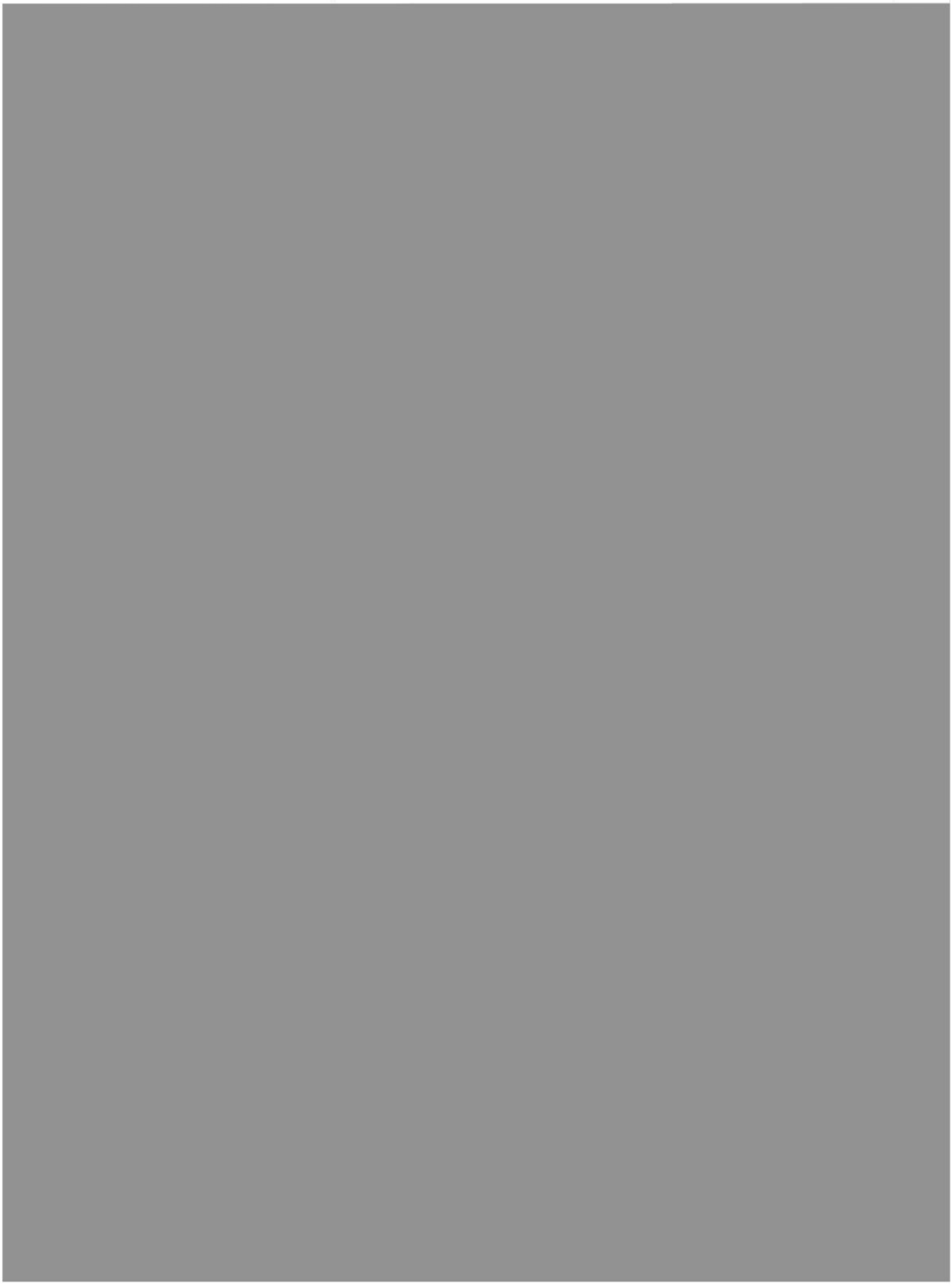

2.3 For these purposes, '*personal data*' has the meaning given to it in section 1(1) of the Data Protection Act 1998, which defines '*personal data*' as follows:

'data which relate to a living[1] individual who can be identified –

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of the data controller [*i.e. in this case, the relevant Intelligence Service*), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

interception of communications. The application of these Arrangements to bulk personal datasets obtained by exercise of these other statutory powers is without prejudice to any additional applicable statutory requirements specified in the relevant legislation.

2.10 Oversight of the obtaining, use, retention and disclosure by the Intelligence Services of bulk personal datasets is provided by the Intelligence Services Commissioner pursuant to the direction given by the Prime Minister on 12 March 2015, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner (as is the case, for example, in relation to bulk personal datasets acquired by the interception of communications pursuant to Part 1 Chapter 1 of RIPA and where the bulk personal data continues to be identifiable as the product of interception).

3.0 The law

3.1 The SSA 1989, the ISA 1994 and the Counter-Terrorism Act 2008 ("the CTA")

3.1.2 The SSA 1989 provides that the functions of the Security Service are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime.

3.1.3 The ISA 1994 sets out the functions of the Secret Intelligence Service and GCHQ. In the case of SIS 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. In the case of GCHQ these are: monitoring or interfering with communications and related equipment; and providing advice on information security and languages. The ISA 1994 goes on to provide that their respective functions (with the exception of GCHQ's information security and language 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.

3.1.4 The information gateway provisions in section 2(2)(a) of the SSA 1989 and sections 2(2)(a) and 4(2)(a) of the ISA 1994 impose a duty on the Heads of the respective Agencies to ensure that there are arrangements for securing (i) that no information is obtained by the relevant Agency except so far as necessary for the proper discharge of its functions; and (ii) that no information is disclosed except so far as is necessary for those 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), section 4(2)(a) of the ISA 1994 (for the purpose of any criminal proceedings) and section 2(2)(a) of the SSA 1989 (for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).

3.1.5 The SSA 1989 and the ISA 1994 accordingly impose specific statutory limits on the information that each of the Intelligence Services can obtain, and on the information that each 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.

3.1.6 Section 19 of the CTA confirms that '*any person*' may disclose information to the Agencies for the exercise of their respective functions, and disapplies any duty of confidence (or any other restriction, however imposed) which might otherwise prevent this. It further confirms that information obtained by any of the Intelligence Services in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its other functions. For example, information that is obtained by the Security Service for national security purposes can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime.

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

3.2.1 Each of the Intelligence Services is a public authority for the purposes of the HRA. When obtaining, using, retaining and disclosing bulk personal datasets, the Intelligence Services must therefore (among other things) 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 both necessary for the performance of a statutory function of the relevant Intelligence Service and proportionate to the achievement of that objective.

3.3 The Data Protection Act 1998 ("the DPA")

3.3.1 Each of the Intelligence Services is a data controller in relation to all the personal data that it holds. Accordingly, when the Intelligence Services use any bulk data that contain personal data, they must ensure that they comply with the DPA (subject only to cases where exemption under section 28 is required for the purpose of safeguarding national security).

4.0 Authorisation and Acquisition

4.1 Each of the Intelligence Services must put in place and maintain procedures, to ensure that staff comply with the SSA 1989 and the ISA 1994, the DPA and the HRA.

4.2 Before obtaining a bulk personal dataset, based on the information available to them at the time, staff should always:

- be satisfied that the objective in question falls within the Service's statutory functions;
- be satisfied that it is **necessary** to obtain and retain the information concerned in order to achieve the objective;
- be satisfied that obtaining and retaining the information in question is **proportionate** to the objective;
- be satisfied that only as much information will be obtained as is necessary to achieve that objective.

When will acquisition be "necessary"?

4.3 What is **necessary** in a particular 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 and retention, staff must consider why obtaining the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of the relevant Intelligence Service. 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.

The obtaining must also be "proportionate"

4.4 The obtaining and retention of the bulk personal dataset 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 that will still meet the proposed objective - i.e. which involves less intrusion.

4.5 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or legal advisers for guidance, and may seek guidance or a decision from the relevant Secretary of State.

4.6 Before a new dataset is loaded into an analytical system for use, staff in each Intelligence Service must consider the factors set out in paragraph 4.2 based on the information available to it at the time. Each Agency has a rigorous formal internal authorisation procedure which must be complied with, except in those cases where the acquisition is already authorised by a warrant or other legal authorisation issued by a Secretary of State.

4.7 Staff in each Intelligence Service must always complete the formal internal authorisation procedure before the dataset is loaded into an analytical system for use. The authorisation procedure involves an application to a senior manager designated for the purpose which is required to set out the following:

- a description of the requested dataset, including details of the personal data requested, and any sensitive personal data;
- the operational and legal justification for acquisition and retention, including the purpose for which the dataset is required and the necessity and proportionality of the acquisition;
- an assessment of the level of intrusion into privacy;
- the extent of political, corporate, or reputational risk;

4.8 The relevant Intelligence Service's legal advisers must be consulted on all new BPD acquisitions and have confirmed the legality of the acquisition and its continued retention before authorisation to use the dataset is given.

4.9 Once authorised, the completed application must be stored on a central record by the appropriate Intelligence Service's information governance/compliance team, which will include the date of approval. This record must also contain the date of acquisition of the relevant data, which should be the date used for the review process (*for which see paragraph 7.1-7.5 below*).

When seeking authorisation for acquisition of a BPD, staff must satisfy themselves as to, and explain in their application for authorisation:

- **The reasons why is it necessary to acquire and retain the data,**

including in particular what intelligence aim is likely to be met and how the data will support that objective.

- **The proportionality of acquiring and retaining the data, including in particular whether there is a less intrusive method of obtaining the data.**

When seeking authorisation to load a BPD into an analytical system for use, staff must satisfy themselves as to, and explain:

- **The purpose for which the BPD is required; and**
- **The necessity and proportionality of using the BPD.**

5.0 Specific Procedures and Safeguards for Use of and Access to Bulk Personal Datasets inside each Intelligence Service

5.1 Each Intelligence Service attaches the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. In particular, each Intelligence Service must apply the following protective security measures:

- Physical security to protect any premises where the information may be accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

5.2 In relation to information in bulk personal datasets held, each Intelligence Service is obliged to put in place the following additional measures:

- Access to the information contained within the bulk personal datasets must be strictly limited to those with an appropriate business requirement to use these data;
- Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service;
- If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, they must only access the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Service, or for the additional limited purposes described in paragraph 3.1.4 above;
- Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate (as described in paragraphs 4.4 above and 6.3 below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;

- Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;

- A range of audit functions must be put in place: users should be made aware that their access to bulk personal datasets will be monitored and that they must always be able to justify their activity on the systems;

- Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified; and

- Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution.

5.3 The Intelligence Services also take the following measures to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets:

- Data containing sensitive personal data (as defined in section 2 of the DPA) may be subject to further restrictions, including sensitive data fields not being acquired, sensitive fields being acquired but suppressed or deleted, or additional justification required to access sensitive data fields. In addition, the Intelligence Services may expand the list of sensitive data fields beyond those provided for in section 2 of the DPA to provide additional protection where appropriate.

- Working practice seeks to minimise the number of results which are presented to analysts by framing queries in a proportionate way, although this varies in practice depending on the nature of the analytical query;

- If necessary, the Intelligence Services can - and will - limit access to specific data to a very limited number of analysts.

Each Intelligence Service must:

- **Establish procedures to ensure that the integrity and confidentiality of the information in BPDs is protected, including through: physical security for premises, IT security and a vetting regime for staff.**

- **Maintain measures so that only staff with an appropriate business requirement are able to access/use information in BPDs.**

- **Ensure staff are appropriately trained; that audit functions are in place; that staff are aware their access will be monitored; and are warned of disciplinary procedures resulting from misuse.**

Before accessing information in a BPD, staff must be satisfied:

- **That it is necessary to do so for the performance of the Intelligence Service's functions.**

- **That it is proportionate to do so, including whether other less intrusive methods could be used to achieve the desired outcome.**

6.0 Procedures and Safeguards for Disclosure of Bulk Personal Datasets outside the relevant Intelligence Service

6.1 Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:

- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective;
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

When will disclosure be necessary?

6.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.

The disclosure must also be "proportionate"

6.3 The disclosure of the bulk personal dataset 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 the Intelligence Service'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 dataset.

6.4 Before disclosing any bulk personal data, staff must take reasonable steps to ensure that the intended recipient organisation has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled, or that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

6.5 These conditions must be met for all disclosure, including between the Intelligence Services.

6.6 These conditions for disclosure apply equally to the disclosure of an entire bulk personal dataset, a subset of the dataset, or an individual piece of data from the dataset.

6.7 Disclosure of **the whole (or a subset) of a bulk personal dataset** is subject to internal authorisation procedures in addition to those that apply to an item of data. The authorisation process requires an application to a senior manager designated for the purpose, describing the dataset it is proposed to disclose (in whole or in part) and setting out the operational and legal justification for the proposed disclosure along with the other information specified in paragraph 4.7, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so that the senior manager can then consider the factors in paragraph 6.1, with operational, legal and

policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State.

When seeking to disclose the whole (or a subset) of a BPD, staff must be satisfied that disclosure is:

- **Justified on the basis of the relevant statutory disclosure gateway.**
- **Determined to be necessary and proportionate to the objective.**
- **Limited to only as much information as will achieve the objective.**
- **Authorised by a senior manager or, in difficult case, the Secretary of State.**

7.0 Review of Retention and Deletion

7.1 Each Intelligence Service must regularly review the operational and legal justification for its **continued retention and use** of each bulk personal dataset. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Intelligence Service must be deleted or destroyed.

7.2 The retention and review process requires consideration of the following factors:

- The operational and legal justification for continued retention, including its necessity and proportionality;
- Whether such information could be obtained elsewhere through less intrusive means;
- An assessment of the value and examples of use;
- Frequency of acquisition;
- The level of intrusion into privacy;
- The extent of political, corporate, or reputational risk;
- Whether any caveats or restrictions should be applied to continued retention.

For the purposes of retention, review and deletion of BPD-sets, each Intelligence Service must:

- **Regularly review the justification for continued retention and use, including its necessity and proportionality.**
- **Delete a BPD after a decision is made that retention or use of it is no longer necessary or proportionate.**

8.0 Other management controls within the Intelligence Services

8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose function is to ensure that each bulk personal dataset has been properly acquired, that any disclosure is properly justified, that its retention remains necessary for the proper

discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective.

8.2 The Review Panel in each Intelligence Service meets at six-monthly intervals and are comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

8.3 Use of bulk personal data by staff is monitored by the relevant audit team in each Intelligence Service in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution.

8.4 All reports on audit investigations are made available to the Intelligence Services Commissioner for scrutiny (see paragraph 10 below).

8.5 Staff within each Intelligence Service will keep their senior leadership (at Director level or above) apprised as appropriate of the relevant Service's bulk personal data holdings and operations.

For the purposes of management control:

- **A Review Panel in each Intelligence Service must meet at six- monthly intervals to review that Intelligence Service's BPD holdings.**
- **Staff must keep senior leadership (Director level or above) apprised of BPD holdings and operations.**

9.0 Ministerial Oversight

9.1 Each Intelligence Service will report as appropriate on its bulk personal data holdings and operations to the relevant Secretary of State (the Home Secretary in the case of the Security Service, and the Foreign Secretary in the case of SIS and GCHQ).

10.0 Oversight by the Intelligence Services Commissioner

10.1 The acquisition, use, retention and disclosure of bulk personal datasets by the Intelligence Services, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.

Note: The Prime Minister's section 59A RIPA direction was issued on 11 March 2015. Paragraph 3 of this makes it clear that the Commissioner's oversight extends not only to the practical operation of the Arrangements, but also to the adequacy of the Arrangements themselves.

10.2 The Intelligence Services must ensure that they can demonstrate to the appropriate Commissioner that proper judgements have been made on the necessity

and proportionality of acquisition, use, disclosure and retention of bulk personal datasets. In particular, the Intelligence Services should ensure that they can establish to the satisfaction of the appropriate Commissioner that their policies and procedures in this area (a) are sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements.

10.3 The Intelligence Services Commissioner also has oversight of controls to prevent and detect misuse of bulk personal data, as outlined in paragraph 8.3 and 8.4 above.

10.4 The Intelligence Services must provide to the appropriate Commissioner all such documents and information as the latter may require for the purpose of enabling him to exercise the oversight described in paragraph 10.1 and 10.2 above.

For the purposes of oversight by Ministers and the Intelligence Services Commissioner, each Intelligence Service must:

- **Report on its BPD holdings to the relevant Secretary of State.**
- **Make available to the Commissioner all reports on audit investigations.**
- **Be able to demonstrate to the Commissioner that proper judgements have been made as to the necessity and proportionality of the acquisition, disclosure and retention of BPDs.**

Published: 4th November 2015