



Home Office

# Security and Intelligence Agencies' retention and use of bulk personal datasets

## Draft Code of Practice

[Autumn] 2016

DRAFT

# **Security and Intelligence Agencies' retention and use of bulk personal datasets**

DRAFT Code of Practice

Pursuant to section 219 and Schedule 7 to the Investigatory Powers Act 2016

[Autumn] 2016

DRAFT

# Contents

1	Introduction	5
2	Scope and definitions	6
	Different statutory routes by which BPDs may be acquired	8
3	BPDs – general rules	9
	Requirement for authorisation by warrant	9
	Types of warrant that may be issued	9
	Exception to general requirement for authorisation by warrant	9
4	BPD warrant applications	11
	Applications for class BPD warrants	11
	Class BPD warrants	12
	Restriction on use of class BPD warrants	12
	Applications for specific BPD warrants	13
	Intrusiveness of data	14
	Confidential information relating to members of sensitive professions	15
5	Authorisation of class and specific BPD warrants by a Secretary of State	17
	Necessity and proportionality	20
	When will retaining or examining a BPD be necessary?	20
	When will retaining or examining a BPD be proportionate?	20
	Authorisation of a specific warrant: senior officials	21
	Approval of the issue of BPD warrants by a Judicial Commissioner	21
	Urgent authorisations	22
	Duration of BPD warrants	24
	Modification of a BPD warrant	24
	Urgent modification of a BPD warrant	25
	Renewal of BPD warrants	25
	Cancellation of warrant	26
	Non-renewal or cancellation of class BPD warrants	27
6	Authorisation of the retention and use of BPDs falling within a class BPD warrant	29
7	Safeguards	31
	Storage	31
	Safeguards before a BPD is made accessible	31
	Access and examination	32
	Personnel security	33
	Additional access safeguards for confidential information relating to sensitive professions	33
	Review of retention and deletion	35
	Destruction	36

Other management controls	36
8 Record-keeping and error-reporting	38
9 Oversight	41
10 Complaints	43
11 Annex A	44
The Security Service Act 1989 and the Intelligence Services Act 1994	44
The Counter-Terrorism Act 2008	45
The Human Rights Act 1998	45
The Data Protection Act 1998	45
12 Annex B	47
13 Annex C	
BPD warrant applications	48
Safeguards	55

DRAFT

# 1 Introduction

- 1.1 This code of practice relates to the powers and duties conferred or imposed under Part 7 of the Investigatory Powers Act [2016] (“the Act”). It provides guidance on the procedures that must be followed before bulk personal datasets can be retained and examined by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (“the Security and Intelligence Agencies”). This code of practice is intended for use by the Security and Intelligence Agencies.
- 1.2 The Act provides that all codes of practice issued under Schedule 6 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, it must be taken into account.
- 1.3 For the avoidance of doubt, the guidance in this code takes precedence over any Security and Intelligence Agency’s internal advice or guidance.

DRAFT

## 2 Scope and definitions

- 2.1 The Security and Intelligence Agencies need to collect a range of information from a variety of sources to meet the requirements of their statutory functions. They do this in accordance with section 2(2)(a) of the Security Service Act 1989 (SSA) and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 (ISA) (“the information gateway provisions” – see paragraph 11.1 and subsequent paragraphs of Annex A) and through the exercise of various existing statutory powers (see further at paragraph 2.11 and subsequent paragraphs).
- 2.2 Among the range of information collected are bulk personal datasets (“BPDs”). For the purposes of the Act and this Code, a set of data that has been obtained by a Security and Intelligence agency comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.
- 2.3 Section 183 of the Act specifies that a Security and Intelligence Agency “retains” a BPD for the purposes of the Act if, after any initial examination of the contents, it retains a BPD for the purpose of the exercise of its functions and it holds the BPD electronically for analysis in the exercise of those functions.
- 2.4 As section 201 makes clear, the initial examination enables the Security and Intelligence Agency, when it comes into possession of a BPD, to carry out a preliminary examination of the contents with a view to establishing whether it is a BPD, and whether that BPD is of a nature that the Security and Intelligence Agency would wish to retain and/or examine it. If so, the Security and Intelligence Agency will consider whether in the light of the dataset’s potential intelligence or investigative value, it would be necessary and proportionate to retain the dataset for the purposes of analysis in the exercise of its statutory functions. If it concludes that it would be necessary and proportionate to retain the dataset for these purposes, that retention must be authorised by a BPD warrant. If the dataset is not covered by an existing class BPD warrant, the Security and Intelligence Agency must apply for a specific BPD warrant as soon as reasonably practicable after reaching that conclusion. (See chapters 3 and 4 for further details on these two types of BPD warrant.)
- 2.5 This initial examination may only be carried out by a Security and Intelligence Agency for these limited purposes, and not for the purposes of any intelligence investigations or operations.
- 2.6 A Security and Intelligence Agency should complete this initial examination as soon as reasonably practicable. What is ‘reasonably practicable’ will depend on many different factors. In cases where the Security and Intelligence Agency comes into possession of a BPD which has been created outside of

the UK, there may be a period of time before the Security and Intelligence Agency is in a position to properly assess the data for the purpose of determining whether it wishes to retain or use the BPD (and to apply for a specific warrant, if required). For example, the BPD may need to be brought back to the UK from overseas; the BPD may be in a foreign language; and/or the BPD may be part of a much larger set of data from which it needs to be separated.

- 2.7 In the light of these considerations, section 201(4) specifies that in cases of BPD created outside of the UK, the acquiring Security and Intelligence Agency has six months from the date on which the head of the intelligence Agency believes a BPD has – or may have been - obtained to conduct the initial examination and, where required, to apply for a specific BPD warrant. Where the BPD is created in the UK, the acquiring Security and Intelligence Agency has three months from the date on which the head of the intelligence services believes that a BPD has – or may have been – obtained to conduct the initial examination and where required apply for a specific BPD warrant.
- 2.8 Section 201(5) makes it clear that a Security and Intelligence Agency is not in breach of the requirement for a warrant to retain BPD for the period between deciding (as part of the initial examination) that it wants to retain a BPD and the determination of the Security and Intelligence Agency’s application for a specific BPD warrant for that BPD. This allows a Security and Intelligence Agency which has received a BPD that falls outside an existing class BPD warrant to retain the dataset while going through the process of obtaining the necessary specific warrant. This is most likely to occur where a BPD is unsolicited (i.e. one which the recipient Security and Intelligence Agency has not requested or sought to obtain), because a Security and Intelligence Agency will not have had the opportunity to assess whether the BPD is covered by a class warrant. However, it could also arise where a solicited BPD is received which contains unexpected material. In such circumstances, the relevant Security and Intelligence Agency should complete its initial examination of the BPD and apply for a specific warrant within the timeframes referred to in section 201(4) (and described in paragraph 2.7 above). Pending issue of the specific warrant, the Security and Intelligence Agency may not examine the BPD for the purposes of any intelligence investigations or operations.
- 2.9 For the purposes of the Act, ‘personal data’ has the meaning given to it in section 1(1) of the Data Protection Act 1998 (“DPA” – see also paragraph 11.7 and subsequent paragraphs of Annex A), which defines ‘personal data’ as follows:
- ‘data which relate to a living 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 Security and Intelligence Agency), 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’.

- 2.10 While the DPA refers to a ‘living individual’, bulk personal datasets may contain details about individuals who are dead. In the case of some BPDs there may be no indication whether the individuals referred to in the dataset are deceased or not. For example, the electoral roll will inevitably include individuals who are deceased, given that it is not continuously updated: such a dataset would require a warrant under the Act if it had been retained electronically for analysis by a Security and Intelligence Agency in the exercise of its statutory functions. If a BPD contains information about individuals who are known to be deceased, the relevant Security and Intelligence Agency may only decide to retain the dataset if it considers that it would be necessary and proportionate to do so for the purposes of its statutory functions.

## Different statutory routes by which BPDs may be acquired

- 2.11 This code of practice applies not only to BPDs obtained under the information gateway provisions themselves (section 2(2)(a) of SSA and sections 2(2)(a) and 4(2)(a) of ISA), but also to BPDs where the mechanism for obtaining the datasets is subject to authorisation through the exercise of other statutory powers.
- 2.12 These other statutory powers include, but are not limited to, those exercisable under warrants issued under section 5 of ISA in respect of property interference otherwise than for the purpose of facilitating the obtaining of communications, equipment data or other information; 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; and covert human intelligence source authorisations issued under section 29 of RIPA. The application of this code of practice to BPDs obtained by exercise of the statutory powers listed above is without prejudice to any additional requirements specified in the legislation relevant to those statutory powers.
- 2.13 For the avoidance of doubt, this code of practice does not apply to BPDs obtained by a Security and Intelligence Agency when it is exercising a power under a warrant or other authorisation issued or given under the Investigatory Powers Act [2016], for example, under a targeted or bulk interception or equipment interference warrant or under a bulk acquisition warrant (for bulk communications data). BPDs acquired under such other Investigatory Powers Act powers will be subject to the applicable regime under the relevant part of the Act (see also paragraph 3.3 below). This is unless the Security and Intelligence Agency successfully applies to the Secretary of State to give a direction, with Judicial Commissioner approval, to disapply that regime in order to apply the Part 7 regime – see section 203 and paragraph 3.4 below. Once under the Part 7 regime, the provisions of this code of practice will apply.



## 3 BPDs – general rules

### Requirement for authorisation by warrant

- 3.1 The Act does not create any new power to obtain BPDs. Rather it requires that the retention and use of BPDs must be subject to an authorisation scheme and a comprehensive set of robust and transparent safeguards. Specifically, section 184 of the Act provides that a Security and Intelligence Agency may not exercise a power for the purpose of retaining or examining a BPD unless this is authorised by the issue of a warrant under Part 7 of the Act.

### Types of warrant that may be issued

- 3.2 Section 184(3) describes the two types of warrant provided for by Part 7: a '**class BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, BPDs that fall within a class described in the warrant; and a '**specific BPD warrant**' authorising a Security and Intelligence Agency to retain, or to retain and examine, the particular BPD described in the warrant.

### Exception to general requirement for authorisation by warrant

- 3.3 Section 185 explains the specific circumstances in which the general requirement under section 184 for a BPD warrant does not apply. Section 185(1) provides that the Part 7 authorisation scheme does not apply to BPD when this is obtained by a Security and Intelligence Agency by the exercise of **other** powers under the Act, for example, under a targeted or bulk interception or equipment interference warrant. An example of this might be where an email had been intercepted and a BPD was attached to the email. In such cases, the retention and examination of the BPD will be governed by the applicable regime under the relevant part of the Act – for example, the interception regime where a BPD is acquired as a result of interception.
- 3.4 However, under section 203, a Security and Intelligence Agency can apply to the Secretary of State for a direction that a BPD retained by it under a targeted or bulk interception or equipment interference warrant should have the provisions relating to that other power disapplied, and the provisions of Part 7 of the Act applied instead. Such a direction can only be given with the approval of a Judicial Commissioner. Such a direction can also be varied by the Secretary of State, but again only with the approval of the Judicial Commissioner. Where an application for a direction under section 203 is made by the head of a Security and Intelligence Agency, consideration should also be given to whether an application for a specific warrant should be made

at the same time. An application for a specific warrant should be made if the nature of the BPD which is subject to the direction is BPD that would require a specific warrant under Part 7. Under section 203(12), the Secretary of State may issue a specific warrant at the same time as giving a direction under this section.

- 3.5 In issuing any direction, the Secretary of State is permitted to provide that any of the associated regulatory provisions which applied to the regime under which the BPD was obtained, should continue to apply once the direction has been issued (with or without modifications). Therefore, in making an application for a direction, a Security and Intelligence Agency should consider which, if any, of the associated regulatory provisions it considers should – or should not – apply to the BPD, if the direction is issued.
- 3.6 In the case of a BPD obtained by interception which identifies itself as the product of interception, such a direction may not disapply the provisions in section 53 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act proceedings (see section 203(6)(a)). Nor may such a direction disapply sections 54-56 of the Act, which impose further restrictions on the disclosure of such material and make it an offence to make an unauthorised disclosure of the existence of an intercept warrant or any intercepted material (see section 203(6)(b)).
- 3.7 Section 185(2) makes it clear that a BPD can be retained or examined to enable the information contained in it to be destroyed. This provision allows the Security and Intelligence Agencies to hold, temporarily, a BPD which is no longer authorised by a warrant for the purpose only of ensuring that the relevant data is removed from their systems. If a warrant is cancelled or an application for a specific warrant is not approved, it will not always be possible for the Security and Intelligence Agency to delete the BPD immediately from its analytical systems. This is for two reasons. First, as the data has been ingested into wider analytical systems, it may take some time to delete the data – e.g. because the system must be taken off-line and/or because of the need for checks to ensure the correct data is deleted. Secondly, it may be that in some cases only part of a BPD is required to be deleted. This will, as a result, require examination of the dataset first to enable deletion.
- 3.8 Section 185(3) makes clear that other sections of Part 7 of the Act also provide for exceptions from the requirement to obtain a warrant in particular circumstances. These relate to cases where the Judicial Commissioner has failed to approve an urgent specific BPD warrant but has imposed conditions as to the use or retention of the BPD (section 192(3)(b) – see paragraph 5.34 below); to a time-limited period in which an Agency is conducting an initial examination of a potential BPD (section 201(5) – see paragraph 2.3 above and subsequent paragraphs); and to a limited period after the non-renewal or cancellation of a warrant (section 200(6) – see paragraph 5.59 and subsequent paragraphs).

## 4 BPD warrant applications

- 4.1 An application for a BPD warrant is made to the Secretary of State. The requirements set out in Part 7 of the Act only relate to the Security and Intelligence Agencies. An application for a BPD warrant therefore may only be made by or on behalf of the following persons:
- The Director General of the Security Service.
  - The Chief of the Secret Intelligence Service.
  - The Director of the Government Communications Headquarters (GCHQ).
- 4.2 All BPD warrants are issued by the Secretary of State. No BPD warrant may be issued unless and until it has been approved by a Judicial Commissioner (see paragraph 5.26 and subsequent paragraphs).
- 4.3 The only exception to this is a case where the Secretary of State considers that there is an urgent need to issue a specific warrant (see paragraph 5.30 and subsequent paragraphs). Even where the urgency procedure is followed, the Secretary of State still must personally authorise the warrant. In any case where the Secretary of State decides to issue a specific warrant (whether under the urgent procedure or otherwise), he or she must personally sign the warrant where reasonably practicable. However, a designated senior official can sign the warrant if it is not reasonably practicable for the Secretary of State to sign it. When a BPD warrant is issued, it is addressed to the person who submitted the application (or on whose behalf it was submitted).
- 4.4 Prior to submission, each application should be subject to a review within the Security and Intelligence Agency making the application. This involves consideration as to whether the application is for a purpose falling within sections 187(3)(a)(i) or 188(6)(a)(i) (in the interests of national security), 187(3)(a)(ii) or 188(6)(a)(ii) (for the purpose of preventing or detecting serious crime) or 187(3)(a)(iii) or 188(6)(a)(iii) (in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security). The consideration of the application should also include whether the retention, or the retention and examination, of the BPD is both necessary and proportionate and whether the examination of the BPD is necessary for the operational purposes specified in the application (on which see paragraph 5.7 and subsequent paragraphs). There may be circumstances in which a Security and Intelligence Agency may consider it appropriate to apply for a warrant to retain a BPD before it has physically acquired that BPD.

### Applications for class BPD warrants

- 4.5 Section 187 of the Act explains how the class BPD warrant authorisation process works. It specifies that an application for a class warrant must include:
- a description of the class of BPD to which the application relates; and

- if the Security and Intelligence Agency wishes to examine BPDs of that class, an explanation of the “operational purposes” for which the relevant Security and Intelligence Agency wishes to examine BPDs falling within that class.

## Class BPD warrants

- 4.6 Class BPD warrants are for those datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity, and the proportionality of using the data. This allows the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class: a class warrant might, for example, authorise a Security and Intelligence Agency to acquire travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.
- 4.7 Before submitting an application for a class warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:
- retention of BPDs within the class specified in the warrant is **necessary** for one or more of the purposes specified in section 187 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
  - examination of BPDs within that class is **necessary** for one or more of the operational purposes to be specified in the class warrant and for one or more of the statutory purposes specified in section 187 of the Act; and
  - examining and retaining BPDs within that class in question is **proportionate** to the functions and purposes referred to in (a) and (b) above; only as much information will be obtained as is necessary to achieve those functions and purposes; and there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.
- 4.8 Section 187(4) makes clear that the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

## Restriction on use of class BPD warrants

- 4.9 Section 186 provides that a Security and Intelligence Agency may not retain, or retain and examine, a BPD in reliance on a class BPD warrant if the Head of the Agency considers (a) that the BPD consists of, or includes, **health records**, or (b) that a substantial proportion of the BPD consists of **sensitive personal data**, or (c) that the nature of the BPD, or the circumstances in which it was created, is or are such that its retention, or retention and examination, raises **novel or contentious issues** which ought to be

considered by the Secretary of State and a Judicial Commissioner on an application by the Head of the Agency for a specific BPD warrant.

- 4.10 'Health record' is defined by section 189(6) to mean a record, or a copy of a record, which (a) consists of information relating to the physical or mental health of an individual, (b) was made by or on behalf of a health professional in connection with the care of that individual, and (c) was obtained by the Security and Intelligence Agency from a health professional or a health service body [or from a person acting on behalf of a health professional or health service body in relation to the record or the copy]. 'Sensitive personal data' is as defined in section 2 of the Data Protection Act 1998: see paragraph 11.8 of Annex A below.

## Applications for specific BPD warrants

- 4.11 Section 188 provides for two sets of circumstances in which a Security and Intelligence Agency may apply to the Secretary of State for a specific BPD warrant. A specific warrant is a warrant for one specific BPD rather than a warrant for a class of BPDs. If either of these two circumstances apply, the relevant Security and Intelligence Agency should consider whether to make an application for a specific warrant.
- 4.12 In the 'Case 1' scenario, the dataset does not fall within the scope of an existing class BPD warrant.
- 4.13 In the 'Case 2' scenario, the dataset falls within a class of BPD authorised by an existing class warrant, but either (i) the Security and Intelligence Agency is prevented by section 186 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraphs 4.9 and 4.10 above) or (ii) the relevant Security and Intelligence Agency nevertheless considers that it would be appropriate to seek a specific BPD warrant. Examples of the sort of situation where an Security and Intelligence Agency should seek a specific warrant are as follows (with the first two bullets reflecting the provisions of section 186):
- where the dataset consists of, or includes, **health records**; or includes a substantial proportion of **sensitive personal data**; .or
  - the nature of the dataset, or the circumstances in which it was created, raise **novel or contentious** issues. An example of this could be where the nature of the BPD is such that its retention, or retention and examination, could raise international relations concerns, which the Agency believes it would be appropriate for the Secretary of State and Judicial Commissioner to consider on an application for a specific warrant.
  - The BPD has been assessed by the Security and Intelligence Agency as being relatively more intrusive, such assessment having been carried out in accordance with paragraph 4.17 and subsequent paragraphs.

- The dataset contains confidential information relating to members of sensitive professions. A 'sensitive profession' for these purposes includes lawyers, doctors, journalists, Members of Parliament and Ministers of religion. (References to a Member of Parliament include references to a Member of the UK Parliament, the Scottish Parliament, the Welsh Assembly, the Northern Ireland Assembly and a UK Member of the European Parliament.) (See paragraph 4.19 and subsequent paragraphs.)
- 4.14 Where section 186 applies, the Security and Intelligence Agency is required by section 188 to include in its application for a specific BPD warrant an explanation of why it is prevented from retaining, or retaining and examining, the BPD in reliance on a class warrant, i.e. it must explain whether this is because the dataset consists of, or includes, health records, or because it includes a substantial proportion of sensitive personal data, or because it raises novel or contentious issues. This should not simply refer back to the statute: it should provide a more detailed explanation of the nature and extent of the material in question, to aid the Secretary of State's understanding of the dataset and the warrant application.
- 4.15 In the case of a dataset which includes a substantial proportion of sensitive personal data, in its application for the specific BPD warrant the Agency should describe the nature and extent of sensitive personal data in the dataset, where possible by reference to the different categories of sensitive data set out in section 2(a)-(f) of the Data Protection Act 1998 (see paragraph 11.8 in Annex A).
- 4.16 If required in an individual case, the Security and Intelligence Agency can seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner on whether it would be appropriate for a specific BPD warrant to be sought. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

## Intrusiveness of data

- 4.17 When considering whether to retain and examine a BPD, the Security and Intelligence Agencies will assess the degree or extent of the intrusiveness which retaining and examining the BPD would involve, that is to say the degree or extent of interference with individuals' right to privacy under Article 8 of the European Convention on Human Rights (ECHR). Each dataset is assessed on a case-by-case basis, and in the round, having regard (amongst other things) to the following factors or indicators:
- Is there an expectation of privacy? Did the individual provide their personal data in confidence to another organisation, not expecting that anyone except that organisation would have access to their data?
  - Does the data consist of more than basic personal details (e.g. more than name, date of birth, address, telephone number and e-mail address)?
  - Is there information on a person's activities or movements or travel?



- Does the data include ‘sensitive personal data’ within the meaning of section 2 of the Data Protection Act 1998 (“DPA” - see paragraph 11.8 of Annex A)?
  - To what degree does the data, by virtue of its quality, nature or size, mean that, when it is examined, there will be a significant degree of intrusion into the privacy of individuals not of intelligence interest?
- 4.18 The indicators provide a framework which assists the relevant Security and Intelligence Agency in reaching a decision on the degree or extent of intrusiveness which retaining and examining the dataset would involve. The indicators are not intended to be prescriptive; the presence of one or more will not necessarily result in the dataset as a whole being considered to be relatively more intrusive. (It should be noted that, in accordance with section 186, any dataset containing a substantial proportion of DPA-sensitive data will in any event be required to be authorised by a specific BPD warrant.)

## Confidential information relating to members of sensitive professions

- 4.19 Most BPDs do not include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to the sensitive professions. However, in the unlikely event that the Security and Intelligence Agency believed that a BPD contained confidential information relating to a member, or members, of a sensitive profession, the Agency must seek a specific warrant.
- 4.20 In this context, confidential information would include the content of communications between the professional, acting in their professional capacity, and another party, and any information which identified journalistic sources. Thus, for example, it would include the content of lawyer/client, doctor/patient and MP/constituent communications. However, information relating to a member of a sensitive profession is not, in and of itself, considered confidential. Confidential information in this context would not include the mere fact of membership of the profession, or basic biographical details of a member of the profession. Thus, the fact that a solicitor’s telephone number appeared in a telephone directory, would not be considered confidential information.
- 4.21 Section 188 specifies that an application for a specific BPD warrant must include:
- a description of the specific dataset to which the application relates; and
  - an explanation of the “operational purposes” for which the relevant Security and Intelligence Agency wishes to examine the BPD.
- 4.22 Section 188(6) also enables a Security and Intelligence Agency, when applying for a specific BPD warrant in respect of a particular BPD (‘dataset A’), to request at the same time that the authorisation should extend to the retention and use of ‘**replacement datasets**’, i.e. other bulk personal datasets that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

4.23 Before submitting an application for a specific warrant to the Secretary of State, the Security and Intelligence Agency must be satisfied that:

- retention of the BPD is **necessary** for one or more of the statutory purposes specified in section 188 of the Act, namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- examination of the BPD is **necessary** for one or more of the operational purposes to be specified in the specific warrant and for one or more of the statutory purposes specified in section 188 of the Act; and
- examining and retaining the BPD in question is **proportionate** to what is sought to be achieved by the conduct.

4.24 Section 188(7) makes clear that the fact that the information that would be obtained under the a warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

DRAFT



## 5 Authorisation of class and specific BPD warrants by a Secretary of State

- 5.1 The Secretary of State may only issue a warrant under sections 187 (class BPD warrants) or 188 (specific BPD warrants) if the Secretary of State considers the following tests are met:
- The warrant is necessary:<sup>1</sup>
    - In the interests of national security;
    - For the purpose of preventing or detecting serious crime; or
    - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.
  - The conduct authorised by the warrant is proportionate to what it seeks to achieve.
  - Each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a). (See paragraph 5.7 and subsequent paragraphs for more on operational purposes.)
  - There are satisfactory safeguards in place. The Secretary of State must consider that satisfactory arrangements are made for storing the BPD and for protecting them from unauthorised disclosure. (See paragraph 7.3 and subsequent paragraphs).
- 5.2 A Judicial Commissioner has approved the issue of the warrant. Except in the case of an urgent specific warrant, the Secretary of State may not issue a warrant unless and until the decision to issue the warrant has been approved by a Judicial Commissioner (see paragraph 5.26 and subsequent paragraphs).
- 5.3 When considering whether to issue a class BPD warrant, the Secretary of State will have regard to:
- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class, the necessity and proportionality considerations, and any other factors specified in paragraph 4.6 which apply; and
  - the number of individual bulk personal datasets which are likely to fall within that class warrant.

---

<sup>1</sup> A single warrant can be justified on more than one of the grounds listed.

- 5.4 The Secretary of State will not issue the warrant unconditionally unless satisfied that:
- having regard to the considerations referred to in the first bullet point in paragraph 5.3 above, it is appropriate to issue the warrant; and
  - the number of bulk personal datasets referred to in the second bullet point in paragraph 5.3 above is such that it will still be possible for the Secretary of State and Judicial Commissioner, including the Investigatory Powers Commissioner, to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.
- 5.5 In the event that the Secretary of State is satisfied in relation to the two bullet points in paragraph 5.4 above, he or she will issue the warrant.
- 5.6 In the event that the Secretary of State is not satisfied in relation to either bullet-point, he or she will either require the boundaries of the class to be reduced and/or (as the case may be) specify what the upper limit of BPDs in the class ('the cap') should be. He or she would do this by either (a) refusing to issue the warrant and instead inviting the relevant Security and Intelligence Agency to split the class into smaller classes and submit revised applications for class BPD warrants accordingly, or (b) issuing the class BPD warrant subject to the specified cap and inviting the relevant Agency to submit applications for a separate class BPD warrant or specific BPD warrants for any individual BPDs which could not be included in the class warrant that has been issued without exceeding the cap specified for that class.

## What are operational purposes?

- 5.7 Section 202 provides specific safeguards relating to the selection of data contained in a BPD under class or specific BPD warrant for examination. References to examination of data from a BPD are references to it being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant (see section 239 of the Act for general definitions in the Act).
- 5.8 Sections 202(1) and 202(2) make clear that selection for examination of data from a BPD may only take place for one or more of the operational purposes that are specified on the warrant. Operational purposes limit the purposes for which data collected under the warrant can be selected for examination, rather than limiting the information which can be examined per se, and no official is permitted to select for examination, data from a BPD, otherwise than in accordance with a specified operational purpose. For the avoidance of doubt, data from a BPD selected for an operational purpose can, where it is necessary and proportionate to do so, be used, disclosed and retained for any statutory purpose.
- 5.9 Sections 187 and 188 make clear that operational purposes must relate to one or more of the statutory purposes specified on the warrant. However, section 194(5) provides that the operational purposes specified in the warrant must be ones specified in the list of operational purposes which the Heads of

the Security and Intelligence Agencies are required to maintain. Section 194(6) makes clear that a warrant may specify all the operational purposes that appear on that list of operational purposes. Section 194(7) and 194(8) provide that an operational purpose may be specified in that list only with the Secretary of State's approval, which may only be given if the Secretary of State is satisfied that the operational purpose is specified in a greater level of detail than the wording of one of the statutory purposes. Thus, operational purposes provide the Secretary of State and the Judicial Commissioner with a more granular understanding of the purposes for which the BPD will be retained and examined by the Security and Intelligence Agencies.

- 5.10 Section 194(9) provides that every three months (from when that provision comes into force) the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament. Section 194(11) requires the Prime Minister to review the list of operational purposes at least once a year.
- 5.11 The Security and Intelligence Agencies need to retain the operational agility to respond to developing and changing threats and the range of operational purposes that may need to be specified on a BPD warrant needs to reflect this. New operational purposes will therefore be required over time. The Act provides (under section 197) that a BPD warrant may be modified to amend the operational purposes specified on it; for further detail on the process for this, see later sections of this chapter.
- 5.12 In line with this, the Security and Intelligence Agencies will need to ensure the full range of their BPD warrants are relevant to the current threat picture and, where applicable, the intelligence priorities set by the National Security Council. They will need to identify operational purposes that need to be added to or removed from BPD warrants, including in urgent circumstances. This would be done through the modifications process set out in the Act.
- 5.13 Some operational purposes that may need to be specified on a bulk warrant will be consistent across the three Agencies, although some purposes will be relevant to a particular Agency or two of the three. Operational purposes should as far as possible be consistent across the bulk capabilities provided for by the Act.
- 5.14 The Act does not limit the number of operational purposes that may be specified in the warrant. Where the necessity and proportionality test is satisfied, a warrant may include all operational purposes currently in use by an Agency. BPDs are likely to have potential relevance and utility across the full range, or most, of a Security and Intelligence Agency's operations or investigations. In the majority of cases, it will therefore be highly likely that it would be considered necessary for BPD warrants to specify the full range of an Agency's operational purposes.
- 5.15 An example of an "operational purpose" in the context of the security and intelligence agencies' international counter-terrorism work might be 'The Investigation, assessment and disruption of attack planning by Daesh in Iraq/Syria against the UK.'

## Necessity and proportionality

- 5.16 Where the retention or examination of a BPD involves an interference with an individual's rights under Article 8 (right to respect for private and family life) of the ECHR, this will only be justifiable if the interference is necessary and proportionate. The Act recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the statutory purposes set out in section 187(3) and 188(6) of the Act:
- In the interests of national security;
  - For the purpose of preventing or detecting serious crime;
  - In the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.
- 5.17 The Secretary of State must also believe that the retaining or examination of the BPD is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into privacy against the need for the activity in investigative, operational or capability terms.

## When will retaining or examining a BPD be necessary?

- 5.18 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 retention and examination, the Security and Intelligence Agencies and the Secretary of State must consider why retaining or retaining and examining the bulk personal dataset is 'really needed' for the statutory and operational purposes referred to in paragraph 5.1 above.
- 5.19 Chapter 7 includes further material on the necessity considerations that apply to examination of BPDs.

## When will retaining or examining a BPD be proportionate?

- 5.20 The retention or examination of the bulk personal dataset must also be proportionate to what is sought to be achieved by the conduct authorised under the warrant. In order to meet the 'proportionality' requirement, the Security and Intelligence Agencies and the Secretary of State 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 dataset and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the dataset.
- 5.21 The Security and Intelligence Agency and the Secretary of State 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 dataset and the importance of the operational purposes to be achieved. The

Security and Intelligence Agency and the Secretary of State must also consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion.

- 5.22 The warrant will not be proportionate if it is excessive in the overall circumstances of the case. The conduct authorised should bring an expected benefit to the Security and Intelligence Agency's investigations or operations and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not necessarily render intrusive conduct proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.
- 5.23 Chapter 7 includes further material on the proportionality considerations that apply to examination of BPDs.

### **Authorisation of a specific warrant: senior officials**

- 5.24 The Act permits that when it is not reasonably practicable for the Secretary of State to sign a specific BPD warrant a senior official may sign the warrant on their behalf. Typically this scenario will arise where the appropriate Secretary of State is not physically available to sign the warrant because, for example, he or she is on an external visit or in their constituency. The Secretary of State must still personally authorise the BPD warrant. When seeking authorisation the senior official must explain the case, either in writing or orally, to the Secretary of State and this explanation should include considerations of necessity and proportionality. Once authorisation has been granted the warrant may be signed by a senior official. If the Secretary of State refuses to authorise the warrant the warrant must not be issued. When a warrant is issued in this way the warrant instrument must contain a statement to that effect. A warrant that has been signed by a senior official is not an urgent warrant unless there is a statement to that effect from the Secretary of State. Except in urgent cases the decision to issue the warrant must then be approved by a Judicial Commissioner before the warrant is issued.
- 5.25 The Act does not mandate how the Judicial Commissioner must show or record his or her decision. These practical arrangements should be agreed between the relevant Government Departments and the Investigatory Powers Commissioner. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to issue a warrant. It is important that a written record is taken of any such approvals.

### **Approval of the issue of BPD warrants by a Judicial Commissioner**

- 5.26 Before a class or specific BPD warrant can be issued by the Secretary of State, it must be approved by a Judicial Commissioner.

- 5.27 Section 190 of the Act provides that, when deciding whether to approve the decision to issue a BPD warrant, the Judicial Commissioner must review the Secretary of State's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. The Judicial Commissioner must also review the Secretary of State's conclusions as to whether each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary, and whether the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a). In reviewing these matters, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner must also consider the matters sufficiently carefully so as to ensure he or she complies with the duties set out in section 2 (general duties in relation to privacy). The Judicial Commissioner may speak to the warrant granting department or warrant seeking agency as part of their considerations.
- 5.28 If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either:
- not issue the warrant;
  - refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).
- 5.29 If the Investigatory Powers Commissioner refuses the decision to issue a warrant the Secretary of State must not issue the warrant. There is no avenue of appeal available to the Secretary of State.

## Urgent authorisations

- 5.30 The Act makes provision (see sections 191 – 193) for cases in which a specific BPD warrant is required urgently. It is not possible to seek an urgent class BPD warrant.
- 5.31 In addition to the tests sets out at paragraph 5.1 above, the Secretary of State must believe that there was an urgent need to issue the warrant. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time. Accordingly, urgent warrants can be issued by the Secretary of State without prior approval from a Judicial Commissioner. The requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need. Urgent warrants should, therefore, fall into at least one of the following three categories:
- Imminent threat to life or serious harm – for example, an individual has been kidnapped and it is assessed that his life is in imminent danger;

- A significant intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas.
  - A significant investigative opportunity – for example, there is an imminent attempt to smuggle weapons into the UK to a known terrorist by boat; we may wish to use BPD to identify the vessel to prevent the weapons reaching the terrorist.
- 5.32 The decision by the Secretary of State to issue an urgent warrant must be reviewed by a Judicial Commissioner within three working days following the day of issue. In the case of warrants signed by a senior official, the Judicial Commissioner’s review should be on the base of a written record, including any contemporaneous notes, of the oral briefing of the Secretary of State by a senior official (and any questioning or points raised by the Secretary of State).
- 5.33 If the Judicial Commissioner retrospectively agrees to the Secretary of State’s issuance of the urgent warrant, and it is still considered necessary and proportionate by the warrant requesting agency, renewal of the urgent warrant may be sought. A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it expires after six months, in the same way as non-urgent BPD warrants.
- 5.34 The Judicial Commissioner may refuse to approve the Secretary of State’s decision to issue the urgent warrant. If that is the case, the urgent warrant ceases to have effect and may not be renewed. However, the Judicial Commissioner may:
- direct that any BPD retained in reliance on the warrant must be destroyed; or
  - impose conditions as to the use or retention of any such datasets. The Security and Intelligence Agency or the Secretary of State can make, or be required to make by the Judicial Commissioner, representations to the Commissioner about requirements to destroy datasets and/or conditions relating to use or retention.
- 5.35 A Security and Intelligence Agency is not to be regarded as in breach of the requirement to have a warrant where it retains or (as the case may be) examines a bulk personal dataset in accordance with conditions imposed by the Judicial Commissioner in the way described in paragraph 5.34 above.
- 5.36 If the Judicial Commissioner does not approve the urgent warrant, the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant stopped as soon as possible. In such a scenario, activity undertaken by virtue of that urgent warrant remains lawful, including activity in process at the time the warrant ceases to have effect which it is not reasonably practicable to stop.
- 5.37 A flowchart setting out the urgent authorisation process is provided at Annex B.



## Duration of BPD warrants

- 5.38 Section 195 provides that, for non-urgent warrants, the warrant comes into effect at the point at which it is issued or, in the case of a renewed warrant, the day following the day on which it would otherwise have ceased to have effect. In either case, the warrant lasts for six months. Such warrants may only be renewed in the last 30 days of the period for which they have effect. An urgent warrant lasts for five working days after the day on which it was issued.
- 5.39 Where modifications to a BPD warrant are made, the warrant expiry date remains unchanged.
- 5.40 Where a change in circumstance leads the Security and Intelligence Agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the Agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

## Modification of a BPD warrant

- 5.41 Section 197 provides for modifications of BPD warrants. There are two kinds of modifications: (a) major modifications, which add or vary any operational purpose specified in the warrant; and (b) minor modifications, which remove any operational purpose specified in the warrant. A class or specific BPD warrant may be modified by an instrument under the provisions at section 197.
- 5.42 A modification to add or vary an operational purpose must be made by the Secretary of State (except in the situation described in paragraph 5.43 below), and except where the Secretary of State considers it urgent, the decision to make the modification must be approved by a Judicial Commissioner before the modification comes into force. (See paragraph 5.46 and subsequent paragraphs for more on urgent modifications.) A modification to remove an operational purpose may be made by Secretary of State or a designated senior official acting on behalf of the Secretary of State.
- 5.43 If it is not reasonably practicable for the Secretary of State to make a modification to add or vary an operational purpose – for example where he or she is out of the country, working within his or her constituency, or otherwise unavailable – a senior official acting on behalf of the Secretary of State may make the modification with the express authorisation of the Secretary of State. In such a case, the modification instrument must contain a statement (a) that it is not reasonably practicable for the instrument to be signed by the Secretary of State and (b) that the Secretary of State has personally and expressly authorised the making of the modification.
- 5.44 If a modification removing an operational purpose is made by a designated senior official, the Secretary of State must be notified personally of the modification and the reasons for making it. This can be done in writing or orally, though if it is done orally a record must be kept (see Chapter 8 of this Code for further information on record-keeping). It should happen as quickly as reasonably practicable. If at any time the Secretary of State, or a senior



official acting on their behalf, considers that a specified operational purpose is no longer necessary in the interests of the statutory purposes listed on the warrant, they must modify the warrant to remove that operational purpose.

- 5.45 The modification instrument should be addressed to the person to whom the warrant was issued (i.e. the head of the relevant Security and Intelligence Agency).

## **Urgent modification of a BPD warrant**

- 5.46 Sections 197 and 198 provide for urgent modifications of BPD warrants. An operational purpose may be added to or varied on an urgent basis. In such a case, the Secretary of State's decision to make the modification does not need to be approved by a Judicial Commissioner prior to having effect. A Judicial Commissioner must decide whether to approve the decision to make such a modification within five working days.
- 5.47 If the Judicial Commissioner does not approve the urgent modification, the warrant has effect as if the modification had not been made, and the relevant Security and Intelligence Agency must do whatever is reasonably practicable to ensure that anything in the process of being done under the warrant by virtue of that modification is stopped as soon as possible. In such a scenario, activity undertaken by virtue of that modification remains lawful, including activity in process at the time the modification ceases to have effect which it is not reasonably practicable to stop.

## **Renewal of BPD warrants**

- 5.48 The Secretary of State may renew a warrant. Non-urgent warrants may only be renewed in the last 30 days of the period for which they have effect. Urgent warrants may be renewed at any point before their expiry date (section 196 of the Act). Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.1 above. In particular, the applicant must give an assessment of the value derived to date from the specific BPD or from the class of BPD in question, and explain why it continues to be necessary to retain and/or examine the specific BPD(s) or the class of BPDs, and why this continues to be proportionate.
- 5.49 In deciding whether to renew a BPD warrant, the Secretary of State must also consider whether the examination of the specific BPD or the class of BPDs continues to be necessary for one or more of the specified operational purposes, and that any examination of that material for these purposes is necessary for one or more of the statutory purposes (as set out in the first bullet-point in paragraph 5.1 above) on the warrant.
- 5.50 When considering whether to renew a class BPD warrant, the Secretary of State will have regard to:

- the nature and scope of the class for which the warrant is being sought, i.e. the category of data and breadth or width of the class, the necessity and proportionality considerations, and any other factors specified in paragraph 4.6 which apply; and
  - the number of individual bulk personal datasets which are likely to fall within that class warrant.
- 5.51 The Secretary of State will not issue the warrant unconditionally unless satisfied that:
- having regard to the considerations referred to in the first bullet point in paragraph 5.50 above, it is appropriate to issue the warrant; and
  - the number of bulk personal datasets referred to in the second bullet point in paragraph 5.50 above is such that it will still be possible for the Secretary of State and Judicial Commissioner, including the Investigatory Powers Commissioner, to continue to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of the individual BPDs authorised by that warrant.
- 5.52 In the event that the Secretary of State is satisfied in relation to the two bullet points in paragraph 5.51 above, he or she will issue the warrant.
- 5.53 In the event that the Secretary of State is not satisfied in relation to either bullet-point, he or she will either require the boundaries of the class to be reduced and/or (as the case may be) specify what the upper limit of BPDs in the class ('the cap') should be. He or she would do this by either (a) refusing to issue the warrant and instead inviting the relevant Security and Intelligence Agency to split the class into smaller classes and submit revised applications for class BPD warrants accordingly, or (b) issuing the class BPD warrant subject to the specified cap and inviting the relevant Agency to submit applications for a separate class BPD warrant or specific BPD warrants for any individual BPDs which could not be included in the class warrant that has been issued without exceeding the cap specified for that class.
- 5.54 Where the Secretary of State is satisfied that the retention and/or examination of the BPD continues to meet the requirements of the Act, the Secretary of State may renew the warrant. In all cases, a BPD warrant may only be renewed if the decision to renew that warrant has been approved by a Judicial Commissioner. The renewed warrant is valid for six months from the day following the day on which it would otherwise have ceased to have effect.
- 5.55 A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

## **Cancellation of warrant**

- 5.56 The Secretary of State, or a senior official acting on his or her behalf, may cancel a BPD warrant at any time (see section 199). Such persons must cancel a BPD warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on the grounds of any one of the statutory purposes for which it was issued. The Security and Intelligence

Agencies will therefore need to keep their BPD warrants under continuous review and must notify the Secretary of State if they assess that a warrant is no longer necessary. In practice, the responsibility to cancel a warrant will normally be exercised by a senior official in the warrant granting department on behalf of the Secretary of State.

- 5.57 The cancellation instrument will be addressed to the person to whom the warrant was issued.
- 5.58 The cancellation of a warrant does not prevent the Secretary of State deciding, with Judicial Commissioner approval, to issue a new warrant, covering the same or different bulk personal datasets and operational purposes, in the future should it be considered necessary and proportionate to do so. Where there is a requirement to modify the warrant, other than to amend the operational purposes for which the data can be examined, then the warrant may be cancelled and a new warrant issued in its place.

## **Non-renewal or cancellation of class BPD warrants**

- 5.59 Section 200 provides for the situation where a BPD warrant is not renewed or is cancelled and, in particular, sets out the process for dealing with the material that was retained under the warrant in question. The material may be destroyed; section 200(2) ensures retention or examination of the material for the purpose of deleting the material is lawful. But depending on the reasons why the warrant has been cancelled or not renewed, the relevant Security and Intelligence Agency may consider it necessary and proportionate to retain some or all of the material that had been retained under the authority of that warrant. Section 200 therefore includes bridging provisions to ensure any retention and examination of the material in question is lawful pending any authorisation via a new warrant. The relevant Security and Intelligence Agency may apply for a new class or specific BPD warrant within five working days (section 200(2)).
- 5.60 If the relevant Agency needs further time to consider whether to apply for a new warrant, it may instead apply to the Secretary of State for authorisation to retain or retain and examine some or all the material retained under the warrant. The Agency can only apply for such authorisation if it is considering whether to apply for a new class or specific BPD warrant to authorise retention or retention and examination of the material. In particular, under section 200(6) and 200(7), the Agency has five working days in which to decide whether it wants to apply for such authorisation. Retention and examination of that data is lawful pending the Secretary of State's decision under such an application. If the agency so applies, the Secretary of State can then direct that any of the material should be destroyed or, with the approval of the Judicial Commissioner, can authorise the retention or examination of any of the material, subject to such conditions as the Secretary of State considers appropriate. Retention or examination is lawful under such a direction. During that period, the agency must consider whether to and then apply for a new warrant as soon as reasonably practicable and in any event within three months. Retention and examination remains lawful for the period between the agency applying for a new warrant and the determination of that

application, even if determination takes place after the end of the three month period.

- 5.61 These provisions may be required if, for example, the Secretary of State is no longer satisfied that all the individual bulk personal datasets in a BPD class authorised by a warrant should be retained, because e.g. the class is considered too wide in scope, but would be willing to issue to the relevant Security and Intelligence Agency a class BPD warrant for a more restricted class of BPD (or a specific warrant). In such a situation, the Secretary of State might be satisfied that it was necessary and proportionate for the relevant Intelligence Agency to retain some of the individual bulk personal datasets in the BPD class or a subset or subsets of that material, pending the issue of a new class warrant or specific warrant. Or the Secretary of State may be willing to authorise the continued retention and examination of some but not all the material held under a specific BPD warrant.
- 5.62 If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, section 200(4) requires that he or she must give the Secretary of State written reasons for this. If it was a Judicial Commissioner other than the Investigatory Powers Commissioner who did not approve the decision, the Secretary of State can ask the Investigatory Powers Commissioner to decide whether to approve the decision (section 200(5)).

## 6 Authorisation of the retention and use of BPDs falling within a class BPD warrant

- 6.1 For the purpose of dealing with BPD falling within the scope of an existing class BPD warrant, each Security and Intelligence Agency should have a formal internal authorisation procedure which must be complied with.
- 6.2 Before deciding to retain a BPD falling within the scope of an existing class BPD warrant (“the relevant class warrant”) for the purpose of the exercise of its statutory functions, the Security and Intelligence Agency must be satisfied that:
- the BPD in question falls within the scope of the relevant class warrant;
  - the Agency must be satisfied that it is not prevented by section 186 from retaining, or retaining and examining, the dataset in reliance on the class BPD warrant (see paragraph 4.9 and subsequent paragraphs);
  - retention of the BPD is **necessary** for one or more of the relevant Agency’s statutory functions;
  - each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary; and the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in section 187(3)(a) or section 188(6)(a)
  - retaining and examining the BPD in question is **proportionate** to what is sought to be achieved by the conduct;
  - only as much information will be obtained as is **necessary** to achieve those functions and purposes; and
  - there is no reasonable alternative that will still meet the proposed objective in a less intrusive way.
- 6.3 An explanation of the necessity and proportionality tests is provided at paragraph 5.16 and subsequent paragraphs and of operational purposes at paragraph 5.7 and subsequent paragraphs.
- 6.4 Before a new dataset falling within the scope of a class BPD warrant is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions, the relevant staff in that Agency should consider the factors set out in paragraph 6.2 above and complete the formal internal authorisation procedure. The authorisation procedure involves an application to a senior manager which should include the following:
- a description of the particular BPD, including details of the personal data contained in the dataset, and any confidential information relating

to members of sensitive professions or data that is considered to be intrusive (as assessed by reference to the factors in paragraph 4.17 and subsequent paragraphs) of which staff are aware;

- a description of the class BPD warrant within which the dataset falls;
- the justification for retention and examination, including the operational purposes for which examination of the dataset is required, the statutory functions which are engaged and the necessity and proportionality of the proposed retention and examination;
- an assessment of the level of intrusion into privacy;
- the consideration and advice of the relevant Agency's legal advisers; and
- the extent of political, reputational or other risk.

6.5 The relevant Security and Intelligence Agency should consult line or senior management for guidance. They may also seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant warrant-issuing Department), the Secretary of State and/or the Investigatory Powers Commissioner. If the Security and Intelligence Agency is not clear on whether an internal authorisation is appropriate, then they should seek guidance from the Secretary of State (or his or her relevant senior officials) and / or a Judicial Commissioner. The Security and Intelligence Agency should also take into account any guidance provided by the Secretary of State or the Judicial Commissioner in this regard.

6.6 Once authorised, the completed application should be stored on a record by the appropriate Security and Intelligence Agency's information governance/compliance team, which will include the date of approval. This record should also contain the date when the Agency decided to retain the dataset after the initial examination referred to in paragraph 2.3 and subsequent paragraphs, which should be the date used for the review process (for which see paragraph 7.18 and subsequent paragraphs).

# 7 Safeguards

- 7.1 This chapter sets out the safeguards which each Security and Intelligence Agency should put in place in relation to storage of bulk personal datasets (whether acquired under class BPD or specific BPD warrants), record-keeping, access to and examination of BPDs, disclosure and review and retention of BPDs. The Secretary of State may only issue a BPD warrant if s/he considers that arrangements made by the relevant Security and Intelligence Agency for storing BPD and for protecting the datasets from unauthorised disclosure are satisfactory (as set out in sections 187(3)(d) and 188(6)(d)).
- 7.2 The safeguards in this chapter are in addition to those set out in earlier chapters of this code, including the requirement for the retention and examination of a BPD to be necessary and proportionate for it to take place; the need to ensure only as much information will be obtained as is necessary and that there is no reasonable alternative that will still meet the proposed objective in a less intrusive way; the particular considerations that need to be given to the intrusiveness of the data and the extent to which that data includes confidential information relating to sensitive professions; and the requirement for Secretary of State and Judicial Commissioner approval for BPD warrants. (See chapters 4 and 5).

## Storage

- 7.3 Each Security and Intelligence Agency should maintain robust data security and protective security standards. They should have in place handling procedures so as to ensure that the integrity and confidentiality of the information in the BPD is effectively protected, 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 it is detected and that appropriate disciplinary action is taken. In particular, each Agency should 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; and
  - A security-vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

## Safeguards before a BPD is made accessible

- 7.4 Where a BPD contains either material assessed by the Security and Intelligence Agency as relatively more intrusive (see paragraph 4.17 and



subsequent paragraphs) or confidential information relating to sensitive professions (see paragraph 4.19 and subsequent paragraphs), before such a BPD is held electronically by a Security and Intelligence Agency for analysis in the exercise of its functions the relevant Agency should consider whether access by its staff to such data should be subject to any particular restrictions, including sensitive fields being suppressed or deleted, or additional justification required to access and examine sensitive data-fields.

## Access and examination

- 7.5 In relation to information held in bulk personal datasets, each Security and Intelligence Agency should have in place the following additional measures:
- Access to and examination of the information contained within the bulk personal datasets should be strictly limited to those with an appropriate business requirement to use these data;
  - Individuals may only access information within a bulk personal dataset if examination of the BPD is necessary for one or more of the operational purposes specified in the relevant class warrant or specific warrant and for one or more of the relevant statutory purposes specified in the Act (see paragraph 5.16 and subsequent paragraphs);
  - If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, (in addition to satisfying the condition in the above bullet) they may only access and examine the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Agency or for the additional limited purposes set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
  - Before accessing or disclosing information, individuals must also consider whether to do so would be proportionate (as described in paragraph 5.20 and subsequent paragraphs and below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;
  - Users should receive mandatory training regarding their professional and legal responsibilities, including the application of the provisions of the Act and this Code of Practice. Refresher training and/or updated guidance should be provided when systems or policies are updated;
  - Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal data by staff in order to detect misuse or identify activity that may give rise to security concerns;
  - Appropriate disciplinary action should be taken in the event of inappropriate behaviour being identified;



- Users should 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; and
  - The Secretary of State must ensure that the safeguards are in force before any BPD warrant authorising use can begin.
- 7.6 The Security and Intelligence Agencies should also take the following measures – by establishing the necessary underpinning working practices - to reduce the level of interference with privacy arising from the retention and examination of bulk personal datasets:
- Minimising the number of results which are presented for analysis, by training and requiring staff to frame queries in a proportionate way; and
  - If necessary, confining access to specific datasets (or subsets thereof) to a limited number of analysts.

## Personnel security

- 7.7 All persons within the Security and Intelligence Agencies who may have access to BPDs or need to see any reporting in relation to them must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one Agency to disclose BPDs to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

## Additional access safeguards for confidential information relating to sensitive professions

- 7.8 The Security and Intelligence Agencies should ensure that, before Security and Intelligence Agency staff who are searching a bulk personal dataset specifically target for access or examination confidential information relating to members of sensitive professions, **special consideration** is given to the necessity and proportionality justification for the interference with privacy that will be involved.
- 7.9 The Security and Intelligence Agencies should also ensure that particular care is taken when deciding whether to seek such access to data or information of the kind described in paragraph 7.8 above, and should consider whether there might be unintended consequences of such access and whether the public interest is best served by this, and only to do so if authorised beforehand by a senior manager.
- 7.10 All cases where Security and Intelligence Agency staff intentionally seek to examine such data or information, they should be required to record the fact that such information or data has been accessed and selected and flag this to the Investigatory Powers Commissioner at the next inspection. Likewise, where Security and Intelligence Agency staff are aware that in searching a

bulk personal dataset they have unintentionally accessed such data or information but have decided to select and retain it, they should be required to record the fact of this access and intentional selection and flag this to the Investigatory Powers Commissioner at the next inspection.

## Disclosure

- 7.11 Information in bulk personal datasets held by a Security and Intelligence Agency (whether acquired under class BPD or specific BPD warrants) may only be disclosed to persons outside the relevant Agency if the following conditions are met:
- that the objective of the disclosure falls within the Agency's statutory functions or is for the additional limited purposes set out in the information gateway provisions (sections 2(2)(a) and 4(2)(a) of the ISA and section 2(2)(a) of the SSA – see paragraph 11.3 of Annex A);
  - that it is **necessary** to disclose the information in question in order to achieve that objective;
  - that the disclosure is **proportionate** to the objective; and
  - that only as much of the information will be disclosed as is **necessary** to achieve that objective.
- 7.12 In order to meet the 'necessity' requirement in relation to disclosure, the Security and Intelligence Agency must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Agency or for the additional limited purposes set out in the information gateway provisions.
- 7.13 The disclosure of the bulk personal dataset must also be proportionate to the purpose in question. In order to meet the 'proportionality' requirement, the relevant Security and Intelligence Agency 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 Agency's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. The relevant Security and Intelligence Agency 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.
- 7.14 Before disclosing any bulk personal data, the relevant Security and Intelligence Agency must either take reasonable steps to ensure that the intended recipient organisation has, and will maintain, satisfactory arrangements regarding the use of the BPD, and for safeguarding the confidentiality of the data and ensuring that it is securely handled. What steps should to be viewed as reasonable in any particular instance of disclosure will depend on the circumstances of the case, but will include consideration of the nature of the disclosure and what is known about the recipient.

- 7.15 Where the BPD has been acquired under an interception warrant, the relevant Security and Intelligence Agency must also consider whether the restrictions on the use of disclosure of material obtained under an interception warrant into legal proceedings, will be relevant (see section 203(6)).
- 7.16 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. 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 individual item of data. The authorisation process requires an application to a senior manager designated for the purpose which is required to set out the following:
- a description of the dataset it is proposed to disclose (in whole or in part), including details of the personal data contained in the dataset, and any significant component of intrusive data or confidential information relating to sensitive professions of which staff are aware;
  - the operational and legal justification for the proposed disclosure, and the necessity and proportionality of the disclosure;
  - an assessment of the level of intrusion into privacy;
  - the extent of political, reputational or other risk;
  - whether any caveats or restrictions should be applied to the proposed disclosure; and
  - confirmation that reasonable steps have been taken to ensure that disclosure to the recipient organisation is in accordance with paragraph 7.14 above.
- 7.17 This information should be included, so that the senior manager can then consider the factors in paragraph 7.11 with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Agency may seek guidance from relevant Senior Officials (i.e. members of the Senior Civil Service in the relevant Department), the Secretary of State and/or the Investigatory Powers Commissioner.

## Review of retention and deletion

- 7.18 Each Security and Intelligence Agency must regularly review the operational and legal justification for its **continued retention, examination and use** of each bulk personal dataset retained by it under a class warrant. The frequency of the review – as agreed with the Secretary of State – should be guided by the level of intrusion which is generated by the holding of the BPD (and any other factors that the Security and Intelligence Agency or the Secretary of State consider appropriate), and must in any event be such as to ensure that the justification for the continued retention of bulk personal datasets covered by the relevant class warrant is adequately considered.
- 7.19 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 of the dataset and its examination for the operational purposes, with examples of use;
- The extent to which the dataset originally acquired needs to be replaced by a more up-to-date;
- The level of intrusion into privacy;
- The extent of political, reputational or other risk; and
- Whether any caveats or restrictions should be applied to continued retention.

## **Destruction**

7.20 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 Security and Intelligence Agency should be destroyed. Section 239 of the Act provides definition of ‘destroy’. Each Agency should report to the Secretary of State, on a six-monthly basis, with a list of all BPDs destroyed in the previous six months.

## **Other management controls**

- 7.21 The retention and disclosure of a bulk personal dataset should be subject to scrutiny in each Security and Intelligence Agency, which should put in place an effective system to ensure each of the following:
- that each bulk personal dataset has been properly obtained;
  - that access to a BPD is permitted only for the specified operational purposes and for the relevant Security and Intelligence Agency’s statutory functions;
  - that any disclosure is properly justified; and
  - that retention and examination of the BPD remains necessary for the specified operational purposes and the proper discharge of the relevant Security and Intelligence Agency’s statutory functions and is proportionate to achieving that objective.
- 7.22 Each Security and Intelligence Agency should ensure that there is a system in place whereby the relevant audit team effectively monitors the examination of bulk personal datasets by staff in order to detect misuse or identify activity that may give rise to security concerns.
- 7.23 Any such identified activity initiates a formal investigation process in which legal, policy and 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.

- 7.24 All reports on audit investigations are required to be made available to the Investigatory Powers Commissioner for scrutiny (see chapter 9 below).

DRAFT

## 8 Record-keeping and error-reporting

- 8.1 The oversight regime allows the Investigatory Powers Commissioner to inspect the warrant application upon which the authorisation was based, and the applicant may be required to justify the content. Each Security and Intelligence Agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:
- All applications made for BPD warrants and all applications made for the renewal of such warrants;
  - All BPD warrant instruments, associated schedules, renewal instruments and copies of modification applications; and
  - Where any application is refused, the grounds for refusal as given by the Secretary of State.
- 8.2 Records should also be kept by the relevant Department of State of the warrant authorisation process. This will include:
- All advice provided to the Secretary of State to support his/her consideration as to whether to issue or renew the BPD warrant;
  - Written records, including contemporaneous notes, of requests for urgent authorisations of warrants or modifications; and
  - Where the issuing of any application is not approved by the Judicial Commissioner, the grounds for refusal as given by the Judicial Commissioner and any associated advice / applications to the Investigatory Powers Commissioner if there is an appeal.
- 8.3 Each Security and Intelligence Agency must also keep a record of the following information to assist the Investigatory Powers Commissioner to carry out his/her statutory functions:
- The number of applications for (a) class and (b) specific BPD warrants submitted.
  - The number of applications for (a) class and (b) specific BPD warrants refused by the Secretary of State.
  - The number of decisions to issue (a) class and (b) specific BPD warrants refused by a Judicial Commissioner.
  - The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse the Secretary of State decision to issue (a) class and (b) specific BPD warrants.
  - The number of (a) class and (b) specific BPD warrants issued by the Secretary of State and approved by a Judicial Commissioner.

- The number of times an urgent specific BPD warrant has been (a) submitted and (b) authorised by the Secretary of State and issued by a senior official.
  - The number of times that the decision to authorise an urgent specific BPD warrant has subsequently been refused by a Judicial Commissioner.
  - The number of renewals of (a) class and (b) specific BPD warrants that were made.
  - The number of (a) class and (b) specific BPD warrants that were cancelled.
  - The number of (a) class and (b) specific BPD warrants extant at the end of the calendar year.
  - The number and details of modifications to add an operational purpose to the warrant, vary an operational purpose or remove an operational purpose from the warrant.
  - The number and details of urgent modifications to add an operational purpose to the warrant or vary an operational purpose the warrant.
  - The number and details of urgent modifications to add or vary an operational purpose (including on an urgent basis) where the decision was refused by a Judicial Commissioner.
  - The number of occasions that a referral was made by the Secretary of State to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve a decision to modify an urgent specific BPD warrant.
  - A record of BPDs held that fall within a particular class warrant (see chapter 6 above)
  - A record of any intentional examination of confidential information relating to sensitive professions (see paragraph 7.8 and subsequent paragraphs)
  - A list of all BPD deleted or destroyed in the previous six months (see paragraph 7.20)
- 8.4 These records must be sent in written or electronic form to the Investigatory Powers Commissioner, as determined by the Commissioner. Guidance on record keeping may be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Commissioner by the Security and Intelligence Agencies.
- 8.5 The Investigatory Powers Commissioner will use this information to inform their oversight and, where appropriate, include in their report to the Prime Minister about the carrying-out of the functions of the Judicial Commissioners. The Prime Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of the report if, in the opinion of the Prime Minister, the publication would be contrary to the public interest or prejudicial to national security, prevention or detection of serious crime, or the continued discharge of the functions of the overseen public authorities.

- 8.6 Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management. And any serious breaches of safeguards that have resulted in an unauthorised or unjustifiable interference with privacy, as agreed with the Investigatory Powers Commissioner, must be reported to the Commissioner. The Investigatory Powers Commissioner may issue guidance in respect of error-reporting which the Security and Intelligence Agency must have regard to.

DRAFT



## 9 Oversight

- 9.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the IPC'), whose remit includes providing comprehensive oversight of the retention, use or disclosure of bulk personal datasets by the security and intelligence agencies and adherence to the practices and processes described by this code. By statute the IPC will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The IPC will be supported by inspectors and others, such as technical experts, qualified to assist the IPC in their work.
- 9.2 The IPC, and those that work under the authority of the Commissioner, will ensure compliance with the law and this code by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister.
- 9.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out a full and thorough inspection regime. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the IPC and anyone who is acting on behalf of the Commissioner.
- 9.4 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in error reporting provisions of chapter 8 of the code, report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).
- 9.5 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to an individual who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the individual affected. Further information on errors can be found in chapter 8 of this code. The public body who has committed the error will be able to make representations to the Commissioner before they make their decision on whether it is in the public interest for the individual to be informed.
- 9.6 The Commissioner must also inform the affected individual of their right to apply to the IPT (see chapter 10 for more information on how this can be

done) who will be able to fully investigate the error and decide if a remedy is appropriate. The IPC must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions for reasons of national security. Only the Prime Minister will be able to authorise redactions to the IPC's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

- 9.7 The IPC may also report, at any time, on any of its investigations and findings as they see fit. These reports will also be made publically available subject to national security considerations. Public authorities and communications service providers may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible this guidance will be published in the interests of public transparency.
- 9.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

DRAFT

# 10 Complaints

- 10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.
- 10.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. The IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination.
- 10.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: <http://www.ipt-uk.com>. Alternatively information on how to make a complaint can be obtained from the following address:
- The Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ
- 10.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

# 11 Annex A

## The Security Service Act 1989 and the Intelligence Services Act 1994

- 11.1 The **Security Service Act 1989** (SSA) 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.
- 11.2 The **Intelligence Services Act 1994** (ISA) sets out the functions of the Secret Intelligence Service (SIS) and Government Communications headquarters (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, making use of or interfering with communications and related equipment; and providing advice on information security and languages. ISA 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.
- 11.3 The information gateway provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of ISA 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 ISA (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 ISA (for the purpose of any criminal proceedings) and section 2(2)(a) of SSA (for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).
- 11.4 SSA and ISA accordingly impose specific statutory limits on the information that each of the Security and Intelligence Agencies 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.

## The Counter-Terrorism Act 2008

- 11.5 Section 19 of the **Counter-Terrorism Act 2008** 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 Security and Intelligence Agencies 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.

## The Human Rights Act 1998

- 11.6 Each of the Security and Intelligence Agencies is a public authority for the purposes of the Human Rights Act 1998. When obtaining, using, retaining and disclosing bulk personal datasets, the Security and Intelligence Agencies 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 Agency and proportionate to the achievement of that objective.

## The Data Protection Act 1998

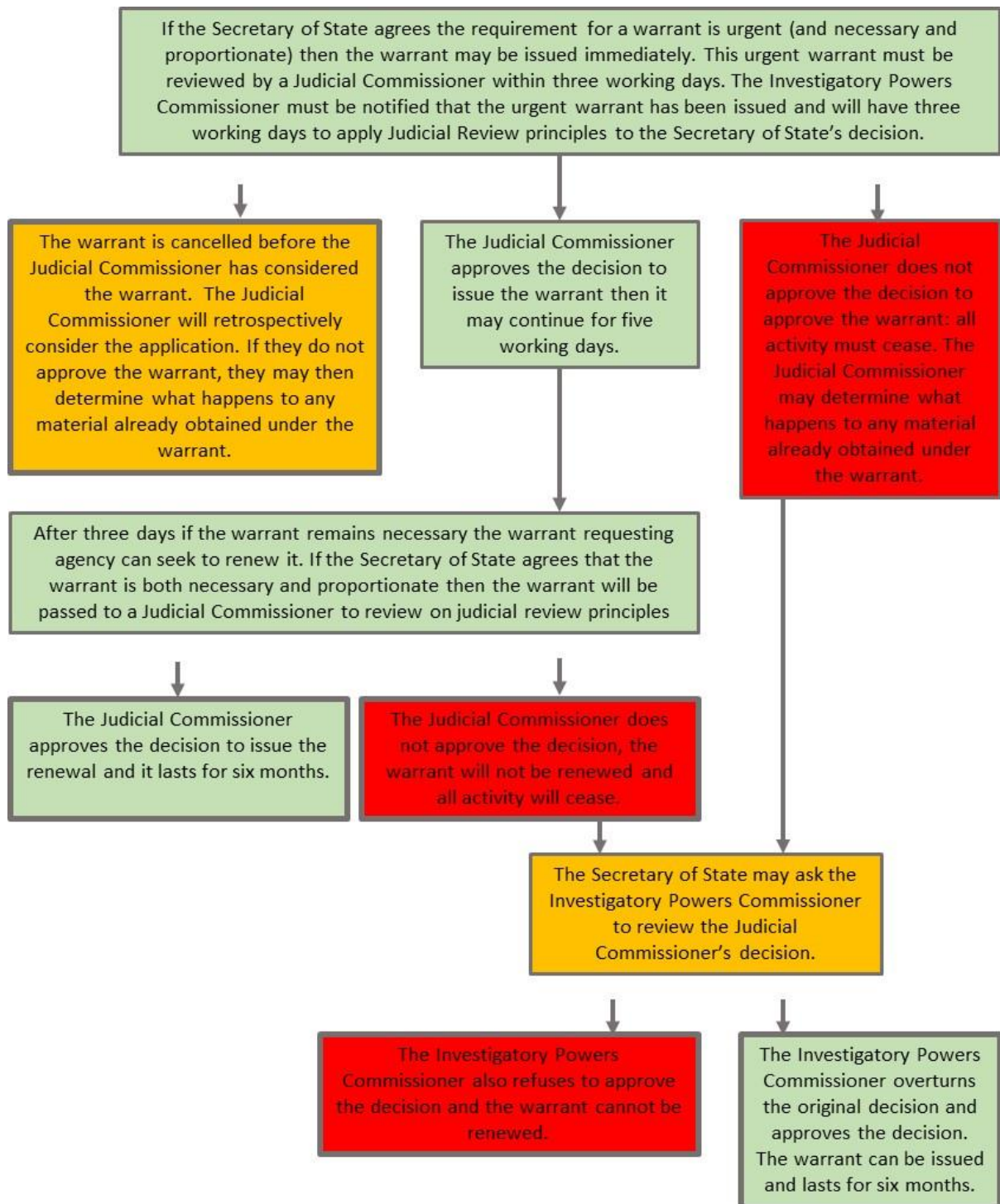
- 11.7 Section 1(1) of the **Data Protection Act 1998** defines ‘*personal data*’ as:
- “data which relate to a living individual who can be identified –
- from those data; or
  - from those data and other information which is in the possession of, or is likely to come into the possession of the data 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”.
- 11.8 Section 2 of the DPA defines “sensitive personal data” as meaning personal data in relation to a data subject consisting of information as to the following:
- Racial or ethnic origin
  - Political opinions
  - Religious belief or other beliefs of a similar nature
  - Membership of a trade union
  - Physical or mental health or condition

- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

11.9 Each of the Security and Intelligence Agencies is a data controller in relation to all the personal data that it holds. Accordingly, when the Security and Intelligence Agencies use any bulk data that contain personal data, they must ensure that they comply with the Data Protection Act 1998 (except in cases where exemption under section 28 is required for the purpose of safeguarding national security).

DRAFT

# 12 Annex B





# 13 Annex C

*The text in this annex is intended to provide an indication of the additional safeguards that would be added to the BPD code of practice if amendments to Part 7 of the Bill relating to protected data and legal professional privilege (LPP) are passed by the House of Lords at Report. The text does not aim to reflect a definitive list of all other related amendments (to for example, LPP) that may be made to other Parts of the Bill at Report and read across to Part 7 – and so necessitate further changes to all the associated codes of practice.*

## BPD warrant applications

*Extra bullet to be added to list at paragraph 4.13 of draft code – ‘In the ‘Case 2’ scenario...’ – as the first bullet. NB in the introductory text above the bullets, the word ‘two’ will need to be changed to ‘three’:*

- If the Agency considers that the BPD contains any **protected data** (see paragraph xxx and subsequent paragraphs).

*Footnote to be added to the last bullet of paragraph 4.13. The footnote would read:*

‘See paragraph 4.xx and paragraph 7.yy for specific safeguards in respect of legal professional privilege (LPP). In practice, LPP will only arise in the case of ‘protected data’, and so a BPD containing LPP will in any event be caught by the specific provisions in the Bill on such data: namely, a statutory prohibition on the use of class warrants and requirement to apply for a specific warrant, coupled with a power for the Secretary of State to attach conditions where ‘UK content’ is selected for examination, and specific access controls for intended/expected selection for examination of LPP.’

*The following text is to be inserted at the end of chapter 4 of the BPD code of practice:*

## **BPDs containing ‘protected data’ – further restriction on class warrants and provision for attaching conditions to specific warrants**

### **Introduction**

- 13.1 Part 7 does not regulate a technique for acquiring information, but rather a species of data that may be acquired from a variety of different sources and by different methods, as set out in Chapter 2 of this Code. This fact means that, to the extent that the retention and examination of BPDs may be

regarded as a capability, it is one that is of a different nature and kind from the techniques of bulk interception and bulk equipment interference.

- 13.2 Where data are acquired via bulk interception or bulk equipment interference, the degree of intrusiveness of the data falling into the protected class will depend on the nature and variety of the communications or items of information that are obtained from the systems or equipment in issue. It may therefore be difficult for the Agency implementing the warrant to assess in advance the nature and intrusiveness of all the data falling into the protected class that may be obtained by means of the bulk warrant. The Act must therefore apply the most stringent access controls to the selection for examination of all protected material relating to an individual known to be in the British Islands at the time of the selection. The statutory framework governing bulk interception and bulk equipment interference accordingly requires an Agency to obtain a targeted examination warrant when selecting for examination any protected material obtained under the warrant relating to an individual known to be in the British Islands at the time of the selection.
- 13.3 By contrast, where an Agency obtains a set of information other than in exercise of a power conferred by the Act, the Agency must conduct an initial examination to determine whether the set of information constitutes a BPD. If the set of information is retained as a BPD, the Agency will therefore be better able to assess the nature and intrusiveness of any data in the dataset that fall into the protected class. In particular, the Agency should be able to identify any protected data that comprise the contents of e-mails, letters or other documents. It will accordingly be possible for the Secretary of State and the Judicial Commissioner, at the time a specific BPD warrant is issued, and having regard to the Agency's initial examination and assessment, to determine the safeguards that should apply to the selection for examination of protected data relating to an individual known to be in the British Islands up to, and including, a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.
- 13.4 The stringent selection for examination safeguards in section 202 of the Act will already be sufficient to regulate the vast majority of cases where data contained in a BPD is selected for examination. These safeguards ensure that any selection for examination of data contained in a BPD is carried out only for the operational purposes specified in the warrant (which have been approved by the Secretary of State and Judicial Commissioner "double lock"). In addition, the selection of any such data for examination must be necessary and proportionate in all the circumstances.
- 13.5 Given the range and variation in intrusiveness of protected data (as defined in the annex to this Code) contained in BPDs, it is not necessary or appropriate to apply additional controls to the selection for examination of all protected data in BPDs relating to an individual known to be in the British Islands at the time of the selection. Nor is it feasible for the Act to seek to identify all the various types of protected data that may be contained in BPDs, or to provide in detail for the limitations on access to each type of field depending on its relative intrusiveness, over and above those already mandated in section 202.
- 13.6 This Chapter of the Code accordingly sets out a scheme that enables the Secretary of State (with the approval of the Judicial Commissioner) to impose

additional controls in relation to the selection for examination of any protected data in the dataset relating to individual is known to be in the British Islands at the time of the selection. The scheme applies on a dataset by dataset basis having regard to the range of factors set out below, including the nature and intrusiveness of the protected data in the dataset.

### Categorising data in BPD

- 13.7 For the purposes of this scheme, “protected data” has the meaning prescribed by section xxx of the Act and set out in this Code.
- 13.8 When categorising data contained in a BPD, the Agencies should first consider whether the dataset as a whole comprises data that are not “private information” (see paragraph 13.13). For example, a dataset consisting of data that are freely available online and are not subject to any privacy settings or access controls should be categorised as non-private information. No data fields in non-private datasets are protected data for the purposes of Part 7.
- 13.9 Except where paragraph 13.8 applies, the Agency should approach categorisation by determining whether the data contained in the BPD are systems data or identifying data (or both) and, if not, whether the data are not private information. These definitions are explained further below. Data that are systems data, identifying data or non-private are not protected. In cases where the Agency’s initial examination of the BPD suggests that data within the dataset are the contents of letters, e-mails or other documents, then the Agency should assume that the BPD contains protected data (though that does not mean that all the data contained in that BPD are protected).
- 13.10 **Identifying data** in a BPD is data that may help to identify persons, systems services, locations or events. Identifying data in a BPD does not therefore, of itself, need to identify a person etc. For example, a person’s name, address, occupation and country of birth in a BPD will all be identifying data, even though any one of them, on its own, might not identify that person etc. The majority of non-protected data in a BPD are likely to be categorised as identifying data.
- 13.11 **Systems data** is any data that enables or facilitates the functioning of any system or service. It includes all data that a system requires to function and provide its services. For example, if a passport number in a flight booking system has to be valid for the passenger to be able to fly then that passport number, when included in a travel BPD, will be systems data. The passport number will also be BPD identifying data.
- 13.12 Where a data field is correctly classified as systems data because the operation of the system or service is dependent on the validity of the value of that field, the data field should be permanently categorised as systems data. That remains the case even if the dataset containing the systems data field is passed to a third party and is retained on a different system.
- 13.13 **Private information** includes information relating to a person’s private or family life. In the BPD context, information falling which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, web forums, online social networking, mapping imagery, commercial subscription databases, academic articles, conference proceedings, business reports, and more. Such

information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

13.14 **Protected data** in relation to a BPD is any data contained in a BPD other than data which is one or more of the following: (a) identifying data (see paragraphs 13.10 and 13.15), (b) systems data, or (c) data which is not private information (see sections xx and 239(2) to 239(4) of the Act).

13.15 Protected data may contain embedded data items that individually:

- fall within the definition of identifying data (see section 239(2) to 239(3));
- are capable of being logically separated from the BPD or the other data in the BPD; and
- if they were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the BPD or that other data, disregarding any meaning arising from the existence of the BPD or the other data or from any data relating to that fact.

13.16 If an individual data item meets these conditions then it should be categorised as identifying data in its own right – whilst the categorisation of the protected data from which it was derived remains unaffected.

#### **Requirement to apply for a specific warrant for BPDs containing protected data**

13.17 Where, to the best of the relevant Security and Intelligence Agency's knowledge or belief (and having regard to paragraph 13.7 above), it considers it likely that a BPD contains any protected data, it must apply for a specific warrant.

13.18 As required by section 188, the application for a specific BPD warrant in such a case must include:

- a description of the specific dataset to which the application relates; and
- the "operational purposes" for which the relevant Security and Intelligence Agency wishes to examine the BPD.

#### **Additional range of factors to be included in the specific BPD warrant application**

13.19 In addition, the warrant application in a case falling within paragraph 13.17 above should also contain as much information, and be as specific as is practically possible, in relation to the protected data in the BPD, including **the nature and type of the data and any other factors that may be relevant when assessing the level of intrusiveness of the protected data**. This is with a view to ensuring that the Secretary of State can:

- assess whether the safeguards in section 202 are adequate and sufficient for the selection for examination of protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection; and

- if the safeguards in section 202 are not sufficient, attach conditions to the warrant in accordance with section xx of the Act.

13.20 In particular, without prejudice to the generality of the foregoing, the application for a specific warrant in such a case should include (so far as reasonably practicable) the following specific information:

- a description of the structure and scope of the dataset and of the information contained within it, including the different data involved and the nature and categories of data captured in those data, and, in particular, whether those data are legally privileged<sup>2</sup>;
- a description, to include as much detail as is practically possible, of the nature and extent of the data which, following the relevant Agency's initial examination of the dataset, it is known or believed may contain protected data;
- whether any of the protected data are the contents of e-mails, letters or other documents;
- whether any of the protected data contain communications between a member of a relevant legislature (as defined in sections 26 and 106) and another person on constituency matters or other parliamentary business;
- any other factors that may be relevant to the Secretary of State's assessment of the level of intrusiveness of the protected data in the BPD (and therefore of the adequacy of the section 202 safeguards), including the extent of the expectation of privacy arising from the circumstances and context in which the protected data were included in the BPD;
- the Agency's assessment of whether, having regard to the above factors, the specific warrant should be issued unconditionally or only subject to such conditions as may be approved by the Secretary of State.

#### Authorising specific warrants for BPDs containing protected data

13.21 When considering a warrant application for any dataset falling within paragraph 13.17 above, the Secretary of State must determine, in the light of the **range of factors** set out in paragraphs 13.19 and 13.20 above, whether the Secretary of State is satisfied that the selection for examination safeguards set out in section 202 would be adequate and sufficient for the selection for examination of the protected data in the dataset relating to an individual known to be in the British Islands at the time of the selection. The section 202 safeguards are likely to be adequate and sufficient to provide the necessary Article 8 protections in cases where the BPD comprises a dataset containing a relatively small number of protected data of a low level of intrusiveness (for example, protected data contained in a travel BPD provided by a prospective traveller to a service provider or in an internet dataset with minimal privacy settings which is accessible by a very large user group).

13.22 Where the Secretary of State is so satisfied, the Secretary of State may issue the warrant without conditions.

---

<sup>2</sup> The additional safeguards that apply when a Security and Intelligence Agency wishes to select for examination legally protected fields are set out in Chapter 7 of this Code.

13.23 Where the Secretary of State is not so satisfied, but would otherwise be minded to issue the warrant (subject to the approval of the Judicial Commissioner), the Secretary of State may by virtue of the power conferred by section xxx of the Act **attach conditions** to the issue of the warrant in the way set out in paragraphs 13.24 to 13.27 below. In cases where the dataset contains the contents of letters, e-mails and documents, the Secretary of State will ordinarily require the Agency to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

#### **Conditions which may be attached to the warrant in the exercise of the Secretary of State's discretion**

13.24 In cases falling within paragraph 13.21 above, pursuant to the power conferred by section xxx of the Act, the Secretary of State may attach conditions to the issue of the warrant, in the exercise of the Secretary of State's discretion, up to, and including, a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner when:

- the relevant Agency wishes to select for examination any protected data contained in the BPD using criteria referable to an individual known to be in the British Islands at that time, and
- the purpose of using those criteria is to identify protected data relating to that individual.

13.25 The conditions that may be attached to the warrant by the Secretary of State in accordance with paragraph 13.24 may also include (as an alternative to the requirement referred to in paragraph 13.24) such requirement or requirements as the relevant Security and Intelligence Agency may suggest and which the Secretary of State agrees are appropriate. These may include – but are not limited to – one or more of the following requirements:

- to seek the prior approval of a senior manager in the relevant Security and Intelligence Agency and, if the Secretary of State considers appropriate, subject to the condition that the senior manager in question is independent of the investigation, operation or analytic work to which the selection for examination relates;
- to seek the prior approval of a senior official in the Secretary of State's Department; or
- a prohibition on selecting for examination any protected fields in the BPD using criteria referable to an individual known to be in the British Islands at the time of the selection (and a determination, on that basis, that the section 202 safeguards are adequate and sufficient).

13.26 Where the dataset contains protected data of differing levels of intrusiveness, and the Secretary of State considers that only some of those data require the additional controls, the Secretary of State may choose either (a) to apply the additional controls only to those data which require the additional controls or (b) to apply the additional controls to all the protected data contained in the dataset.



13.27 An approval for the purposes of paragraph 13.24 or paragraph 13.25 need not relate to a particular person or organisation. For example, an authorisation may cover a group who share a common purpose or who are carrying on a particular activity, or may relate to more than person where the authorisation is given for the purposes of a single operation or investigation.

#### **Renewals of specific BPD warrants issued unconditionally**

13.28 When applying for **the renewal of a specific BPD warrant** issued without conditions, the relevant Security and Intelligence Agency should report to the Secretary of State on the extent to which any protected data in the dataset have, since the issue or last renewal of the warrant, been selected for examination using criteria referable to an individual known to be in the British Islands at that time.

13.29 In cases where the Secretary of State is minded to renew such a warrant, the Secretary of State may either (a) renew the specific BPD warrant, or (b) approve the retention of the BPD as part of a class BPD warrant. Each time such a class BPD warrant is subsequently renewed, the relevant Security and Intelligence Agency should, so far as is reasonably practicable, report to the Secretary of State on the frequency with which protected data in the dataset has, since the issue or last renewal of the warrant, been selected for examination using criteria referable to an individual known to be in the British Islands at that time.

#### **BPDs containing unanticipated protected data**

13.30 It is possible that cases may occasionally arise where an agency discovers, following the selection for examination of data contained in a BPD retained pursuant to a BPD warrant, that the BPD contains protected data fields which were not identified as protected at the time of the initial examination or where there was an urgent need to issue the warrant. Where such cases arise, the Agency must apply for a specific BPD warrant as soon as possible in accordance with the procedure set out at paragraphs 13.17 to 13.27. The Agency must also ensure, as soon as reasonably practicable, that any selection for examination of the protected data in the BPD using criteria referable to an individual known to be in the British Islands ceases, until such time as the specific BPD warrant has been issued.



## Safeguards

*New sentence to be added to the end of paragraph 7.9:*

13.31 The Agencies should also ensure that SIA staff, when undertaking such searches, comply with the additional safeguards set out below relating to Members of Parliament, legally privileged material and journalistic material.

*For insertion after the section in chapter 7 titled 'Additional access safeguards for confidential information relating to sensitive professions':*

### **Selection for examination of protected data relating to a Member of Parliament**

13.32 These paragraphs apply where:

- A Security and Intelligence Agency wishes to search a BPD retained pursuant to a specific BPD warrant and the purpose of the search is to select for examination protected data relating to a member of a relevant legislature; and
- the specific warrant has been issued subject to a requirement to obtain the prior written approval of the Secretary of State and the Judicial Commissioner.

13.33 Where these paragraphs apply, the Agency must have obtained the prior approval of the Prime Minister to target the member of the legislature. Prior approval must be obtained regardless of whether the member of the relevant legislature is inside or outside the British Islands at the time of the selection for examination.

13.34 "Member of a relevant legislature" for these purposes has the meaning given in sections 26 and 106 of the Act.

### **Material subject to legal privilege**

13.35 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, the definition of matters subject to legal privilege contained in section 412 of the Proceeds of Crime Act 2002 should be applied. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.

13.36 Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged material will lose its protection if, for example, the professional legal adviser is intending to hold or use the material for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal

privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

- 13.37 For the purposes of this Code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the items do not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the ‘furthering a criminal purpose’ exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether the material is not subject to legal privilege due to the “in furtherance of a criminal purpose” exception, advice should be sought from a legal adviser within the relevant Security and Intelligence Agency.
- 13.38 Selecting legally privileged protected material for examination is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The selection for examination of legally privileged protected data contained in BPDs (whether deliberately or otherwise) is therefore subject to the additional safeguards set out in paragraph 13.39 and subsequent paragraphs of this Code. The guidance set out may in part depend on whether the legally privileged protected data have been selected intentionally or incidentally to other data which have been sought.

## Selection of legally privileged protected fields for examination

- 13.39 These paragraphs apply where a Security and Intelligence Agency wishes to search a BPD and:
- the purpose, or one of the purposes of the search, is to select for examination protected data subject to legal privilege, or
  - the use of the relevant search criteria is likely to identify such data.
- 13.40 Where these paragraphs apply (and without prejudice to Chapter 4 of this Code), the Agency is prohibited from carrying out the search unless prior approval has been given by a relevant approver. The relevant approver in the case of a search relating to an individual known to be in the British Islands at the time of the selection is the Secretary of State, subject to the approval of the Judicial Commissioner. In any other case, the relevant approver is a senior official (who must not be a member of the Security and Intelligence Agencies).
- 13.41 Before carrying out the search, the Agency must notify the relevant approver. Where the use of the search criteria is likely to identify legally privileged protected data, the notification to the senior official should include, in addition to the reasons why it is considered necessary for the selection for examination to take place, an assessment of how likely it is that legally privileged protected data will be selected. In addition, the notification should state whether the purpose, or one of the purposes of the search, is to select

for examination legally privileged protected data. Where the intention is not to identify legally privileged protected data, but it is likely that such data will nevertheless be selected, that should be made clear in the notification, and the Agency should confirm that any inadvertently obtained privileged data will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to those data.

- 13.42 On receiving the notification, the relevant approver must decide whether to give an approval for the search to be carried out. The relevant approver may give an approval only if:
- the approver considers that the arrangements made for the purposes of section 188(6)(d) include specific arrangements for the handling, retention, use and destruction of legally privileged protected data, and
  - where the first bullet of paragraph 13.39 applies, the approver considers that there are exceptional and compelling circumstances that make it necessary to authorise the search. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or in the interests of national security, and the selection for examination is reasonably regarded as likely to yield intelligence necessary to counter the threat.
- 13.43 In the event that legally privileged protected data are inadvertently and unexpectedly selected for examination (and where the enhanced procedure set out above has consequently not been followed), any protected data so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged protected data may be intentionally selected for examination by reference to the relevant search criteria unless approved by the relevant approver as set out in paragraph 13.42.

## Handling, retention and deletion

- 13.44 Officials who examine protected data contained in BPDs should be alert to any data which may be subject to legal privilege.
- 13.45 Where it is discovered that legally privileged protected data have been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain them. If not, the protected data should be securely destroyed as soon as possible.
- 13.46 Where protected data have been identified following examination as legally privileged, and are recorded and retained separately from the bulk personal dataset for purposes other than their destruction they should be clearly marked as subject to legal privilege. Such data should be retained only where it is necessary and proportionate to do so. It must be securely destroyed when its retention is no longer needed for the authorised statutory purposes. If such data are retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for those purposes.

## Dissemination

- 13.47 Protected data subject to legal privilege must not be acted on or further disseminated unless a legal adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.
- 13.48 The dissemination of legally privileged protected data to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged protected data held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged protected data in order to gain a litigation advantage over another party in legal proceedings.
- 13.49 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or policy officials with conduct of legal proceedings should not see legally privileged protected data relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such content could yield a litigation advantage, the direction of the Court must be sought.

## Reporting to the Commissioner

- 13.50 In those cases where legally privileged protected data following their examination are recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant Agency must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any legally privileged protected data that are still being retained should be made available to the Commissioner on request, including detail of whether those data have been disseminated.

## Selection for examination of confidential journalistic protected data

- 13.51 Confidential journalistic protected data are data in a BPD that contain data acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

- 13.52 Where the intention is to select for examination confidential journalistic protected data, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the selection for examination of confidential journalistic protected data is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the Security and Intelligence Agency.
- 13.53 Confidential journalistic protected data which have been identified as such should be retained only where it is necessary and proportionate to do so for. It must be securely destroyed when its retention is no longer needed for those purposes. If such data are retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate.
- 13.54 Where confidential journalistic protected data have been identified in a bulk personal dataset following their examination, they should be retained only where it is necessary and proportionate to do so. In those cases where such data are recorded and retained separately from the dataset for purposes other than their destruction or are disseminated to an outside body, all reasonable steps should be taken to protect the confidentiality of the data. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential journalistic protected data, advice should be sought from a legal adviser within the Security and Intelligence Agency and before any further dissemination of the content takes place.
- 13.55 In any case where confidential journalistic protected data following their examination are recorded and retained separately from the bulk personal dataset for purposes other than their destruction, the relevant agency must inform the Investigatory Powers Commissioner as soon as is reasonably practicable, as agreed with the Commissioner. Any data which has been retained should be made available to the Commissioner on request.