**KEY EXCERPTS - Codes of Practice: Intelligence services use of third party bulk personal datasets**

[Scope and definitions 1](#_Toc151721751)

[Third parties 3](#_Toc151721752)

[Initial examination 3](#_Toc151721753)

[3PD warrant applications 4](#_Toc151721754)

[Presence of sensitive information 6](#_Toc151721755)

[Confidential information relating to members of sensitive professions 6](#_Toc151721756)

[Safeguards: Access and examination 7](#_Toc151721757)

[Oversight 8](#_Toc151721758)

# Scope and definitions

Part 7 of the Act defines a bulk personal dataset (BPD) as a set of data that has been obtained and retained by an intelligence service, where that dataset 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.

Part 7B of the Act provides a statutory framework for cases where an intelligence service, in the course of exercising its functions, needs to access, but not obtain and retain, datasets that are held by a third party, which, if they were retained by the intelligence service itself, may fall within Part 7 or Part 7A of the IPA.

Part 7B of the Act applies where an intelligence service has ‘relevant access’ to a dataset that is held electronically by a person other than the intelligence service, where the dataset contains personal data relating to a number of individuals, where the nature of the set is such that the majority of the individuals are not of intelligence interest, and are unlikely to become so; and where, after any initial inspection, the intelligence service examines but does not obtain the set electronically for the purpose of the exercise of its functions.

‘Relevant access’ is defined as direct, electronic access, where the type and extent of the access available to the intelligence service is not generally available.

For the purpose of Part 7B, access will be direct where the intelligence service is able to access the data electronically, without the involvement of an intermediary. The dataset will be accessed *in situ*, on the third party’s system, rather than being obtained and retained by the intelligence service.

When considering whether Part 7B applies to examination of a particular dataset or datasets, the intelligence service must assess whether the type and extent of the access available is ‘generally available’.

Accesses will be considered on a case by case basis. Examples of accesses that would be considered generally available include accesses that are widely available online, whether for free or upon payment of a charge, and accesses that are available to commercial customers.

Examples of generally available accesses include but are not limited to:

* searches of an online encyclopedia;
* a subscription to an online newspaper (including where credentials may be needed to access an account);
* access to datasets that are made available for public searching of company records;
* public phone or other directories;
* services that provide a general user with the ability to search across academic literature.

In such cases, the requirements of Part 7B do not apply.

Access will not be considered generally available where it is made available only to a particular group of individuals or organisations that fulfil a specific and limited set of qualifying criteria. For example, a particular access might only be available to public authorities, or to law enforcement agencies and intelligence services, or to bodies concerned with the protection of national security. Access to such datasets would fall within the requirements of Part 7B, providing that the other tests set out in 226E are met.

Access may not be generally available even where an intelligence service is able to examine a dataset that is widely available if the nature of the intelligence service’s access is broader than that which other users of the set enjoy. For example, the intelligence service might be able to query additional data fields that other users or customers cannot. This is likely to be sufficient to render the access not ‘generally available’, and therefore potentially subject to the provisions of Part 7B.

Examples of accesses that would not be generally available may include:

* access to data held by a UK government department which is not public and that would constitute a BPD if obtained and retained by an intelligence service. For example, an intelligence service may access HMG held immigration related datasets to conduct checks to ensure those entering the UK do not pose a risk to national security.

## Third parties

For the purposes of this Code, a third party is a person or organisation, other than an UK intelligence service. This may include individuals, companies, government departments or other public authorities.

Part 7B sets out the requirements that must be followed when an intelligence service wishes to examine a third party held bulk dataset.

## Initial examination

Considerable work may be needed on the part of the intelligence service, before a 3PD access can be successfully established and the 3PD is able to be examined for the purpose of the exercise of the intelligence service’s functions.

Part 7B of the Act recognises this, and allows an intelligence service to carry out an initial inspection of a 3PD before deciding whether to make an application to the Secretary of State for a 3PD warrant to authorise the examination of the 3PD.

This initial inspection is likely to be necessary for a number of reasons, which may include:

* To assess the value of the data being made available
* To assess whether the dataset constitutes a 3PD
* To assess whether it is necessary and proportionate to seek access to the data
* To establish practical steps for enabling access e.g. engineering and system access
* To establish the operational safety of access
* To build a relationship with the third party supplier of the data

The initial inspection should be carried out by the minimum number of people necessary in order to do what is required, which will be assessed on a case-by-case basis.

As part of the initial assessment of value, it may be necessary to run data outputs from the 3PD under inspection through separate systems controlled by the intelligence service, for the sole purpose of assessing the potential value of the dataset. This may allow a fuller assessment of the necessity and proportionality of access to data to be made, and inform the decision as to whether to seek a 3PD warrant.

If, after the initial inspection, the intelligence service assesses that examining the dataset falls within Part 7B, and that it would be necessary and proportionate to examine the 3PD in pursuit of its statutory functions, they should apply for a 3PD warrant.

If, after the initial inspection, the intelligence service assesses that it would not be necessary and proportionate to examine the 3PD, the 3PD should not be further accessed.

# 3PD warrant applications

An application for a 3PD warrant is made to the Secretary of State. The requirements set out in Part 7B of the Act only relate to the intelligence services. An application for a 3PD warrant therefore may only be made by or on behalf of the following persons:

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

All 3PD warrants can only be issued by the Secretary of State. No 3PD warrant may be issued unless and until the decision to do so has been approved by a Judicial Commissioner (see paragraph XX and subsequent paragraphs). A Judicial Commissioner will have access to the same application for a warrant as the Secretary of State.

The only exception to this is a case where the Secretary of State considers that there is an urgent need to issue a warrant (see paragraph XX and subsequent paragraphs). Even where the urgency procedure is followed, the Secretary of State must personally take the decision to issue the warrant. In any case where the Secretary of State decides to issue a warrant (whether under the urgency procedure or otherwise), he or she must personally sign the warrant unless it is not reasonably practicable to do so, in which case a designated senior official can sign the warrant. When a 3PD warrant is issued, it is addressed to the person who submitted the application (or on whose behalf it was submitted).

Prior to submission, each application should be subject to a review within the intelligence service making the application. This involves consideration as to whether the application is necessary for the intelligence services statutory functions (see the Security Service Act 1989 and the Intelligence Services Act 1994) . The consideration of the application should also include whether access to and examination of the 3PD is proportionate.

When completing a warrant application, the intelligence service must ensure that the case for the warrant 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 warrant.

Where the intelligence services are working jointly to establish a 3PD access, or where an access has been established that would be of operational benefit to more than one service, a joint application may be made.

When making an application for a 3PD warrant, the intelligence service may make a single application where one access covers multiple datasets or types of dataset. For example, an arrangement may be in place with a third party that performs a service which brings together datasets from multiple sources and makes these available to query as a single access. In such a case, a single application to the Secretary of State would be made.

Additionally, the intelligence service may choose to make one application to cover multiple 3PD accesses where those accesses raise similar considerations. For example, if an intelligence service has access to multiple 3PDs that are similar in content and degree of intrusion they might choose to group such accesses into a single 3PD warrant application, so that the Secretary of State could consider the necessity and proportionality case for those accesses in the round.

The application for a 3PD warrant must include a general description of the bulk personal dataset or datasets to which the application relates. The description will necessarily be general in nature because the intelligence service is not itself in possession of the dataset or datasets to which access is being sought, and, as a result, in some cases it will not have more than a general knowledge of the data contained therein.

Moreover, where an access is provided by a third party which aggregates multiple datasets, the intelligence service may not be aware when particular new datasets are added to that access, or when other datasets are removed. Section 226F(3) recognises this by making it clear that a 3PD warrant may authorise the examination of a bulk personal dataset:

1. ‘the content of which may vary from time to time, or
2. That does not exist at the time of the issue of the warrant.’

Section 226G(5) makes clear that the fact that the information that would be examined under the warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

## Presence of sensitive information

Section 226G(3) provides that, in cases where the intelligence service knows that the 3PD access includes certain types of sensitive or other information the warrant application must include a statement to this effect. The relevant types of sensitive or other information for this requirement are set out in section 226G(6), and this requirement applies where:

* the dataset consists of, or includes protected data or health records (see s226G(7)),
* a substantial proportion of the dataset consists of sensitive personal data, or
* the nature of the dataset, or the circumstances in which it was created, is or are such that its examination by the intelligence service is likely to raise novel or contentious issues.

The application should set out what is known about the nature and extent of the sensitive information within the dataset, and why the intelligence service believes that the examination of the 3PD is nevertheless proportionate in the circumstances.

## Confidential information relating to members of sensitive professions

Most 3PDs are unlikely to include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to the sensitive professions. A ‘sensitive profession’ for these purposes includes lawyers, doctors, journalists, Members of a relevant legislature, and Ministers of religion. (References to Members of a relevant legislature include a Member of either House of the UK Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly and Member of the European Parliament elected for the United Kingdom (see paragraph xxx)).

In particular, information relating to a member of a sensitive profession is unlikely, in and of itself, to be considered confidential. For example, it would not include the mere fact of membership of the profession, or basic biographical details of a member of the profession. Thus, the fact that a solicitor’s telephone number appeared in a telephone directory would not be considered confidential information.

There are two scenarios in which the examination of a 3PD could give rise to the need for additional protection for confidential information relating to members of sensitive professions.

First, it is possible that a 3PD which contains protected data could include confidential information relating to a member, or members, of a sensitive profession. In this context, confidential information would include the content of communications between the professional, acting in their professional capacity, and another party. Thus, for example, it would include the content of communications between lawyer and client, doctor and patient, or MP and constituent. Such protected data could also include confidential information which identified a journalistic source.

Secondly, there is a small possibility that examination of data of 3PDs could reveal the sources of journalistic material. In circumstances where the selection for examination conducted by an authorised person is for the purpose of identifying a source of journalistic material, the safeguards set out below must be applied.

The intelligence services should ensure that, before intelligence service staff use a 3PD specifically with the intention of searching for confidential information relating to members of sensitive professions, particular consideration is given to the necessity and proportionality justification for the interference with privacy that will be involved. Sections 226IB and 226IC make provision for additional safeguards that apply where examination of the 3PD is intended or likely to identify items subject to legal privilege.

# Safeguards: Access and examination

In relation to information held in 3PDs, each intelligence service should have in place the following additional measures:

* access to and examination of the information contained within the 3PD should be strictly limited to those with an appropriate business requirement to use these data;
* individuals may only access information within a 3PD if the examination is necessary and proportionate for the exercise of the intelligence service functions
* if individuals access information within a 3PD with a view to subsequent disclosure of that information, (in addition to satisfying the condition in the above bullet) they may only access and examine the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant intelligence service.
* before accessing or disclosing information, individuals must also consider whether to do so would be proportionate (as described in paragraph xxx). For instance, they must consider whether other, less intrusive methods can reasonably be used to achieve the desired outcome;
* users should receive mandatory training regarding their professional and legal responsibilities, including the application of the provisions of the Act and this code of practice. Refresher training and/or updated guidance should be provided when systems or policies are updated;
* appropriate disciplinary action should be taken in the event of inappropriate behaviour being identified;
* users should be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution; and
* the Secretary of State must ensure that the safeguards are in force before any 3PD warrant can be issued.

For each arrangement for access to a 3PD, the intelligence service should consider an appropriate way to appraise examination of that 3PD, in order to ensure that examination is necessary and proportionate in all the circumstances. These arrangements may vary substantially between different 3PDs, given the wide range of ways in which an intelligence service might access and examine a 3PD. Intelligence service arrangements for access and examination will be kept under review by the Investigatory Powers Commissioner during his or her inspections.

Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards must be reported to the Investigatory Powers Commissioner.

The intelligence services should also take the following measures – by establishing the necessary underpinning working practices - to reduce the level of interference with privacy arising from the examination of 3PDs:

* minimising the number of results which are presented for analysis, by training and requiring persons with access to 3PDs to frame queries in a proportionate way; and
* confining access to specific datasets (or subsets thereof) to a limited number of analysts.

# Oversight

The Investigatory Powers Act provides for an Investigatory Powers Commissioner (“the Commissioner”), whose remit includes providing comprehensive oversight of the use of the powers contained within Part 7B of the Act 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 Her 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.

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.

The Commissioner will have unfettered access to all of the intelligence service’s 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 Her 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.

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 x of the code, report to the Commissioner any relevant error of which he is aware. Here, relevant error has the meaning given by section xxx). This may be in addition to the person raising concerns through the internal mechanisms within the public authority.

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 x 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).

The Investigatory Powers 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.

The Investigatory Powers Commissioner may also report, at any time, on any of its 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.

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