
STATUTORY INSTRUMENTS

2018 No. 1123

The Data Retention and Acquisition Regulations 2018

Citation and commencement

- 1.—(1) These Regulations may be cited as the Data Retention and Acquisition Regulations 2018.
- (2) This regulation and regulation 2 come into force on the day after the day on which these Regulations are made.
- (3) The following provisions of these Regulations come into force on 1st November 2018—
- (a) regulation 3;
 - (b) regulation 4 for the purposes of regulations 8 to 10;
 - (c) regulations 8 and 9;
 - (d) regulation 10 for the purposes of paragraphs 22, 23 and 27(b) and (c) of Schedule 1;
 - (e) regulation 11 for the purposes of paragraph 2 of Schedule 2;
 - (f) paragraphs 22, 23 and 27(b) and (c) of Schedule 1;
 - (g) paragraph 2 of Schedule 2.
- (4) Subject to paragraph (5), the following provisions of these Regulations come into force on the day that section 61(1) of the Investigatory Powers Act 2016 comes into force—
- (a) regulation 4 for all remaining purposes;
 - (b) regulations 5 to 7;
 - (c) regulations 10 and 11 for all remaining purposes;
 - (d) Schedule 1 so far as not already in force;
 - (e) paragraph 1 of Schedule 2.
- (5) Where section 61(1) of the Investigatory Powers Act 2016 comes into force on a day only for a particular purpose or purposes specified in regulations under section 272(1) of that Act, the provisions specified in paragraph (4) come into force on that day only for that purpose or (as the case may be) those purposes.

Code of Practice

2. The code of practice entitled “Communications Data” laid before Parliament on 28th June 2018 has effect.

Amendments of the Regulation of Investigatory Powers Act 2000

- 3.—(1) Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000(1) is amended as follows.

(2) Section 22 (obtaining and disclosing communications data)(2) is amended in accordance with paragraphs (3) to (5).

(3) For subsection (2)(b) substitute—

“(b) for the applicable crime purpose;”.

(4) Omit subsections (2)(e) and (f).

(5) After subsection (2) insert—

“(2A) In this section, “the applicable crime purpose” means—

- (a) where the communications data is wholly or partly data falling within section 21(4)(a) or (b), the purpose of preventing or detecting serious crime;
- (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.”.

(6) In section 25 (interpretation of Chapter 2 of Part 1)(3), in subsection (1), after the definition of “relevant public authority” insert—

““serious crime” includes crime which would not satisfy the test in section 81(3)(a) or (b) 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 that section, after subsection (1) insert—

“(1A) Until the day on which the amendment made to section 81(3)(a) of this Act by paragraph 211 of Schedule 7 to the Criminal Justice and Court Services Act 2000 comes into force, the definition of “serious crime” in subsection (1) is to be read as if for the words “the age of 18 (or, in relation to Scotland or Northern Ireland, 21)” there were substituted “the age of 21”.”.

Amendments of the Investigatory Powers Act 2016

4. The Investigatory Powers Act 2016 is amended in accordance with regulations 5 to 10.

Grant of authorisations by the Investigatory Powers Commissioner

5. After the heading of Part 3 insert—

-
- (2) Section 22 was amended by the Policing and Crime Act 2009 (c. 26), section 7(1) and (2); the Protection of Freedoms Act 2012 (c. 9) Schedule 9, Part 3, paragraphs 6 and 7; the Data Retention and Investigatory Powers Act 2014 (c. 27), sections 3(3) and (4), 4(8) to (10); and by S.I. 2013/602. The amendments made by the Data Retention and Investigatory Powers Act 2014 are saved by paragraph 9 of Schedule 9 to the Investigatory Powers Act 2016.
 - (3) Section 25 was amended by the Serious Organised Crime and Police Act 2005 (c. 15), Schedule 4, paragraphs 131, 135(1), (3) and (4); the Serious Crime Act 2007 (c. 27) Schedule 12, paragraphs 5 and 8; the Crime and Courts Act 2013 (c. 22), Schedule 8, Part 2, paragraphs 77, 81(1) to (3) and 88; and by S.I. 2007/1098 and 2013/602.

“Targeted authorisations for obtaining data: the Investigatory Powers Commissioner

60A. Power of Investigatory Powers Commissioner to grant authorisations

(1) Subsection (2) applies if the Investigatory Powers Commissioner, on an application made by a relevant public authority, considers—

- (a) that it is necessary for the relevant public authority to obtain communications data for a purpose falling within subsection (7),
- (b) that it is necessary for the relevant public authority 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 Investigatory Powers Commissioner may authorise the relevant public 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) sections 70, 73 and 75 and Schedule 4 (restrictions relating to certain relevant public authorities),
- (c) section 76 (requirement to consult a single point of contact), and
- (d) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of the relevant public authority—

- (a) obtaining the communications data itself from any person or telecommunication system,
- (b) asking any person whom the relevant public authority 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 the relevant public authority, or
- (c) requiring by notice a telecommunications operator whom the relevant public authority 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 the relevant public authority.

(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 other than the relevant public authority, 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 telecommunications 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 may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system.
- (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 applicable crime purpose (see subsection (8)),
 - (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,
 - (e) 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,
 - (f) to assist investigations into alleged miscarriages of justice, or
 - (g) 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 reasons for P’s death or condition.
- (8) In subsection (7)(b), “the applicable crime purpose” means—
- (a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;
 - (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.
- (9) 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).
- (10) See—
- (a) sections 70 and 73 for the meaning of “relevant public authority”;
 - (b) section 84 for the way in which this Part applies to postal operators and postal services;
 - (c) section 86(2A) for the meaning of “serious crime”.

Amendment of section 61

- 6.—(1) In the italic heading before section 61, at the end insert “: designated senior officers”.
- (2) Section 61 (power to grant authorisations) is amended as follows.
- (3) In the heading, after “Power” insert “of designated senior officers”.

- (4) In subsection (3), in paragraph (c), for “and 73 to 75” substitute “, 73 and 75”.
- (5) In subsection (7)—
 - (a) for paragraph (b) substitute—
 - “(b) for the applicable crime purpose (see subsection (7A)), or”;
 - (b) omit paragraphs (d) to (j).
- (6) After subsection (7) insert—
 - “(7A) In subsection (7)(b), “the applicable crime purpose” means—
 - (a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;
 - (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.”.
- (7) In subsection (9), after paragraph (b) insert—
 - “(c) section 86(2A) for the meaning of “serious crime”.”.

Power of designated senior officers to grant authorisations in urgent cases

- 7. After section 61 insert—

“61A. Power of designated senior officers to grant authorisations: urgent cases

- (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 for the purposes of a specific investigation or a specific operation,
 - (c) that there is an urgent need to obtain the data, and
 - (d) 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 relevant public 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) sections 70, 73 and 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 telecommunications 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) for the applicable crime purpose (see subsection (8)),
 - (b) in the interests of public safety,
 - (c) 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,
 - (d) to assist investigations into alleged miscarriages of justice, or
 - (e) 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 reasons for P's death or condition.

- (8) In subsection (7)(a), “the applicable crime purpose” means—
- (a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;
 - (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

(9) 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).

- (10) 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;
 - (c) section 86(2A) for the meaning of “serious crime”.

Retention of communications data

8.—(1) Section 87 (powers to require retention of certain data) is amended as follows.

(2) In subsection (1)(a), for the words from “purposes falling” to “obtained,” substitute “following purposes—

- (i) in the interests of national security,
- (ii) for the applicable crime purpose (see subsection (10A)),
- (iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
- (iv) in the interests of public safety,
- (v) 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,
- (vi) to assist investigations into alleged miscarriages of justice.”.

(3) In subsection (8), after paragraph (a) insert—

“(aa) each telecommunications service (or description of telecommunications service) to which it relates.”.

(4) In subsection (10), for the words from “paragraphs” to the end substitute “sub-paragraphs (i) to (vi) of subsection (1)(a)”.

(5) After subsection (10) insert—

“(10A) In this section, “the applicable crime purpose” means—

- (a) to the extent that a retention notice relates to events data, the purpose of preventing or detecting serious crime;
- (b) to the extent that a retention notice relates to entity data, the purpose of preventing or detecting crime or of preventing disorder.

(10B) In subsection (10A)(a), “serious crime” means, in addition to crime which falls within paragraph (a) or (b) of the definition of “serious crime” in section 263(1), crime 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.”.

Amendment of section 88

9. In section 88 (matters to be taken into account before giving retention notices), in subsection (1)—

- (a) in paragraph (a), after “notice” insert “, including in relation to one or more of the purposes mentioned in sub-paragraphs (i) to (vi) of section 87(1)(a) (purposes for which retention of communications data may be required)”;
- (b) after paragraph (a) insert—
 - “(aa) the telecommunications services to which the retention notice relates,
 - (ab) the appropriateness of limiting the data to be retained by reference to—
 - (i) location, or
 - (ii) descriptions of persons to whom telecommunications services are provided.”.

Further amendments of the Investigatory Powers Act 2016

10. Schedule 1 makes further amendments of the Investigatory Powers Act 2016.

Consequential amendments

11. Schedule 2 makes consequential amendments of other legislation.

31st October 2018

Ben Wallace
Minister of State
Home Office