA partners. As part of SIS's analysis of whether disclosure is in line with its legal obligations, in the event that SIS shares BPD with a liaison service, SIS would require any such service to agree to rigorous requirements in relation to the safeguarding of that BPD. These safeguards would cover, amongst other things, access to the BPD, use (in terms of systems as well as purpose), and onward disclosure and will be set out on handling instructions that accompany each BPD.

7.3.2 The disclosure of BPD is carefully managed by the relevant team to ensure that disclosure only occurs when it is permitted under ISA 1994 and that clear necessity and proportionally cases are evidenced. Responsibility for disclosure of BPD rests with a senior SIS official in the relevant team.

Before disclosure an SIS officer must ensure;

- **There is a legal gateway for disclosure under ISA 1994.**
- **The disclosure is assessed to be necessary and proportionate.**
- **Appropriate handling instructions are passed with each dataset.**
- **[Redacted]**

8.0 DATA RETENTION AND REVIEW

8.0.1 The Dataset Retention and Review Panel (DRR) meets every 6 months to review BPD. It is a formal process made up of a panel of members comprising senior SIS officials and legal representatives.

Representatives from MI5 and GCHQ are normally invited to attend SIS DRR to observe and contribute to discussion.

8.0.2 The aim of the panel is to ensure that BPD are only retained by SIS where necessary and proportionate to enable SIS to carry out its statutory functions. When a dataset is authorised for retention, it will be given a retention period in accordance with the level of intrusion posed by the retention and use of the dataset. This retention period determines the frequency with which the dataset is reviewed by the DRR. On review, DRR members must satisfy themselves that the levels of intrusion are justifiable under SIS's governing legislation (including Article 8(2) ECHR 1998 and the DPA 1998). If it is judged (at any time, but including on review) that it is no longer necessary and proportionate to retain a dataset, it will be deleted.

8.0.3 When considering the necessity and proportionality of retaining a dataset, the Panel considers:

- Use of the dataset, including action taken by SIS as a result of use.
- The level of actual and collateral intrusion posed by retention and exploitation
- Potential corporate, legal, reputational and political risk.
- Frequency of acquisition and updates
- Whether such information could be acquired elsewhere through less intrusive means.
- The operational and legal justification for continued retention, including its necessity and proportionality.
- Frequency of review of retention
- Whether any caveats or restrictions should be applied.

8.0.4 The Panel considers [redacted] recommendations for each dataset and decides whether to retain the dataset [redacted]. In particularly sensitive cases, the Panel may recommend an earlier review.

8.0.5 [Redacted]

8.0.6 If the decision is taken to remove data from an analytical platform or to delete it completely from SIS systems, these actions would be undertaken by the relevant team as they are the only officers with the appropriate access rights and technical knowledge, to carry this out.

8.0.7 The DRR panel report is formally recorded and passed to a senior SIS official who can raise relevant points to the SIS Executive Committee or SIS Board as necessary. A summarised version of the report and a list of SIS BPD holdings are also made available for the SoSFCA.

The Data Retention and Review Panel must:

- **Review BPD holdings to ensure that retention and use remains necessary and proportionate for SIS to carry out its statutory duties.**
- **Delete BPD holdings after the decision is made that it is no longer necessary or proportionate to hold the data.**

9.0 OVERSIGHT

9.1 SIS Audit of use

9.1.1 All uses of SIS's database are audited by SIS's audit team.

9.1.2 [Redacted]

9.1.3 [Redacted]

9.1.4 All audit investigations are available to the Commissioner for scrutiny. Audit is vital to ensure users are not abusing their access to BPD.

9.1.5 [Redacted] All analysts, if selected, would be expected to justify their searches in front of the IS Commissioner.

9.2 Ministerial Oversight

9.2.1 SIS does not routinely seek Ministerial approval for the acquisition or use of BPD. However, in acquisition operations where there is a risk that a particular activity could either cause significant embarrassment to HMG, or would conflict with or prejudice the policies of HMG, SIS would seek political clearance before proceeding. A submission seeking political clearance from SoSFCA would also give detail on the dataset which SIS was trying to acquire. In the last year the relevant team has sought clearance on one occasion.

9.3 External Oversight

9.3.1 Oversight of BPD is provided by the IS Commissioner pursuant to the direction given by the Prime Minister on 12 March 2015. The IS Commissioner scrutinises SIS's authorisations and use of BPD, including the audit of BPD, and makes twice yearly scrutiny visits to DX.

9.3.2 The purpose of the IS Commissioner's oversight is to review and test SIS judgements on the necessity and proportionality of acquiring and using BPD and to ensure that SIS policies and procedures for the control of, and access to, these datasets is both sound and strictly observed. SIS aims for the IS Commissioner to be able to report positively to the Prime Minister on its arrangements for working with and handling of BPD.

9.3.3 All papers requested by the IS Commissioner must be made available to him. Those papers include, but are not limited to the following;

- Selected Data Authorisations
- Selected Audit challenges
- All Audits challenges which require further investigation (i.e. potential audits resulting from the misuse of BPD)
- A list of current datasets available for exploitation in SIS
- The minutes of the previous Data Retention Review
- Papers outlining any changes to current BPD policies

9.3.4 [Redacted]