Home Office

Bulk Personal Datasets: Low or no reasonable expectation of privacy

Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act 2016

[Draft for consultation]

Contents

1. Introduction

1.1. This Code of Practice relates to the exercise of functions conferred by virtue of Part 7A of the Investigatory Powers Act 2016 ("the Act"). It should be read alongside Part 7 and Part 7A of the Act and the explanatory notes. It provides guidance on the procedures that must be followed when the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the intelligence services") wishes to exercise the powers in Part 7A to retain, or to retain and examine, bulk personal datasets that have a low or no reasonable expectation of privacy ("low/no BPD"). This Code of Practice is intended for use by the intelligence services.

1.2. The Act provides that all codes of practice issued under Schedule 7 to the Act are admissible as evidence in criminal and civil proceedings. If any provision of this Code appears relevant to any court or tribunal considering any such proceedings, the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and functions conferred by the Act, it may be taken into account.

1.3. For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an intelligence service's internal advice or guidance.

1.4. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

1.5. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the intelligence services seek to obtain personal information about a person by selecting for examination from bulk personal datasets. Other rights may also be engaged, such as the right to freedom of expression (Article 10).

1.6. Persons with access to low/no BPDs 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 where systems or policies are updated.

2. Scope and definitions

2.1. The Act defines a bulk personal dataset (BPD) as a set of information that 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 intelligence services in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.

2.2. The Act provides for three regimes for the intelligence services' examination of BPD. The authorisation processes, safeguards and oversight differ based on the particular circumstances of the dataset, including the level of sensitivity and how it is accessed by an intelligence service. The three parts of the Act are:

- **Part 7**, which makes provision for the retention and examination of BPDs by an intelligence service where the BPD is held electronically for analysis in the exercise of the service's functions.
- **Part 7A**, which makes provision for the retention and examination of BPDs by an intelligence service where it is considered that the individuals to whom the data relates could have a low or no reasonable expectation of privacy in relation to the data (low/no BPD) and where it is held electronically for analysis in the exercise of the service's functions.
- **Part 7B**, which is concerned with circumstances in which a BPD is not retained by an intelligence service but is instead retained by a third party. It provides a statutory framework by means of which an intelligence service can examine a third party BPD (3PD) in situ, rather than retaining the BPD itself.

2.3. **This Code of Practice is concerned with datasets retained or retained for examination under Part 7A of the Act.** Separate statutory codes of practice provide specific guidance on intelligence service use of datasets under Part 7 and Part 7B of the Act and should be referred to accordingly.

2.4. Part 7 of the Act is concerned with the retention and examination of BPDs generally. Where the nature of the BPD is such that the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to the data then an intelligence service may choose not to apply Part 7 and instead deal with the BPD under Part 7A. For example, this might include (but is not limited to) a dataset published on the internet consisting of a collection of news articles published subject to professional standards and editorial control. In this Code, these BPD are called "low/no BPD".

Initial examination

2.5. Section 199 of the Act specifies that an intelligence service "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 holds the BPD electronically for analysis in the exercise of those functions. Section 199 applies equally to low/no BPD.

2.6. Section 220 of the Act sets out a process of initial examination which is carried out by an intelligence service when it obtains a set of information. This is a process by means of which the intelligence service: (a) decides whether, if it were to retain the set of information and hold it electronically for analysis in the exercise of its functions, it would be retaining a BPD, (b) if so, whether to retain it, and (c) if it is to be retained, whether it is to be retained pursuant to a warrant issued under Part 7, or an individual authorisation granted under Part 7A. If the BPD is to be retained pursuant to a warrant issued under Part 7, then the intelligence service must go on to decide whether the BPD may be retained pursuant to an existing class BPD warrant, or whether a specific BPD warrant must be sought.

2.7. This initial examination may only be carried out by an intelligence service for these limited purposes. An intelligence service can examine a dataset during the initial examination period if such examination is necessary to determine whether to retain the dataset and, where necessary, to apply for a Part 7 warrant or grant a Part 7A authorisation. However, the BPD may not be examined for the purposes of any intelligence service's investigations or operations until the necessary authorisation is in place.

2.8. An initial examination can include processing a set of information so that it no longer meets the definition of a BPD and the requirement for authorisation no longer applies(e.g. by deleting information from the set so that the majority of the information remaining relates to individuals who are of potential interest to the intelligence services). In some circumstances, processing of this nature results in the creation from the set of information of one or more new targeted datasets. Any new targeted dataset, which does not meet the definition of a BPD, can be used for intelligence investigations or operations whether or not the original set of information from which it was derived is subsequently retained or deleted.

2.9. As part of the initial examination, an intelligence service may also carry out any technical work necessary to enable a dataset to be used as soon as its retention and examination has been authorised.

2.10. The initial examination should be completed as soon as reasonably practicable and, in any event, within the "permitted period". For a set of information created outside the UK, the permitted period lasts six months; for a set created in the UK, the permitted period lasts three months.

2.11. The permitted period begins on the day after the date on which the Head of the intelligence service (or a person acting on their behalf) forms the belief that the set

includes (or may include) personal data about a number of individuals, the majority of whom are not and are unlikely to become of intelligence interest.

2.12. Some preliminary processing of the set of information may be necessary before the permitted period begins so that the intelligence service is able to access the set of information in a form that enables the necessary belief to be formed. For example: (i) the set of information may need physically to be brought back to the UK from overseas; (ii) the set may require translation from a foreign language; (iii) the set may be part of a much larger set of information from which it needs to be separated, (iv) the set may require decryption, or there may be other technical barriers such as complex formatting to be addressed.

2.13. Once a decision has been made to seek a specific BPD warrant under Part 7 or to grant an individual authorisation under Part 7A, the intelligence service may continue to retain the dataset pending the approval by a Judicial Commissioner (if required) of that decision. This is particularly relevant in circumstances in which an intelligence service has received an unsolicited set of information (i.e. one which the recipient intelligence service has not requested or sought to obtain). In those circumstances the intelligence service will not have had the opportunity, before receiving the set of information, to consider whether the set would be a BPD and, if so, then how its retention and examination would be authorised. It will also be relevant in circumstances in which a solicited set of information is obtained which contains unexpected material. In both cases, the relevant intelligence service should complete the initial examination and apply for the relevant warrant or authorisation within the permitted period.

Personal data

2.14. For the purposes of Part 7 of the Act, 'personal data' has the meaning given to it in section 3(2) of the Data Protection Act 2018 ("DPA" – see also Annex A, from paragraph 7 onwards) and extends that definition to include data relating to deceased individuals where such data would fall within section 3(2) of DPA if it related to a living individual.

2.15. BPDs can contain details about individuals who are deceased. 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.

2.16. This means that even if a BPD consists exclusively of information about individuals who are known to be deceased, the retention of that dataset by an intelligence service for analysis in the exercise of its functions must still be authorised by a Part 7 warrant or a Part 7A authorisation.[1]

[1] Whether a particular dataset should be held under Part 7 or Part 7A will require consideration of the specific facts of the case.

Different statutory routes by which BPDs may be acquired

2.17. The intelligence services 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 1 and subsequent paragraphs of Annex A) and through the exercise of various existing statutory powers.

2.18. This Code of Practice applies not only to BPDs obtained under the information gateway provisions, but also to BPDs where the mechanism for obtaining the datasets is subject to authorisation through the exercise of other statutory powers.

2.19. These other statutory powers include, but are not limited to, (i) warrants issued under section 5 of ISA in respect of property interference; (ii) intrusive surveillance warrants issued under section 32 of the Regulation of Investigatory Powers Act 2000 ('RIPA'); (iii) directed surveillance authorisations issued under section 28 of RIPA; and (iv) 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 or codes of practice relevant to the exercise of those statutory powers.

2.20. Subject to the following paragraph, and for the avoidance of doubt, this Code of Practice does not apply to datasets obtained by an intelligence service when it is exercising a power under a warrant or other authorisation issued or given under the Investigatory Powers Act 2016, for example, warrants under Part 2 (lawful interception of communications), Part 5 (equipment interference) or Part 6 (bulk warrants). Datasets 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 3.6).

2.21. This Code of Practice will apply to such datasets if they are subject to a direction given by the Secretary of State under section 225 of the Act. A section 225 direction brings a dataset obtained under IPA powers within scope of Part 7 or Part 7A, as the case may be. A section 225 direction may be given on the application of the head of an intelligence service (or a person acting on their behalf) and must be approved by a Judicial Commissioner. See section 225 and paragraph 3.8 and subsequent paragraphs.

3. Low/no BPDs – general rules

Requirement for authorisation

3.1. Part 7 of the Act, together with Part 7A, regulates the retention and examination of bulk personal datasets. These parts of the Act provide for an authorisation scheme and a comprehensive set of robust, transparent and proportionate safeguards. Specifically, section 200 of the Act provides that an intelligence service may not exercise a power to retain or examine a BPD unless this is authorised by a warrant under Part 7 or authorisation under Part 7A of the Act.

3.2. This Code is concerned only with the provisions of Part 7A and the authorisations issued under it. Part 7 and warrants granted under that Part are covered in a separate code.

Types of authorisation that may be granted

3.3. Section 226B of the Act describes the principal type of authorisation provided for by Part 7A: an 'individual authorisation' authorising an intelligence service to retain, or to retain and examine, the low/no BPD described in the authorisation. An individual authorisation is always required to retain, or retain and examine, a low/no BPD.

3.4. Section 226BA of the Act describes a 'category authorisation'. Category authorisations determine whether the intelligence service must seek prior approval from a Judicial Commissioner when deciding to grant an individual authorisation. For further detail, see paragraph 5.8.

3.5. If, in the course of examining a third party dataset pursuant to a Part 7B warrant, the intelligence service obtains, and subsequently wishes to retain, data that itself constitutes a BPD, the intelligence service would need to apply for a BPD warrant to retain or retain and examine that BPD under Part 7 or Part 7A of the Act as appropriate.

Exception to general requirement for authorisation

3.6. Section 201 of the Act explains the specific circumstances in which the general requirement for authorisation under section 200 does not apply.

3.7. Section 201(1) provides that the Part 7 and Part 7A authorisation scheme does not apply to BPD when this is obtained by an intelligence service by the exercise of **other** powers under the Act (Part 7B notwithstanding, see paragraph 3.5) – for example, under a targeted or bulk interception or equipment interference warrant or under a bulk acquisition warrant (for bulk communications data). An example of this might be where an email had been intercepted and attached to the email is a file

containing a set of information that would otherwise amount to a BPD . In such cases, the retention and examination of that file will be governed by the applicable regime under the relevant part of the Act – for example, the interception regime where it was obtained as a result of interception.

3.8. However, under section 225 of the Act, an intelligence service can apply to the Secretary of State for a direction that a dataset obtained by it under a targeted or bulk interception or equipment interference warrant should have the provisions relating to that other regime disapplied, and the provisions of Part 7 or Part 7A 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.

3.9. In circumstances where the Head of an intelligence service, or a person acting on their behalf, makes an application for a direction under section 225 for Part 7A provisions to be applied, consideration should also be given to whether to decide to grant an individual authorisation under Part 7A. An application for an individual authorisation may be made if the nature of the BPD which is subject to the direction is a BPD that falls within the Part 7A regime.

3.10. In giving any direction, the Secretary of State is permitted to provide that any of the associated Investigatory Powers Act regulatory provisions which applied to the regime under which the BPD was obtained should continue to apply once the direction has been given (with or without modifications). Therefore, in making an application for a direction, an intelligence service 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.

3.11. 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 56 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act 2005 proceedings (see section 225(6)(a)). Nor may such a direction disapply sections 57-59 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 225(6)(b)).

3.12. Section 201(2) of the Act 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 intelligence service to hold, temporarily, a BPD which is no longer authorised by a Part 7 warrant or Part 7A authorisation for the purpose only of ensuring that the relevant data is removed from their systems. If a Part 7A authorisation is cancelled or otherwise not renewed, it will not always be possible for the intelligence service 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.

3.13. Section 201(3) of the Act makes clear that other sections of Part 7 and Part 7A also provide for exceptions from the requirement to obtain a warrant or authorisation in particular circumstances. For the purposes of Part 7A, these relate: to a time-limited period in which an intelligence service is conducting an initial examination of a potential BPD (section 220(6) – see paragraph 2.6 and subsequent paragraphs); and to a limited period after the non-renewal or cancellation of a warrant (section 226CC – see paragraph 5.49 and subsequent paragraphs).

3.14. Section 2 of the Act requires a public authority to have regard to the following when issuing, renewing or cancelling an authorisation under Part 7A:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means;
- whether the level of protection to be applied in relation to any obtaining of information by virtue of the authorisation is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems, and
- any other aspects of the public interest in the protection of privacy.

4. Low/no BPD authorisations

4.1. Low/no BPD authorisations are granted by the relevant Head of an intelligence service, or a person acting on their behalf:

- The Director General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).

4.2. The normal rule is that the decision to grant an individual authorisation is subject to prior approval by a Judicial Commissioner (see paragraph 5.21 and subsequent paragraphs). There are two exceptions:

a. First, if the person granting the individual authorisation considers that the BPD in question falls within an existing category authorisation.

b. Secondly, if the person granting the individual authorisation considers that there is an urgent need to do so (see paragraph 5.29 and subsequent paragraphs).

4.3. In urgent cases, an individual authorisation may be granted without the prior approval of a Judicial Commissioner where there is an urgent need to do so. The relevant intelligence service can therefore retain and examine the dataset for a limited period while awaiting the decision of a Judicial Commissioner to approve the granting of the urgent individual authorisation.

4.4. All Part 7A category authorisations granted by, or on behalf of, the above persons must be approved by a Judicial Commissioner (see paragraph 5.21 and subsequent paragraphs) before that category authorisation is relied upon for any subsequent individual authorisations.

4.5. In deciding whether to approve a decision to grant an authorisation, a Judicial Commissioner must review the conclusions of the person who granted the authorisation as to whether the low/no test (set out in section 226A of the Act) applies to the dataset described in the application.

4.6. When completing an application for an individual authorisation, the intelligence service must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular all reasonable efforts should be made to take account of information which weakens the case for the authorisation.

4.7. Where it is intended to make access to the BPD (or BPDs) retained under the authorisation available to any domestic or international partner, consideration of this should be included in the application.

4.8. There may be circumstances in which a Head of an intelligence service, or person acting on their behalf, considers it appropriate to grant a category authorisation before the intelligence service has acquired, and retained, any BPDs that might fall within the category authorised by the category authorisation.

The test and the factors

4.9. Section 226A(1) of the Act contains the test that must be met before the retention, or retention and examination, of a BPD can be authorised under Part 7A. The test is that the nature of the bulk personal dataset is such that the individuals to whom the bulk personal dataset relates could have no, or only a low, reasonable expectation of privacy.

4.10. The nature of the dataset is a broad concept that includes the inherent quality of the data in the dataset but necessarily extends beyond that to consider the wider circumstances insofar as relevant to the test in subsection (1). As subsection (2) makes clear, in addition to the factors set out in subsection (3), regard must be had to all of the circumstances. This enables regard to be had to factors beyond those listed in subsection (3) insofar as germane to a particular dataset. In every case, regard must be had to the factors set out in subsection (3) in particular.

The reasonable expectation of privacy test

4.11. The test is framed around the concept of "reasonable expectation of privacy" because this is the jurisprudential touchstone for the engagement of the right to a private and family life in Article 8 of the European Convention on Human Rights.

4.12. The test is necessarily context-specific and involves the application of judgement depending on the circumstances. This reflects the jurisprudence on Article 8. There are no objective criteria that can be applied to every conceivable circumstance or a "one size fits all" test.

Applying the factors

4.13. The factors in section 226A(3) of the Act are intended to assist the decision-maker in assessing the expectation of privacy. The factors do not themselves constitute pass or fail tests that must be met. When having regard to the factors, the following guidance applies:

- The factors are non-exhaustive and a decision-maker may take into account considerations that are not included in the list of factors. For example, the location from which the data originates or the use to which the data is to be put – see paragraphs 4.13 and subsequent paragraphs.

- Even if one or more factors is relevant or applicable, it does not automatically follow that a dataset is a low/no dataset. There may be datasets in respect of which one or more of the factors are relevant and applicable but, once regard has been had to all the circumstances, it cannot be said that there is only a low or no reasonable expectation of privacy.

- There is no requirement that one or more of the factors must be relevant or applicable before a dataset is a low/no dataset.

- It follows from the above that it is also not necessary for all the factors to be relevant or applicable in order for a dataset to be a low/no dataset.

4.14. It is expected that most of the time reliance on one or more of the factors will provide a sufficient basis on which to draw the conclusion that the dataset in question has low or no reasonable expectation of privacy.

4.15. The following list of hypothetical examples is intended to illustrate how the factors might be relevant in practice:

4.16. Factor (a) is 'the nature of the data'. This might be relied upon to reach a conclusion that there is a low, or no expectation of privacy where the type of information contained in a dataset patently does not give rise to an expectation of privacy: for example, a public telephone directory.

4.17. Factor (b) is 'the extent to which (i) the data has been made public by the individuals, or (ii) the individuals have consented to the data being made public'. This might be relied upon if the dataset consists of a set of responses to a survey, where the participants had provided genuine consent to taking part and knew the results would be published.

4.18. Factor (c) is relevant if the data has been published, and is 'the extent to which it was published subject to editorial control or by a person acting in accordance with editorial standards'. This might be relied upon if the dataset consists of a set of news articles where a level of responsible review and scrutiny has already been applied to the dataset.

4.19. Factor (d) is relevant if the data has been published or is otherwise in the public domain, and is 'the extent to which the data is widely known about'. This might be relied upon if the dataset had been publicly disclosed following legal proceedings, and thus had both been published and discussed as part of those legal proceedings.

4.20. Factor (e) is the extent to which the data has already been used in the public domain. This might be relied upon if the dataset has been widely used by industry or academia – for example in data science – and as a consequence it can be judged that the dataset has low or no reasonable expectation of privacy.

4.21. A decision-maker must have regard to all the circumstances when applying the test in 226A(1). As set out at paragraph 4.10, this can include considerations that are not included in the list of factors in section 226A(3). For example, the reasonable expectation of privacy may vary depending on the jurisdiction that the data originates from or the use to which the dataset will be put.

4.22. In some countries different types of data are treated as private or non-private depending on the laws of that country (such as company ownership or land ownership information). Furthermore, in some countries it is commonplace for data on citizens' lives to be regularly and routinely accessed at scale. For example, datasets containing personal data may be made available, either for free or for a payment, on public forums. This will be a relevant consideration when deciding whether section 226A applies.

4.23. Where the intelligence service assesses that the jurisdiction from which the data originates is a relevant factor in determining the expectation of privacy, this should be made clear and justified in the individual or category authorisation.

4.24. Another example of what might be considered when having regard to all the circumstances when applying the test in 226A(1), is the use to which the data will be put. In many cases, the use to which the dataset will be put will not be a relevant consideration, as other factors will carry more weight in determining whether there is a low or no, reasonable expectation of privacy in relation to the data.

4.25. However, in some cases, the use to which the data will be put may have an impact on the assessment of reasonable expectation of privacy: for example, when using data for capability development such as building and testing machine learning models. This may mean that some data that would not routinely be assessed as having a low reasonable expectation of privacy may come within scope of Part 7A if the sole use of the data will be for capability development.

4.26. Where the intelligence service assesses that the use to which the data is being put is a relevant factor in determining the reasonable expectation of privacy, this should be made clear and justified in the individual or category authorisation.

Requirements to be met by applications

4.27. Any application for an individual authorisation must include the following:

- a description of the dataset to which the application relates;
- why it is considered that the test in section 226A applies to the dataset;
- whether the authorisation is sought for retention or retention and examination;
- the operational and legal justification for retention or retention and examination of the dataset, including the use to which the dataset will be put, the statutory functions which are engaged and the necessity and proportionality of the proposed retention or retention and examination;
- any consideration and advice of legal advisers, where appropriate; and
- the extent of any political, reputational or other risk, so far as may be relevant.

4.28. Any application for a category authorisation must include the following:

- a description of the category to which the application relates;
- why it is considered that the test in section 226A applies to data that is to be added to the category.

BPDs containing information of particular sensitivity

4.29. Part 7A regulates only those BPDs to which section 226A of the Act applies. Conduct in respect of a BPD that does not meet the test in section 226A(1) cannot be authorised under Part 7A and must, if it is to be authorised, be authorised by a warrant under Part 7. By its nature therefore, a BPD that is retained and examined under Part 7A is highly unlikely to contain information of particular sensitivity.

4.30. Examples of information of particular sensitivity include: a substantial proportion of sensitive personal data, health records, or confidential material relating to sensitive professions.

4.31. A low/no BPD could contain sensitive personal data (see section 202), health records, or confidential material relating to sensitive professions, but only where the information is no longer sensitive. For example, a communication between a lawyer and client might have become public in circumstances in which it has lost its necessary quality of confidence: a dataset containing this type of information could meet the test in section 226A(1) and be retained in a low/no BPD.

4.32. Given the nature of the datasets that may be retained and examined under Part 7A, it may not be practicable to establish during the permitted period of initial examination that all of the data in a dataset meets the test in section 226A(1), and a proportionate approach should be taken, particularly where, for example, a dataset is very large and an exhaustive examination is not feasible. It is therefore possible that datasets authorised under Part 7A may contain a relatively small amount of data in respect of which there is more than a low reasonable expectation of privacy.

4.33. The presence of this data, in very small amounts, would not necessarily alter the overall expectation of privacy of a dataset as a whole, given the procedures that are to be followed should the data be identified (see paragraph 4.34). However, where the presence of this type of data is suspected at the time of the application for authorisation, this information should be included in the authorisation application, together with an explanation as to why it is necessary to retain the data and any proposed safeguards concerning examination of it. Such safeguards could include that there is no intention to search the dataset deliberately to select such information.

4.34. Where information of particular sensitivity is not known to be in a dataset at the time the authorisation is granted but is subsequently discovered, then section 226D contains a mechanism to ensure that this information is handled appropriately. In the event that an analyst in the course of examining a dataset discovers information in respect of which there is more than a low, or no, expectation of privacy, the relevant intelligence service must take certain steps. The intelligence service should consider whether the presence of that information means that section 226A (low or no reasonable expectation of privacy) does not apply, or no longer applies, to part of the dataset. If it is considered that 226A no longer applies, the following process under section 226D must be followed. First, the Head of the intelligence service must ensure that anything in the process of being done in relation to that data is stopped as soon as is reasonably practicable. The intelligence service must then treat that part of the low/no BPD as if the relevant authorisation had been cancelled. The relevant information must be removed from the low/no dataset and either deleted or a Part 7 warrant sought in respect of that information.

4.35. If the discovery alters the overall assessment of the expectation of privacy in respect of the dataset, the low/no BPD authorisation must be cancelled as the requirement in section 226B(4)(a) is no longer met. Section 226C (non-renewal or cancellation of an individual authorisation) will apply and the dataset must either be deleted or a warrant sought under Part 7.

Protected Data

4.36. The Part 7 regime contains special protections for “protected data”, defined in Section 203 of the Act. Part 7 contains a scheme that enables the Secretary of State to impose additional protections for protected data, which apply on a dataset-by-dataset basis, having regard to factors including the nature and intrusiveness of the protected data in the dataset.

4.37. Datasets retained and examined under Part 7A will, by their nature, have been considered not to include private information of the kind that the protected data provisions are intended to protect, and so the concept of protected data is not replicated in Part 7A.

5. Authorisation of individual and category authorisations

Individual authorisations

5.1. An individual authorisation permits the relevant intelligence service to retain, or retain and examine, a BPD described in the authorisation.

5.2. Before deciding to retain a BPD under Part 7A for the purpose of the exercise of its statutory functions, the intelligence service must be satisfied that:

- The test in section 226A(1) applies to the dataset;
- the authorisation is necessary for one or more of the relevant intelligence service's statutory functions;
- retaining or retaining and examining the low/no BPD in question is proportionate to what is sought to be achieved by doing so;
- only as much information will be retained 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.

5.3. Section 2 of the Act (general duties in relation to privacy) requires the person granting the authorisation to have regard to the following when granting, renewing, or cancelling an authorisation:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means,
- whether the level of protection applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of that information, and
- any other aspects of the public interest in the protection of privacy.[2]

5.4. An intelligence service should specify in the application, when applying for an individual authorisation in respect of a particular BPD ('dataset A'), if it also wishes the authorisation to extend to the retention and use of **'replacement datasets'** or updates to the dataset, i.e. other data which could reasonably be regarded as falling under the scope of the warrant.

[2] Section 2 of the Act also requires the issuing authority to have regard to the public interest in the integrity and security of telecommunication systems but the duty applies only so far as they are relevant. This would rarely be the case in the BPD context.

5.5. An explanation of the test to determine whether a dataset is a low/no BPD is provided at paragraph 4.9 and subsequent paragraphs and of necessity and proportionality is provided at paragraph 5.15 and subsequent paragraphs.

5.6. Before a new dataset is held electronically by an intelligence service for analysis in the exercise of its functions pursuant to an individual authorisation, the relevant persons with access to BPDs in that intelligence service should consider the requirements set out in paragraph 5.2 and follow the relevant internal procedure(s) for the granting of an individual authorisation.

5.7. Once the individual authorisation has been granted, the completed application should be stored as a record by the intelligence service, which will include the date of approval and expiration.

Category authorisations

5.8. A category authorisation displaces the normal rule that individual authorisations are subject to judicial approval. Where an intelligence service wishes to retain a dataset, and that dataset falls within a category authorisation, then the Head of the intelligence service (or the person acting on their behalf) may grant the individual authorisation without seeking judicial approval. Section 226B(7) of the Act allows judicial approval to nevertheless be sought if the person granting the authorisation considers that it would be appropriate to do so (e.g. where the authorisation is novel or contentious).

5.9. As specified in 226BA(3), the use to which a dataset will be put may form the basis of the description of a category authorisation, for example, a category of datasets may be described as being for the purpose of research and capability development. In such cases the dataset(s) cannot be used for other purposes, unless separately authorised.

Authorisations on behalf of the Head of an intelligence service

5.10. Part 7A provides that another Crown Servant may undertake certain activity on behalf of the Head of an intelligence service, including the granting of individual and category authorisations. Any person granting an authorisation on behalf of the Head of an intelligence service must have appropriate training regarding their professional and legal responsibilities according to the intelligence service's internal procedure(s) in order for be able to fully consider the merits or otherwise of a particular application and to be able to assess any fundamental rights implications that may arise from the proposed retention or retention and examination. The specific detail of this training is a matter for the relevant intelligence service.

5.11. A person granting an authorisation on behalf of the Head of an intelligence service should be functionally independent from the applicant seeking the authorisation. In practice this means that the person granting the authorisation should be far enough removed from the applicant's line management chain so as to not be influenced by operational imperatives.

5.12. In exceptional circumstances an intelligence service may not be able to call upon the services of a person to consider granting an authorisation who is functionally independent from the applicant seeking the authorisation. For example, where there is a significant opportunity to obtain information but the opportunity is rare or fleeting, the time to act is short, and the need to obtain the information is significant and for the purposes of the relevant intelligence service's statutory functions.

5.13. Where the person granting the authorisation is not functionally independent from the applicant, their involvement and their justification for undertaking the role of the decision maker must be explicit in their recorded considerations.

Requirements to be met when granting authorisations

5.14. When granting an individual or category authorisation for retention or retention and examination of a BPD pursuant to Part 7A, the following requirements must be documented by the decision maker:

- the date on which it was authorised or the authorisation renewed and the date on which it expires;
- the designation and office, rank or position of the person who authorised it.

Necessity and proportionality for individual authorisations

5.15. The retention or examination of a BPD pursuant to an individual authorisation will only be justifiable if it is necessary and proportionate. The Act recognises this, requiring the Head of an intelligence service (or person acting on their behalf) to consider that the authorisation is necessary for the purpose of the exercise of a function of the intelligence service.

5.16. The Head of an intelligence service (or person acting on their behalf) must also consider that the retention or examination of the BPD under a Part 7A authorisation is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of any intrusion into privacy against the need for the activity in investigative, operational or capability terms.

When will retaining or examining a BPD under Part 7A be necessary?

5.17. 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 intelligence services must consider why retaining or retaining and examining the BPD under a Part 7A authorisation is necessary for the purpose of the exercise of a function of the intelligence service.

When will retaining or examining a BPD under Part 7A be proportionate?

5.18. The retention or examination of the BPD under a Part 7A authorisation must also be proportionate to what is sought to be achieved by the conduct authorised under the authorisation. In order to meet the 'proportionality' requirement, the intelligence services must balance (a) the level of interference with the individual's right to privacy (and any other rights that might be engaged depending on the circumstances), 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 (in investigative, operational, and/or capability terms) interest, against (b) the expected value of the information or capability to be derived from the retention, or retention and examination, of the dataset.

5.19. The intelligence services must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the information or capability that is sought to be derived from the retention, or retention and examination, of the dataset. The intelligence service must also consider whether there is a reasonable and less intrusive alternative that will still meet the proposed objective.

5.20. The authorisation 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 intelligence service's investigations, operations or capabilities and should not be disproportionate or arbitrary. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

Judicial Commissioner Approval

5.21. The normal rule is that a to grant an authorisation under Part 7A requires prior approval by a Judicial Commissioner. There are two exceptions to the normal rule:

5.21.1. where a given dataset falls within an existing category authorisation:

5.21.2. where an individual authorisation is being granted on an urgent basis (in which case judicial approval must be sought after the event).[3]

5.22. Any decision to grant a category authorisation will always require prior approval by a Judicial Commissioner.

5.23. When submitting an Individual Authorisation for Judicial Commissioner approval, the Head of an intelligence service (or person acting on their behalf) must include all the required fields of an Individual Authorisation application, as detailed in paragraph 4.27, to provide the Judicial Commissioner with the necessary context to determine whether section 226(A) applies.

5.24. Section 226BB sets out that in deciding whether to approve a decision to grant an individual and/or category authorisation, a Judicial Commissioner must review the conclusions of the person who granted the authorisation in relation to whether section 226A (low or no reasonable expectation of privacy) applies:

- in the case of an individual authorisation, to the BPD described in the authorisation, or
- in the case of a category authorisation, to any dataset that falls within the category of datasets described by the authorisation.

5.25. In reviewing these matters, the Judicial Commissioner must apply judicial review principles. The Judicial Commissioner must, when carrying out the review, comply with the duties imposed by section 2 (general duties in relation to privacy) of the Act.

5.26. In accordance with the investigation and information gathering powers at section 235(2) of the Act, there is an obligation on the intelligence services to provide the Judicial Commissioner with information if the Commissioner seeks clarification in relation to an authorisation.

5.27. If the Judicial Commissioner refuses to approve the decision to grant an authorisation, the Head of an intelligence service (or person acting on their behalf) may refer the matter to the Investigatory Powers Commissioner for a decision (unless the Investigatory Powers Commissioner has made the original decision).

5.28. If the Investigatory Powers Commissioner refuses to approve the decision to grant an authorisation, there is no avenue of appeal available to the intelligence service. In such circumstances, the intelligence service may seek to obtain a warrant under Part 7 if appropriate.

[3] See the subheading below: Urgent individual authorisations

Urgent individual authorisations

5.29. Section 226BC of the Act makes provision for cases in which an individual authorisation is required urgently. It is not possible to seek an urgent category authorisation.

5.30. The Head of an intelligence service (or person acting on their behalf) must consider that there was an urgent need to grant the individual authorisation. Urgency is determined by whether it would be reasonably practicable to seek the Judicial Commissioner's approval to grant the authorisation in the requisite time. Accordingly, urgent individual authorisations can be granted by the intelligence service 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 authorisations 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 their life is in imminent danger;

- A significant intelligence-gathering opportunity, which is significant because of the nature of the potential intelligence or because the operational need for the intelligence is significant, and 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 BPDs to identify, or to rapidly develop the capability to identify, the vessel to prevent the weapons reaching the terrorist.

5.31. The Act provides that the decision by the Head of an intelligence service (or person acting on their behalf) to grant an urgent individual authorisation must be reviewed by a Judicial Commissioner within three working days following the day of issue.

5.32. If the Judicial Commissioner approves the decision to grant an urgent individual authorisation, and it is still considered necessary and proportionate by the intelligence service, renewal of the urgent individual authorisation may be sought. An individual authorisation issued under the urgency procedure lasts for five working days following the day of issue unless renewed. If it is renewed it is no longer an urgent individual authorisation and expires after 12 months.

5.33. If the Judicial Commissioner does not approve the decision to grant an urgent individual authorisation, the authorisation ceases to have effect and may not be renewed. The relevant intelligence service must do whatever is reasonably practicable to ensure that anything in the process of being done under the authorisation is stopped as soon as possible. In such a scenario, activity undertaken by virtue of that urgent authorisation remains lawful, including activity in process at the time the authorisation ceases to have effect which it is not reasonably practicable to stop.

5.34. In circumstances in which a Judicial Commissioner refuses to approve a decision to grant an authorisation, by virtue of section 226BC(7) the intelligence service may treat the BPD as set of information to which section 220 (initial examination: time limits) applies. This enables the intelligence service to examine it, to carry out limited processing of it, to decide whether it wishes to retain and examine it, and to seek the necessary authority in order to be able to do so.

Duration of authorisations

5.35. The duration of an individual or category authorisation (other than an urgent individual authorisation) is 12 months from the day it was granted, unless it is cancelled earlier.

5.36. An urgent individual authorisation lasts for five working days after the day on which it was issued.

5.37. Authorisations may only be renewed in the last 30 days of the period for which they have effect. Where an authorisation is renewed, the 12-month duration begins on the day following the day on which it would otherwise have ceased to have effect.

Renewal of authorisations

5.38. A member of an intelligence service may seek to renew an authorisation within the renewal period. In most cases the renewal period for both individual authorisations and category authorisations is 30 days ending with the day at the end of which the authorisation would otherwise cease to have effect. Urgent individual authorisations may be renewed at any point before their expiry date. For BPDs to which section 226CD applies (non-renewal or cancellation of category authorisation), the renewal period is three months ending with the day at the end of which the authorisation would otherwise have ceased to have effect.

5.39. Applications for renewals are made to the Head of an intelligence service (or person acting on their behalf) and contain an update of the matters outlined in paragraph 5.2. In particular, the applicant should explain why it continues to be necessary to retain and/or examine the BPD under an individual authorisation, and why this continues to be proportionate.

5.40. Where the Head of the intelligence service (or person acting on their behalf) is satisfied that the retention and/or examination of the BPD continues to meet the requirements of the Act, they may grant a renewal of the individual authorisation. The renewed individual authorisation is valid for 12 months from the day after the day at the end of which it would otherwise have ceased to have effect if it had not been renewed.

5.41. As with decisions to grant authorisations under Part 7A, the normal rule is that a decision by the Head of an intelligence service (or person acting on their behalf) to renew an authorisation under Part 7A requires approval by a Judicial Commissioner. That requirement does not apply where the authorisation is an individual authorisation and the BPD falls within a category authorisation.

5.42. Where a given dataset was initially authorised under an individual authorisation that required approval by a Judicial Commissioner, and the authorisation is subsequently renewed in reliance on a category authorisation, the renewal of that authorisation will not require approval by a Judicial Commissioner. For example, this may occur where an appropriate category authorisation did not exist at the time the individual authorisation was granted.

Cancellation of authorisations

5.43. The Head of an intelligence service (or person acting on their behalf) may cancel a low/no BPD authorisation at any time (see section 226CB of the Act). Such persons must cancel an individual authorisation if, at any time before its expiry date, they consider that any of the following cancellation conditions are met:

- Section 226A no longer applies to the dataset;
- the authorisation is no longer necessary for the purpose of the exercise of a function of the intelligence service;
- the conduct is no longer proportionate to what is sought to be achieved;
- the intelligence service no longer has arrangements approved by the Secretary of State for storing the low/no BPD and for protecting them from unauthorised disclosure.

5.44. The cancellation condition for category authorisations is that section 226A (low or no reasonable expectation of privacy) no longer applies to any dataset that falls within the category of datasets described in the authorisation.

5.45. The intelligence services will therefore need to keep their Part 7A authorisations under review.

5.46. The person who cancels a Part 7A authorisation does not need to be the same decision maker who granted the authorisation.

5.47. Once an individual authorisation has been cancelled then the dataset to which it relates must be removed from the relevant intelligence service's analytical systems as soon as is technically feasible and destroyed (see paragraph 6.17).

5.48. The cancellation of an authorisation does not prevent an intelligence service from granting a new authorisation covering the same or different bulk personal datasets in the future should it be considered necessary and proportionate to do so. Nor does it prevent an intelligence service from seeking, and the Secretary of State from issuing, a specific or class BPD warrant in respect of the dataset or datasets, as the case may be.

Non-renewal or cancellation of individual authorisations

5.49. Section 226CC of the Act provides for the situation where an individual authorisation is either not renewed or is cancelled and, in particular, sets out the process for dealing with the material that was retained under the authorisation in question. The material may be destroyed; section 201(2) ensures retention or examination of the material for the purpose of deleting the material is lawful (see paragraph 3.12 for further guidance).

5.50. Depending on the reasons why the authorisation has been cancelled or not renewed, the relevant intelligence service may consider it necessary and proportionate to continue to retain some or all of the material that had been retained under the authority of that authorisation. Section 226CC therefore includes bridging provisions to ensure any retention and examination of the material in question is lawful pending a new authorisation. The relevant intelligence service may apply for a new individual authorisation within five working days (section 226CC(3)).

Non-renewal or cancellation of category authorisations

5.51. Section 226CD of the Act provides for a situation where a category authorisation is either not renewed or is cancelled. In particular, it sets out the process for dealing with the individual authorisations granted in reliance on the category authorisation given that the decision to grant these individual authorisations will, in most cases,[4] not have been subject to judicial approval.

5.52. The effect of section 226CD(2) is that the duration of all individual authorisations granted in reliance on a category authorisation, and that were not approved by a Judicial Commissioner, will be extended for a period of three months beginning with the day after the day at the end of which the cancellation or non-renewal of the related category authorisation. The individual authorisations will remain valid during this period unless the authorisation is either renewed during that period or it is cancelled or otherwise ceases to have effect.

[4] The exception is where, in accordance with section 226B(7), the person granting the authorisation considered it appropriate to seek judicial approval.

5.53. This ensures that the intelligence service is able to manage in an orderly fashion the necessary reauthorisation of individual datasets following the cancellation or non-renewal of a category authorisation, ensuring that all necessary conduct continues to be subject to appropriate authorisation.

6. Safeguards

6.1. This chapter sets out the data safeguards the intelligence service should put in place in relation to the retention and examination of datasets authorised under Part 7A. The Secretary of State must be satisfied that arrangements made by the relevant intelligence service for the retention and examination of Part 7A BPD and for protecting the datasets from unauthorised disclosure are satisfactory (as set out in sections 226B(4)(d), and 226CA(2)(iv).

6.2. Datasets that are retained, or retained and examined, pursuant to an authorisation under Part 7A will be safeguarded in the following ways:

- Data will be retained/examined only for lawful, specified and legitimate purposes.
- Data will be retained/examined only for as long as it is necessary and proportionate to do so.
- In order to manage potential risks relating to unauthorised access, storage of Part 7A data will be subject to security measures that are proportionate to the nature of the data and to the intrusion associated with the retention/examination of Part 7A data.
- All copying, sharing and provision of access to data will be necessary, proportionate and carried out in relation to a statutory function and/or purpose.
- The integrity of data will be appropriately protected.
- Appropriate records will be maintained to enable effective management, governance and oversight of the retention/examination of Part 7A data.

Information of particular sensitivity

6.3. In the event that information of particular sensitivity is discovered after a BPD has been authorised pursuant to Part 7A, the relevant intelligence service must consider appropriate remedial steps, which may include one of the following:

- the individual authorisation is cancelled and the whole dataset deleted,
- the particular information is marked as to be retained for deletion only (and the remaining data continues to be authorised under Part 7A), or

- the individual authorisation is cancelled and retention/examination of the dataset is instead authorised under Part 7 (either by application for a specific BPD warrant or by adding the dataset to a suitable existing class BPD warrant, as appropriate). Until appropriate authorisation under Part 7 has been arranged, the dataset will be considered to be retained under the initial examination period as set out in section 220 of the Act.[5]

6.4. The above process is only applicable in instances where information of particular sensitivity is discovered in the course of examining a dataset.

Disclosure

6.5. For the purposes of chapter 6 of this Code, disclosure means providing a copy of a Part 7A BPD retained pursuant to an individual authorisation or information held in such a BPD to a third party. It does not cover third party access to BPDs via the electronic analysis systems of the intelligence service which holds the warrant.

6.6. Disclosure of BPDs retained pursuant to an individual authorisation, or information in such BPDs, is not generally regulated by the Act. In general, disclosure of BPDs, or information in BPDs, continues to be regulated by section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, and by the arrangements made in accordance with those statutory provisions so as to ensure compliance (amongst other things) with the requirements of necessity and proportionality: see paragraph 3 of Annex A.

6.7. An intelligence service may share BPDs held pursuant to an individual authorisation with overseas partners where it is justified. In such circumstances, the following arrangements set out the considerations to be made by the relevant intelligence service.

Overseas sharing of BPDs

6.8. Section 109 of the Data Protection Act 2018 applies to the disclosure of a BPD as defined by Part 7 and Part 7A of the Act or part of a dataset which in itself would meet the statutory definition of a BPD by the intelligence services. The intelligence services cannot disclose personal data to an international organisation or country or territory outside of the United Kingdom unless it is necessary and proportionate to do so for the purposes of the relevant intelligence service's statutory functions (section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA). The sharing of BPD with overseas partners must be carefully managed to ensure that disclosure only takes place to the extent that it is justified on the basis of the relevant statutory disclosure gateway. This would include a consideration of:

- the nature of the BPD that is due to be disclosed;

[5] See section 226D(3) of the Act.

- the nature and remit of the receiving party;
- any approach previously taken by the relevant intelligence service regarding sharing with the receiving party under consideration and with regard to any protocols/understanding that have previously been used/followed;
- whether the individual circumstances of the BPD disclosure under consideration would require the intelligence service to seek assurances from the receiving party as to its handling of the data contained in the BPD, including limitations on access to the data, restrictions on the onward disclosure, copying, distribution, retention of the data to the minimum necessary to achieve the statutory purpose of the disclosure and conditions for the deletion of the data;
- whether the particular circumstances of the BPD disclosure under consideration would require any restriction, or assurances, on the use the data can be put to by the receiving party to ensure its use is in accordance with the UK's international obligations.

6.9. When considering disclosure of BPDs, staff from the relevant intelligence service are required to consider whether the relevant BPD was acquired under a warrant or authorisation under another Part of the Act, and whether any conditions imposed by the method of acquisition or relevant handling arrangements (such as for interception or equipment interference) apply to it. If such conditions or handling arrangements do apply, they must be followed.

6.10. If a BPD is subject to a Secretary of State's direction under section 225 of the Investigatory Powers Act 2016, such a direction may require that any conditions applicable to intercepted material or equipment interference material must also apply to the BPD. These may have an impact on the extent of disclosure or on the requirements that must be met before disclosure can take place, and may mean that the BPD is also subject to the disclosure requirements of the intelligence service's interception or equipment interference handling arrangements.

6.11. If disclosing BPD to an overseas authority, the relevant intelligence service must ensure that the receiving party has safeguards in place for storing data and restricting onwards disclosure, although this does not mean that the safeguards must be comparable to those applied by the intelligence services. The relevant intelligence service will consider whether it is appropriate to require the overseas authority to apply further safeguards limiting the dissemination, storage and copying of the data and requiring its destruction when there are no longer grounds for retaining it and will keep those conditions under review.

6.12. Where appropriate, the same restrictions on the retention, dissemination and destruction of material that apply to the intelligence services should apply to the overseas authority. Where this is not appropriate, staff from the relevant intelligence service considering the authorisation of such a disclosure must balance the risk that the material will not be subject to the same level of safeguards against the risks to national security if material is not disclosed.

6.13. Any data shared with an overseas organisation will be on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance or approved through established processes between the intelligence service and the recipient party.

Review of retention and deletion

6.14. Each intelligence service must regularly review the operational and legal justification for its continued retention/examination of Part 7A data.

6.15. The nature and frequency of the review should be guided by factors that the intelligence service consider appropriate. As a minimum, the relevant intelligence service should carry out at least one review in advance of the decision as to whether to renew the authorisation at the end of the 12-month period. Such a review can be used to inform the decision as to whether or not to seek a renewal.

6.16. In particular, the retention and review process should consider:

- that the test in section 226A(1) continues to apply to the dataset;
- that the conduct being authorised continues to be proportionate (including review of both necessity and intrusion) to what is sought to be achieved;
- whether such information could reasonably be obtained elsewhere through less intrusive means;
- the level of intrusion into privacy;
- that the data continues to be safeguarded appropriately;
- any legal advice that has been provided.

Destruction

6.17. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it held within the relevant intelligence service must be scheduled for destruction as soon as possible once it is no longer needed for any of the authorised purposes.

6.18. Section 263 defines destroy for the purposes of the Act as deleting the data in such a way as to make access to the data impossible, for example by taking such steps as might be necessary to make the data unavailable or inaccessible to analysts or investigators pending destruction. No further steps such as physical destruction of hardware are required.

7. Record-keeping and error-reporting

Records

7.1. The oversight regime allows the Investigatory Powers Commissioner to inspect the applications upon which the authorisations are based, and the applicant may be required to justify the content. Each intelligence service should keep the following to be made available for scrutiny by the Investigatory Powers Commissioner as he or she may require:

- all applications and authorisation records made for Part 7A authorisations and all applications and authorisation records made for the renewal of such authorisations;
- where any application is refused, the grounds for refusal as given by the Head of an intelligence service (or person acting on their behalf) or Judicial Commissioner.

7.2. Each intelligence service must also keep a record of the following information to assist the Investigatory Powers Commissioner to carry out his or her statutory functions:

- the number of applications for (a) individual and (b) category authorisations submitted;
- the number of applications for (a) individual and (b) category authorisations refused by the Head of an intelligence service (or person acting on their behalf);
- the number of (a) individual and (b) category authorisations granted by the Head of an intelligence service (or person acting on their behalf) and approved by a Judicial Commissioner;
- the number of individual authorisation granted for which prior judicial approval was not required;
- the number of decisions to grant (a) individual and (b) category authorisations not approved by a Judicial Commissioner;
- the number of occasions that a referral was made by the Head of an intelligence service (or person acting on their behalf) to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse the decision to grant (a) individual and (b) category authorisations;
- the number of renewals of (a) individual and (b) category authorisations that were made;

- the number of (a) individual and (b) category authorisations that were cancelled;
- the number of (a) individual and (b) category authorisations extant at the end of the calendar year;
- a record of Part 7A datasets held within a particular category authorisation; and a list of all Part 7A datasets destroyed in the previous 12 months;
- the number and details of directions by the Secretary of State under section 225(3) (relating to the application of Part 7 to Part 7A bulk personal datasets obtained under the Act);
- the number of times an urgent individual authorisation has been (a) submitted and (b) granted by the Head of an intelligence service (or person acting on their behalf);
- the number of times that the decision to issue an urgent individual authorisation has subsequently not been approved by a Judicial Commissioner;
- the number of occasions that a referral was made by the Head of an intelligence service (or person acting on their behalf) to the Investigatory Powers Commissioner, following the decision of a Judicial Commissioner to refuse to approve a decision to grant an urgent individual authorisation; and
- A subset of these records must be sent in written or electronic form to the Investigatory Powers Commissioner, as specified and requested by the Commissioner. Those records that are not requested by the Investigatory Powers Commissioner should continue to be retained by the intelligence services as set out in this chapter of the Code. Guidance on record keeping may be issued by the Investigatory Powers Commissioner. Guidance may also be sought from the Investigatory Powers Commissioner by the intelligence services.

7.3. 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.

Errors

7.4. This section provides information regarding errors. Proper application of the Act and thorough procedures for operating its provisions, including for example the careful preparation and checking of applications and authorisations, should reduce the scope for making errors.

7.5. Wherever possible, technical systems should incorporate functionality to minimise errors. A person holding a senior position within each intelligence service must undertake a regular review of errors and a written review must be made of each review.

7.6. Section 231(9) of the Act sets out what is meant by a “relevant error”, and section 236(6) requires that any relevant error of which an intelligence service is aware must be reported to the Investigatory Powers Commissioner.

7.7. Section 231(9)(a) makes clear that an error can only be a relevant error where it is one that has been made by a public authority in complying with any requirements imposed by the Act (or any other enactment), which are subject to review by the Investigatory Powers Commissioner. Section 231(9)(b) sets out that a relevant error must also be one of a description outlined in a code of practice under Schedule 7 of the Act. In the case of BPD, a relevant error is one that meets the description at paragraph 7.8.

7.8. A relevant error occurs where both of the following conditions are met:

- There has been an error by a public authority in complying with any requirements imposed by the Act (or any other enactment) which are subject to review by the Investigatory Powers Commissioner; and
- The error occurs after a BPD has been retained.

7.9. The following provides a non-exhaustive list of possible relevant errors that would amount to an error by the public authority in complying with the requirements imposed on it and that would fall within the description provided at paragraph 7.8:

- failing to apply for a low/no BPD authorisation within the permitted period, unless retention is authorised by a Part 7 BPD warrant;
- failing to obtain Judicial Commissioner approval for a dataset retained under a non-urgent individual authorisation, unless retention of that dataset is subject to an individual authorisation that falls within a category authorisation.
- an error may occur when a BPD is classed low/no in circumstances where the intelligence agency knew at the time of authorisation that it did not meet the low/no criteria as set out in section 226A of the Act.

7.10. Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the Act, all relevant errors must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

7.11. When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

7.12. From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Investigatory Powers Commissioner, the intelligence service responsible must also inform the Commissioner of when it was initially identified that an error may have taken place.

7.13. A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days of establishing the fact of the error, the reasons this is the case. Where the report is being made by the public authority that made the error, that report should also include: the cause of the error; amount of data retained or retained and examined; any unintended collateral intrusion; any analysis or action taken; whether the data has been retained or destroyed; and a summary of the steps taken to prevent recurrence. Where the error has also resulted in an error under another code, this should be made clear so that errors are not double counted.

7.14. As set out at section 231(9) of the Act, the Investigatory Powers Commissioner will keep under review the definition of relevant errors. The Investigatory Powers Commissioner may also issue guidance as necessary, including guidance on the format of error reports. The intelligence services must have regard to any guidance on errors issued by the Investigatory Powers Commissioner.

7.15. Where an error occurs which is also considered to constitute an offence detailed in chapter 3 of this Code, the provisions of this chapter must still be applied to the handling of the error.

Serious errors

7.16. Section 231 of the Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Investigatory Powers Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Investigatory Powers Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient for an error to be a serious error.

7.17. In deciding whether it is in the public interest for the person concerned to be informed of the error, the Investigatory Powers Commissioner must in particular consider:

- the seriousness of the error and its effect on the person concerned; and,
- the extent to which disclosing the error would be contrary to the public interest or prejudicial to:
  - national security;
  - the prevention or detection of serious crime;
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any of the intelligence services.

7.18. Before making his or her decision, the Investigatory Powers Commissioner must ask the intelligence service which has made the error to make submissions on the matters concerned. The intelligence services must take all reasonably practicable steps notified to them by the Investigatory Powers Commissioner to identify the subject of a serious error.

7.19. When informing a person of a serious error, the Investigatory Powers Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Investigatory Powers Commissioner considers to be necessary for the exercise of those rights.

8. Oversight

The Investigatory Powers Commissioner

8.1. The Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers contained within Part 7A and adherence to the practices and processes described by this Code. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of His Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts and legal experts, qualified to assist the Commissioner in their work. The Commissioner will also be advised by the Technology Advisory Panel.

8.2. The Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Commissioner may undertake these inspections, as far as they relate to the Commissioner's statutory functions, entirely on his or her own initiative. Section 236 provides for the Intelligence and Security Committee of Parliament to refer a matter to the Commissioner with a view to carrying out an investigation, inspection or audit.

8.3. The Commissioner 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 Commissioner must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (see section 229(6)). A Commissioner must in particular not jeopardise the success of the intelligence services, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department or His Majesty's forces (see section 229(7)). In using these powers the intelligence services must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

8.4. Anyone, including anyone working for an intelligence service, who has concerns about the way that investigatory powers are being used, may report their concerns to the Commissioner. 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 relevant error of which he or she is aware. Here, relevant error has the meaning given by section 231(9). This may be in addition to the person raising concerns through the internal mechanisms within the public authority or as an alternative to raising a concern internally through a disclosure to IPCO, as enabled by the information gateway set out in section 237 of the IPA.[6]

8.5. Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to a person 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 person affected. Further information on errors can be found in chapter 8 of this Code. The public authority who has made the relevant error will be able to make representations to the Commissioner before the Commissioner decides it is in the public interest for the person to be informed. The Commissioner must also inform the affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal (see chapter 10 for more information on how this can be done).

8.6. The Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Commissioner's report.

8.7. The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. The intelligence services may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

8.8. Further information about the Commissioner, their office and their work may be found at: www.ipco.org.uk

Annual reports

8.9. Section 226DA of the Act sets out that the Head of each intelligence service must provide an annual report to the Secretary of State about BPDs that were authorised under Part 7A to be retained, or retained and examined, by the intelligence service each year. Such reports must be provided to the Secretary of State as soon as reasonably practicable after the end of the period to which the report relates.

[6] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/2022-08-Disclosing-information-to-IPCO.pdf

8.10. Section 226DB of the Act sets out that the Secretary of State must provide an annual report to the Intelligence and Security Committee of Parliament (ISC) setting out information about category authorisations and renewals of category authorisations granted in that period. Such reports must be provided to the ISC as soon as reasonably practicable after the end of the period to which the report relates.

9. Complaints

9.1. The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of certain investigatory powers, including those covered by this Code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in this Code should be directed to the IPT.

9.2. The IPT is entirely independent from His 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. Following receipt of a complaint or claim from a person, 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. A 'person' for these purposes includes an organisation and association or combination of persons (see section 81(1) of RIPA), as well as an individual.

9.3. 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: https://investigatorypowerstribunal.org.uk. 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

9.4. 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.

Annex A

The Security Service Act 1989 and the Intelligence Services Act 1994

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.

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.

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 intelligence services to ensure that there are arrangements for securing (i) that no information is obtained by the relevant intelligence service 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).

4. SSA and ISA accordingly impose specific statutory limits on the information that each of the intelligence services can obtain, and on the information that each can disclose. These statutory limits do not simply apply to the obtaining and disclosing of information from or to other persons in the United Kingdom: they apply equally to obtaining and disclosing information from or to persons abroad.

The Counter-Terrorism Act 2008

5. Section 19 of the **Counter-Terrorism Act 2008** confirms that 'any person' may disclose information to the intelligence services for the exercise of their respective functions, and disapplies any duty of confidence (or any other restriction, however imposed) which might otherwise prevent this. It further confirms that information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its other functions. For example, information that is obtained by the Security Service for national security purposes can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime.

The Human Rights Act 1998

6. Each of the intelligence services is a public authority for the purposes of the **Human Rights Act 1998**. When obtaining, using, retaining and disclosing bulk personal datasets, the intelligence services must therefore (among other things) ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Other Convention rights, for example Article 6 (right to a fair trial) and Article 10 (freedom of expression), may be engaged depending on the circumstances. In practice, this means that any interference must be both necessary for the performance of a statutory function of the relevant intelligence service and proportionate to the achievement of that objective.

The Data Protection Act 2018

7. Section 3(2) of the **Data Protection Act 2018** defines '*personal data*' as:

> "Personal data" means any information relating to an identified or identifiable living individual.

8. Section 86(7)(a–f) of the DPA defines "sensitive processing" as:[7]

- the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- the processing of genetic data for the purpose of uniquely identifying an individual;
- the processing of biometric data for the purpose of uniquely identifying an individual;

[7] For the purposes of the 2016 Act, the definition of sensitive personal data only includes the data types listed at section 86 (7)(a) to (e) of the Data Protection Act 2018, and excludes (f) the processing of personal data as to (i) the commission or alleged commission of an offence by an individual, or (ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

- the processing of data concerning health;
- the processing of data concerning an individual's sex life or sexual orientation;
- the processing of personal data as to—
    i. the commission or alleged commission of an offence by an individual, or
    ii. proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

9. Each of the intelligence services is a data controller in relation to all the personal data that it holds. Accordingly, when the intelligence services use any BPDs that contain personal data, they must ensure that they comply with the Data Protection Act 2018 (except in cases where exemption under section 110 is required for the purpose of safeguarding national security).