



Investigatory Powers Act 2016

2016 CHAPTER 25

PART 3

AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA

Targeted authorisations for obtaining data

61 Power to grant authorisations

- (1) Subsection (2) applies if a designated senior officer of a relevant public authority considers—
 - (a) that it is necessary to obtain communications data for a purpose falling within subsection (7),
 - (b) that it is necessary to obtain the data—
 - (i) for the purposes of a specific investigation or a specific operation, or
 - (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and
 - (c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.
- (2) The designated senior officer may authorise any officer of the authority to engage in any conduct which—
 - (a) is for the purpose of obtaining the data from any person, and
 - (b) relates to—
 - (i) a telecommunication system, or
 - (ii) data derived from a telecommunication system.
- (3) Subsections (1) and (2) are subject to—
 - (a) section 62 (restrictions in relation to internet connection records),
 - (b) section 63 (additional restrictions on grant of authorisations),

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: *Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

- (c) sections 70 and 73 to 75 and Schedule 4 (restrictions relating to certain relevant public authorities),
 - (d) section 76 (requirement to consult a single point of contact), and
 - (e) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).
- (4) Authorised conduct may, in particular, consist of an authorised officer—
- (a) obtaining the communications data themselves from any person or telecommunication system,
 - (b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—
 - (i) to obtain the data (if not already in possession of it), and
 - (ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation, or
 - (c) requiring by notice a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—
 - (i) to obtain the data (if not already in possession of it), and
 - (ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.
- (5) An authorisation—
- (a) may relate to data whether or not in existence at the time of the authorisation,
 - (b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and
 - (c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.
- (6) An authorisation—
- (a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system, and
 - (b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b) or (c), a person to disclose the data to any person other than—
 - (i) an authorised officer, or
 - (ii) an officer of the same relevant public authority as an authorised officer.
- (7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—
- (a) in the interests of national security,
 - (b) for the purpose of preventing or detecting crime or of preventing disorder,
 - (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
 - (d) in the interests of public safety,

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)

- (e) for the purpose of protecting public health,
 - (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
 - (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
 - (h) to assist investigations into alleged miscarriages of justice,
 - (i) where a person (“P”) has died or is unable to identify themselves because of a physical or mental condition—
 - (i) to assist in identifying P, or
 - (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or
 - (j) for the purpose of exercising functions relating to—
 - (i) the regulation of financial services and markets, or
 - (ii) financial stability.
- (8) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).
- (9) See—
- (a) sections 70 and 73 for the meanings of “designated senior officer” and “relevant public authority”;
 - (b) section 84 for the way in which this Part applies to postal operators and postal services.

Commencement Information

II S. 61(7)(a)-(j) in force at 30.12.2016 for specified purposes by [S.I. 2016/1233](#), [reg. 2\(b\)](#)

VALID FROM 05/02/2019

62 Restrictions in relation to internet connection records

- (1) A designated senior officer of a local authority may not grant an authorisation for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record.
- (2) A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.
- (3) Condition A is that the designated senior officer considers that it is necessary, for a purpose falling within section 61(7), to obtain the data to identify which person or apparatus is using an internet service where—
 - (a) the service and time of use are already known, but
 - (b) the identity of the person or apparatus using the service is not known.

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: *Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)*

(4) Condition B is that—

- (a) the purpose for which the data is to be obtained falls within section 61(7) but is not the purpose falling within section 61(7)(b) of preventing or detecting crime, and
- (b) the designated senior officer considers that it is necessary to obtain the data to identify—
 - (i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,
 - (ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or
 - (iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) Condition C is that—

- (a) the purpose for which the data is to be obtained is the purpose falling within section 61(7)(b) of preventing or detecting crime,
- (b) the crime to be prevented or detected is serious crime or other relevant crime, and
- (c) the designated senior officer considers that it is necessary to obtain the data to identify—
 - (i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known,
 - (ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime, or
 - (iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(6) In subsection (5) “other relevant crime” means crime which is not serious crime but where the offence, or one of the offences, which is or would be constituted by the conduct concerned is—

- (a) an offence for which an individual who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) is capable of being sentenced to imprisonment for a term of 12 months or more (disregarding any enactment prohibiting or restricting the imprisonment of individuals who have no previous convictions), or
- (b) an offence—
 - (i) by a person who is not an individual, or
 - (ii) which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

(7) In this Act “internet connection record” means communications data which—

- (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)

telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

- (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

VALID FROM 05/02/2019

63 Additional restrictions on grant of authorisations

- (1) A designated senior officer may not grant an authorisation for the purposes of a specific investigation or a specific operation if the officer is working on that investigation or operation.
- (2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.
- (3) Examples of exceptional circumstances include—
 - (a) an imminent threat to life or another emergency,
 - (b) the investigation or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum,
 - (c) there is an opportunity to obtain information where—
 - (i) the opportunity is rare,
 - (ii) the time to act is short, and
 - (iii) the need to obtain the information is significant and in the interests of national security, or
 - (d) the size of the relevant public authority concerned is such that it is not practicable to have a designated senior officer who is not working on the investigation or operation concerned.

VALID FROM 05/02/2019

64 Procedure for authorisations and authorised notices

- (1) An authorisation must specify—
 - (a) the office, rank or position held by the designated senior officer granting it,
 - (b) the matters falling within section 61(7) by reference to which it is granted,
 - (c) the conduct that is authorised,
 - (d) the data or description of data to be obtained, and
 - (e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.
- (2) An authorisation which authorises a person to impose requirements by notice on a telecommunications operator must also specify—
 - (a) the operator concerned, and
 - (b) the nature of the requirements that are to be imposed,

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)

but need not specify the other contents of the notice.

- (3) The notice itself—
 - (a) must specify—
 - (i) the office, rank or position held by the person giving it,
 - (ii) the requirements that are being imposed, and
 - (iii) the telecommunications operator on whom the requirements are being imposed, and
 - (b) must be given in writing or (if not in writing) in a manner that produces a record of its having been given.
- (4) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

VALID FROM 05/02/2019

65 Duration and cancellation of authorisations and notices

- (1) An authorisation ceases to have effect at the end of the period of one month beginning with the date on which it is granted.
- (2) An authorisation may be renewed at any time before the end of that period by the grant of a further authorisation.
- (3) Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.
- (4) A designated senior officer who has granted an authorisation—
 - (a) may cancel it at any time, and
 - (b) must cancel it if the designated senior officer considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.
- (5) The Secretary of State may by regulations provide for the person by whom any function under subsection (4) is to be exercised where the person who would otherwise have exercised it is no longer available to do so.
- (6) Such regulations may, in particular, provide for the person by whom the function is to be exercised to be a person appointed in accordance with the regulations.
- (7) A notice given in pursuance of an authorisation (and any requirement imposed by the notice)—
 - (a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1), but
 - (b) is cancelled if the authorisation is cancelled under subsection (4).

Status: Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation: Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details)

VALID FROM 05/02/2019

66 Duties of telecommunications operators in relation to authorisations

- (1) It is the duty of a telecommunications operator on whom a requirement is imposed by notice given in pursuance of an authorisation to comply with that requirement.
- (2) It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or requirement for the data in pursuance of an authorisation, to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned.
- (3) A person who is under a duty by virtue of subsection (1) or (2) is not required to take any steps in pursuance of that duty which it is not reasonably practicable for that person to take.
- (4) For the purposes of subsection (3), where obligations have been imposed on a telecommunications operator (“P”) under section 253 (maintenance of technical capability), the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.
- (5) The duty imposed by subsection (1) or (2) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Status:

Point in time view as at 27/12/2018. This version of this cross heading contains provisions that are not valid for this point in time.

Changes to legislation:

Investigatory Powers Act 2016, Cross Heading: Targeted authorisations for obtaining data is up to date with all changes known to be in force on or before 29 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.