Home Office

Acquisition and Disclosure of Communications Data

DRAFT Code of Practice

March 2015

Acquisition and Disclosure of Communications Data

DRAFT Code of Practice

Presented to Parliament pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000

March 2015

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at commsdata@homeoffice.x.gsi.gov.uk.

Print ISBN 9781474115650
Web ISBN 9781474115667

ID 19021502 03/15

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

1 Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA'). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions. This version of the code replaces all previous versions of the code.

1.2 This code applies to relevant public authorities within the meaning of RIPA: those listed in section 25 or specified in orders made by the Secretary of State under section 25.[1]

1.3 Relevant public authorities for the purposes of Chapter II of Part I of RIPA ('Chapter II') should not:

- use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data,[2] or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office; or
- require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

1.4 This code should be readily available to members of a relevant public authority involved in the acquisition of communications data and the exercise of powers to do so under RIPA, and to communications service operators involved in the disclosure of communications data to public authorities under duties imposed by RIPA.[3]

1 See paragraph 2.11.

2 For example, the power available under section 1 of the Social Security Fraud Act 2001. See also the section on Authorisations beginning at paragraph 3.32.

3 See section 22(6) of RIPA.

1.5 Throughout this code an operator who provides a postal or telecommunications service is described as a communications service provider ('CSP'). The meaning of telecommunications service is defined in RIPA[4] and extends to CSPs providing such services where the system for doing so is wholly or partly in the United Kingdom or elsewhere. This includes, for example, a CSP providing a telecommunications system to persons in the United Kingdom where communications data relating to that system is either, or both, processed and stored outside the United Kingdom. Section 4 of the Data Retention and Investigatory Powers Act 2014 ('DRIPA') clarified that communications data acquisition powers under RIPA are exercisable in respect of those CSPs that provide a service to the United Kingdom from outside of the country.

1.6 RIPA provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under RIPA,[5] or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account.

1.7 The exercise of powers and duties under Chapter II is kept under review by the Interception of Communications Commissioner ('the Commissioner') appointed under section 57 of RIPA and by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

1.8 This code **does not** relate to the retention of communications data. The Retention of Communications Data Code of Practice, issued pursuant to regulation 10 of the Data Retention Regulations 2014 and section 71 of RIPA,[6] provides guidance on procedures to be followed in relation to the retention of communications data under a notice made under DRIPA (a 'data retention notice') and the voluntary code of practice under the Anti-terrorism, Crime and Security Act 2001 ('ATCSA').

1.9 Acquisition of data retained under a data retention notice given under section 1 of DRIPA or in accordance with the ATCSA Code can only be acquired in accordance with RIPA, or a court order or other judicial authorisation or warrant.[7] The Retention of Communications Data Code of Practice will cover how this may impact on Service Providers.[8]

---

4 Sections 2(1) and 81(1) of RIPA defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. Section 2(8A) of RIPA makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system are included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition. The definition of 'telecommunications service' in RIPA is intentionally broad so that it remains relevant for new technologies.

5 See paragraphs 9.1 and 9.2.

6 ISBN [to be completed when finalised].

7 The restriction of acquisition of data retained under a data retention notice to RIPA or court orders is without prejudice to the ability of individuals to request their own data under a Data Protection Act (DPA) Subject Access Request (SAR).

8 Note that a company's business data is not affected by the restriction to RIPA or court orders.

1.10 This code ***does not*** relate to the interception of communications nor to the acquisition or disclosure of the contents of communications. The Interception of Communications Code of Practice issued pursuant to Section 71 of RIPA provides guidance on procedures to be followed in relation to the interception of communications.[9]

1.11 Communications data that is obtained directly as a consequence of the execution of an interception warrant ('related communications data', RCD) is intercept product.[10]

1.12 Any related communications data, and any other specific communications data ('other related data') derived directly from it, must be treated in accordance with the restrictions on the use of intercepted material and related communications data.[11]

1.13 Related communications data may be used as a basis for the acquisition of other related data for intelligence purposes[12] only, if there is sufficient intercept product or non-intercept material available to a designated person to allow that person to consider the necessity and proportionality of acquiring the other related data. The application to the designated person[13] and the resultant data acquired should be treated as product of the interception.

1.14 Related communications data may be used as a basis for the acquisition of other related data for use in legal proceedings provided that the related communications data does not identify itself as intercept product. There must also be sufficient non-intercept material available to the designated person to allow that person to consider the necessity and proportionality of acquiring the other related data. In practice it will be rare to achieve this. Consequently, it is best practice when undertaking the acquisition of other related data for use in legal proceedings that the provenance of such data is from a source other than conduct authorised by an interception warrant.

1.15 This code extends to the United Kingdom.[14]

---

9 ISBN 0-11-341281-9.

10 Section 20 of RIPA defines 'related communications data' in relation to a communication intercepted in the course of its transmission, by means of a postal service or telecommunications system, to mean so much of any communications data (within the meaning of Chapter II of Part I of RIPA) as–
(a) is obtained by, or in connection with, the interception; and
(b) relates to the communication or to the sender or recipient, or intended recipient, of the communication.

11 See sections 15, 17, 18 and 19 of RIPA

12 Section 81(5) of RIPA qualifies the reference to preventing or detecting serious crime in section 5(3) – grounds for the issue of an interception warrant – to exclude gathering of evidence for use in any legal proceedings.

13 See paragraph 3.7.

14 This code and the provisions of Chapter II of Part I of RIPA do not extend to the Crown Dependencies and British Overseas Territories. Note that Chapter 7 includes sections on acquisition of communication data on behalf of overseas authorities and the transfer of communications data to overseas authorities.

2 General extent of powers

Scope of Powers, Necessity and Proportionality

2.1 The acquisition of communications data under RIPA will be a justifiable interference with an individual's human rights under Articles 8 and, in certain circumstances, 10 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

2.2 RIPA stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 22(2) of RIPA:[15]

- in the interests of national security;[16]
- for the purpose of preventing or detecting crime[17] or of preventing disorder;
- 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;[18]
- in the interests of public safety; [19]
- for the purpose of protecting public health;[20]

[15] RIPA permits the Secretary of State to add further purposes by means of an Order subject to the affirmative resolution procedure in Parliament.

[16] One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the United Kingdom. A designated person in another public authority should not grant an authorisation or give a notice under RIPA where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where the conduct is to be undertaken by a Special Branch, by the Metropolitan Police Counter Terrorism Command, or where the Security Service has agreed that another public authority can acquire communications data in relation to an operation or investigation which would fall within the responsibilities of the Security Service.

[17] Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 81(5) of RIPA. Where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Chapter II to obtain communications data for the purpose of preventing or detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under RIPA.

[18] DRIPA section 3(3) amended section 22(2)(c) of RIPA to make clear that where acquisition of communications data is necessary in the interests of the economic well-being of the United Kingdom, this purpose may only be used 'so far as those interests are also relevant to the interests of national security.'

[19] This purpose should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as accident investigation or for example, a large scale event that may cause injury to members of the public. Public safety should not be interpreted as for purposes relating to crime that impacts on the public, such as the sale of illegal drugs.

[20] The public health purpose should be used by public authorities with functions to investigate specific and often specialised offences or conduct such as breaches of health and safety legislation and criminal offences which may risk public health, for example, the supply of controlled medicines without licence or prescriptions.

- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, 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;[21]
- to assist investigations into alleged miscarriages of justice;[22]
- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident);[23]
- in relation a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for their death or condition;[24] and
- for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.[25]

2.3 The purposes for which some public authorities may seek to acquire communications data are restricted by order.[26] The designated person may only consider necessity on grounds open to their public authority and only in relation to matters that are the statutory or administrative function of their respective public authority. The purposes noted above should only be used by a public authority in relation to the specific (and often specialist) offences or conduct that it has been given the statutory function to investigate.

2.4 There is a further restriction upon the acquisition of communications data for the following purposes:

- in the interests of public safety;
- for the purpose of protecting public health; and
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

Only communications data within the meaning of section 21(4)(c) of RIPA[27] may be acquired for these purposes and only by those public authorities permitted by order to acquire communications data for one or more of those purposes.

---

21 Such an emergency can include those situations where, for example, there is serious concern for the welfare of a vulnerable person.

22 See article 2 (a), SI 2010/480.

23 See article 2 (b) (i), SI 2010/480.

24 See article 2 (b) (ii), SI 2010/480.

25 See article 2 (c), SI 2010/480, as added by SI 2015/228.

26 See article 6, SI 2010/480.

27 21(4)(c) defines subscriber information. See Chapter 2 for further information on RIPA 21(4) and the different categories of communications data defined in RIPA.

2.5 When a public authority wishes to acquire communications data, the designated person must believe that the acquisition, in the form of an authorisation or notice, is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

2.6 As well as consideration of the rights of the individual under investigation, consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to significant collateral intrusion.

2.7 Particular consideration must also be given, when pertinent, to the right to freedom of expression.[28]

2.8 Taking all these considerations into account in a particular case, an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe.

2.9 Any conduct where the interference is excessive in relation to the aims of the investigation or operation, or is in any way arbitrary, will not be proportionate.

2.10 Before public authorities can request communications data, authorisation must be given by the designated person in the relevant authority. A designated person is someone holding a prescribed office, rank or position within a relevant public authority that has been designated for the purpose of acquiring communications data by order.[29]

2.11 The relevant public authorities for Chapter II are set out in section 25(1). They are:

- a police force (as defined in section 81(1) of RIPA);[30]
- the National Crime Agency;[31]
- HM Revenue and Customs;[32]
- the Security Service;
- the Secret Intelligence Service; and
- the Government Communications Headquarters.

---

[28] See the section on communications data involving certain professions, beginning at paragraph 3.72, for further information and guidance, including on the requirement for the use of the Police and Criminal Evidence Act 1984 until such time as there is specific legislation to provide judicial authorisation for applications for communications data to determine journalistic sources.

[29] See articles 3 and 4, SI 2010/480. By virtue of article 4 of the order all more senior personnel to the designated office, rank or position are also allowed to grant authorisations or give notices.

[30] Each police force is a separate relevant public authority which has implications for the separation of roles in the acquisition of data under RIPA.

[31] References in RIPA to the Serious Organised Crime Agency have been amended by the Crime and Courts Act 2013, www.legislation.gov.uk/ukpga/2013/22.

[32] References in RIPA to HM Customs and Excise and Inland Revenue have been amended by the Commissioners for Revenue and Customs Act 2005.

These and additional relevant public authorities are listed in the Regulation of Investigatory Powers (Communications Data) Order 2010[33] and any similar future orders made under section 25 of the Act.

Communications Data

2.12 The code covers any conduct relating to the exercise of powers and duties under Chapter II of Part I of RIPA to acquire or disclose communications data. Communications data is defined in section 21(4) of RIPA.

2.13 The term 'communications data' embraces the 'who', 'when', 'where', and 'how' of a communication but not the content, not what was said or written.

2.14 It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of 'dial through' fraud and other crimes, where data is passed on to activate communications apparatus in order to obtain communications services fraudulently).

2.15 It can include the address on an envelope, the time and duration of a communication, the telephone number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It can also include data relating to unsuccessful call attempts i.e. when the person being dialled does not answer the call, but where the network has been able to connect it successfully. It does not include data relating to an unconnected call i.e. when a call is placed, but the network is unable to carry it to its intended recipient. It covers electronic communications (not just voice telephony) and also includes postal services.[34]

2.16 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services[35] or telecommunications services.[36] DRIPA[37] clarified the definition of telecommunications service in section 2 of RIPA to make explicit that provision of access to systems for the creation, management or storage of communications is included in the provision of a service.

---

33 See article 3, SI 2010/480.

34 Note that data retained under DRIPA may only be data relating to electronic communications, including telephony, but does not include postal services. See the Data Retention Code of Practice for further details.

35 Sections 2(1) and 81(1) of the Act define 'postal service' to mean any service which consists in the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items and is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

36 See footnote 4.

37 Section 5 of DRIPA.

2.17 'Communications service providers' may therefore include those persons who provide services where customers, guests or members of the public are *provided* with access to *communications services* that are ancillary to the provision of another service, for example in hotels, restaurants, libraries and airport lounges.

2.18 In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of further communications data for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

2.19 Consultation with the public authority's Single Point of Contact (SPoC)[38] will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers, though it is the designated person who ultimately decides which of the CSPs should be given a notice. With the proliferation of modern communications media, including mobile telephony, internet communications, and social networks, and given that one individual can use many different forms of communications, the knowledge and experience of the SPoC in providing advice and guidance to the designated person is significant in ensuring appropriateness of any action taken to acquire the data necessary for an investigation. If a CSP, having been given a notice, believes that in future another CSP is better placed to respond, they should approach the authority to inform them of their view after disclosing the relevant data that they hold.

2.20 Any conduct to determine the CSP that holds, or may hold, specific communications data is not conduct to which the provisions of Chapter II apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service, such as a particular telephone number or an internet protocol address.

2.21 Communications data is defined as:

- traffic data (as defined by sections 21(4)(a) and 21(6) of RIPA) – this is data that is or has been comprised in or attached to a communication for the purpose of its transmission (see section starting at paragraph 2.24 of this code for further detail);
- service use information (as defined by section 21(4)(b) of RIPA) – this is the data relating to the use made by a person of a communications service (see section starting at paragraph 2.28 of this code for further detail); and
- subscriber information (as defined by section 21(4)(c) of RIPA) – this relates to information held or obtained by a CSP about persons[39] to whom the CSP provides or has provided a communications services. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it (see section starting at paragraph 2.30 of this code for further detail).

---

[38] See sub-section on the single point of contact, beginning at paragraph 3.19.

[39] Section 81(1) of RIPA defines 'person' to include any organisation and any association or combination of persons.

2.22 The data available on individuals, and the level of intrusion, differs between the categories of data. The public authorities which can acquire the data and, in some cases, the level of seniority of the designated person differ according to the categories of data in question.[40]

2.23 Where an applicant is unsure of the category of data they are seeking (traffic, service use or subscriber information) or what additional communications data may be retained by a CSP for their own business use, the applicant should discuss this with their SPoC. If a SPoC or designated person wish to find out more, they should consult the relevant CSP or contact the College of Policing CD Knowledge and Engagement Team (KET), ketadmin@college.pnn.police.uk.

Traffic Data

2.24 RIPA defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of RIPA. This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

- identifies, or appears to identify, any person, apparatus[41] or location to or from which a communication is or may be transmitted;
- identifies or selects, or appears to identify or select, transmission apparatus;
- comprises signals that activate apparatus used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud); or
- identifies data as data comprised in, or attached to, a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

2.25 Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page. For example, the fact that a subject of interest has visited pages at http://www.gov.uk/ can be acquired as communications traffic data (if available from the CSP), whereas that a specific webpage that was visited is http://www.gov.uk/government/collections/ripa--forms-2 may not be acquired as communications data (as it would be content).

2.26 Examples of traffic data, within the definition in section 21(6), include:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

[40] See SI 2010/480.

[41] 'Apparatus' is defined in section 81(1) of RIPA to mean 'any equipment, machinery, device, wire or cable'.

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation,[42] file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;
- records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address; and
- online tracking of communications (including postal items and parcels).

2.27 Any message written on the outside of a postal item, which is in transmission, may be content (depending on the author of the message) and fall within the scope of the provisions for interception of communications. For example, a message written by the sender will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is traffic data within section 21(4)(a) of RIPA.

Service Use Information

2.28 Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of RIPA.

2.29 Service use information is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time. Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called);[43]
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;

---

[42] Note that how a CSP processes and generates data relating to an IP address affects the category of communications data it falls into. Unless stored as subscriber or service use information by the CSP (as is often the case for a static IP address), IP addresses should be treated as traffic data. See also the section on subscriber information below.

[43] Itemised bills can include an indication of the cost for receiving communications, for example calls and messages received by a mobile telephone that has been 'roaming' on another network.

- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls; and
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber Information

2.30 The third type of communications data, widely known as 'subscriber information', is set out in section 21(4)(c) of RIPA. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

2.31 Examples of data within the definition at section 21(4) (c) include:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;
- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services, and potentially static IP addresses;[44]
- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;[45] and

[44] It is worth highlighting that, as noted in proceeding paragraphs on traffic data, IP addresses can be allocated as static addresses, in which case they are often stored by the CSP as subscriber information. However, if the IP is dynamic, the address may only be stored as traffic data. It is particularly important to be aware of this as there can be differences in the seniority of the designated person authorising access to subscriber and traffic data.

[45] This includes PUK (Personal Unlocking Key) codes for mobile phones. These are initially set by the handset manufacturer and are required to be disclosed in circumstances where a locked handset has been lawfully seized as evidence in criminal investigations or proceedings.

- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is *not* disclosed save where the requirement for such information is necessary in the interests of national security).[46]

2.32 It will often be appropriate to undertake the acquisition of subscriber information before obtaining related traffic data or service use information to confirm information within the investigation or operation.

2.33 However, where there is sufficient provenance of information within the investigation or operation to justify an application to obtain traffic data or service use information in the first instance, this may be undertaken. For example, in circumstances where:

- a victim reports receiving nuisance or threatening telephone calls or messages;
- a person who is subject of an investigation or operation is identified from high-grade intelligence to be using a specific communication service;
- a victim, a witness or a person who is subject of an investigation or operation has used a public payphone;[47]
- a person who is subject of an investigation or operation is identified during a time critical investigation (such as a kidnap) or from detailed analysis of data available to the investigator to be using a specific communication service;
- a mobile telephone is lawfully seized and communications data is requested relating to either or both the device or its SIM card(s);
- a witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed; or
- an investigation of the allocation of IP addresses is needed to determine relevant subscriber information.[48]

2.34 Where the acquisition of the subscriber information is required to assist an investigation or operation or for evidential purposes, that requirement can be included on an application for traffic data or service use information.

2.35 Additional types of data may fall into the category of subscriber information, as communications services have developed and broadened, for example where a CSP chooses to collect information about the devices used by their customers. Prior to the acquisition of data which does not fall into the illustrative list of traditional subscriber information above, specific consideration should be given to whether it is particularly sensitive or intrusive, in order to ensure that such a request is still necessary and proportionate, and compliant with Chapter II.

---

[46] Information which provides access to the content of any stored communications may only be used for that purpose with necessary lawful authority.

[47] The telephone number and address of a public payphone is normally displayed beside it to assist persons making emergency calls to give their location to the emergency operator.

[48] See footnotes 42 and 44 for certain clarification regarding acquisition of IP addresses, as an IP address, in different circumstances, can be traffic data or subscriber information.

Further Guidance on Necessity and Proportionality

2.36 Training regarding necessity and proportionality should be made available to all those who participate in the acquisition and disclosure of communications data.

Necessity

2.37 In order to justify that an application is necessary, the application needs as a minimum to cover three main points:

- the event under investigation, such as a crime or vulnerable missing person;
- the person, such as a suspect, witness or missing person, and how they are linked to the event; and
- the communications data, such as a telephone number or IP address, and how this data is related to the person and the event.

2.38 Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

2.39 Applications should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

2.40 This should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a phone number may be obtainable from a phone book or other publically available sources.

2.41 The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

2.42 An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

2.43 Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation. Consideration of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

2.44 An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when, relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

2.45 Unintended consequences are more likely in more complicated requests for traffic data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for service use data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered. The special considerations that arise in such cases are discussed further in the section on "Communications data involving certain professions".

3 General rules on the granting of Authorisations and giving of Notices

3.1 Acquisition of communications data under RIPA involves four roles within a relevant public authority:

- the applicant;
- the designated person;
- the single point of contact; and
- the senior responsible officer

3.2 RIPA provides two alternative means for acquiring communications data, by way of:

- an authorisation under section 22(3); or
- a notice under section 22(4).

An authorisation granted to a member of a public authority permits that person to engage in conduct relating to the acquisition and disclosure of communications data under Part I Chapter II of RIPA. A notice given to a postal or telecommunications operator requires it to disclose the relevant communications data held by it to a public authority, or to obtain and disclose the data, when it is reasonably practicable for them to do so. Both authorisations and notices are explained in more detail within this chapter.

The applicant

3.3 The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data.

3.4 An application may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible, and certainly within one working day (paragraphs 3.65 - 3.71 provide more detail on urgent procedures).

3.5 An application[49] – the original or a copy of which must be retained by the SPoC within the public authority – must:

- include the name (or designation[50]) and the office, rank or position held by the person making the application;

[49] Public authorities should ensure their application processes are efficient and do not impose unnecessary bureaucracy on their operational staff which goes beyond the requirements of RIPA and this code. To assist public authorities the Home Office publishes specimen forms, available at https://www.gov.uk/government/collections/ripa-forms--2 .

- include a unique reference number;
- include the operation name (if applicable) to which the application relates;
- specify the purpose for which the data is required, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;[51]
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- identify and explain the time scale within which the data is required.[52]

3.6 The application should record subsequently whether it was approved by a designated person, by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted[53] or notice given.

---

50 The use of a designation rather than a name will be appropriate only for applicants in one of the security and intelligence agencies.

51 See sub-section on further guidance on necessity and proportionality, beginning at paragraph 2.36. This also applies to the next two bullets on collateral intrusion and unintended consequences.

52 The National Policing/Communications Industry (NPCI) Communications Data Strategy Group (CDSG), (formerly known as the ACPO Data Communications Group, DCG) which comprises representatives of CSPs, UK law enforcement and other public authorities to manage the strategic relationship between public authorities and the communications industry has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data. There are three grades:

- Grade 1 – an immediate threat to life;
- Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security; and
- Grade 3 – matters that are routine but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime.

The emphasis within Grade 1 and 2 is that the urgent provision of the communications data will have an immediate and positive impact on the investigation or operation.

53 Cross-referencing will be unnecessary in circumstances where the grant of an authorisation is recorded in the same document as the relevant application.

The designated person

3.7 The designated person is a person holding a prescribed office in a relevant public authority.[54] It is the designated person's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in writing or electronically. If the designated person believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.[55]

3.8 Individuals who undertake the role of a designated person must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II and this code.

3.9 When considering proportionality, the designated person should apply particular consideration to unintended consequences. The seniority, experience and training of the designated person provides them with a particular opportunity to consider possible unintended consequences.

3.10 Designated persons must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a designated person of their office, rank or position in the relevant public authority may grant or give.

3.11 The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the single point of contact (SPoC).

3.12 Designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations.

3.13 Except where it is necessary to act urgently, in circumstances where a public authority is not able to call upon the services of a designated person who is independent from the investigation or operation, the Senior Responsible Officer must inform the Interception of Communications Commissioner of the circumstances and reasons (noting the relevant designated persons who, in these circumstances, will not be independent). These may include:

- small specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies; and
- public authorities which have ongoing operations or investigations immediately impacting on national security issues and are therefore not able to a call upon a designated person who is independent from their operations and investigations.

[54] See article 4, SI 2010/480.

[55] Details on necessity and proportionality are included in section 2 and further information is in the 'Guidance note for Chapter II application', available at https://www.gov.uk/government/collections/ripa-forms--2.

3.14 In all circumstances where public authorities use designated persons who are not independent from an operation or investigation this must be notified to the Commissioner at the next inspection. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

3.15 Where a designated person is not independent from the investigation or operation their involvement and their justification for undertaking the role of the designated person must be explicit in their recorded considerations.

3.16 Particular care must be taken by designated persons when considering any application to obtain communications data to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown.[56] Unless the application is based on information that the apparatus was used or was likely to have been used in a particular location or locations at a particular time or times it will, in practice, be rare that any conduct to obtain communications data will be proportionate or the collateral intrusion justified.

3.17 In situations where there is an immediate threat to life (for example a person threatening to take their own or someone else's life or where threats are made to a victim in a kidnap) some CSPs will undertake to adapt their systems beyond the requirements of their normal business practice to be able to assist the police in preserving life. The use of such bespoke systems must be proportionate, and any collateral intrusion justified, to the specific circumstances of any investigation or operation.

3.18 Where there is no immediate threat to life in an investigation or operation, any conduct to obtain communications data using any other bespoke systems (for example, those used to trace malicious and nuisance communications) must be reliant upon both the co-operation and technical capability of the CSP to provide such assistance outside of its normal business practice.

The single point of contact

3.19 The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Despite the name, in practice many organisations will have multiple SPoCs, working together. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier.[57] SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. Details of all accredited individuals are available to CSPs for authentication purposes.

[56] Communications Data Strategy Group is able to offer additional advice to SPoCs where investigations or operations in their public authority are considering the acquisition of such data.

[57] At the time of writing, the authentication identifier is a SPoC Personal Identification Number ('SPoC PIN').

3.20 Communications data should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate.[58] When handling, processing, and distributing such information, SPoCs must comply with local security policies and operating procedures. The SENSITIVE caveat is for OFFICIAL information that is subject to 'need to know' controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that communications data must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts. Communications data acquired by public authorities must also by stored and handled in accordance with duties under the Data Protection Act.[59]

3.21 An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a 'guardian and gatekeeper' function ensuring that public authorities act in an informed and lawful manner.

3.22 The SPoC[60] should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;
- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;[61]
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- advise applicants and designated persons on the interpretation of RIPA, particularly whether an authorisation or notice is appropriate;
- provide assurance to designated persons that authorisations and notices are lawful under RIPA and free from errors;
- consider and, where appropriate, provide advice to the designated person on possible unintended consequences of the application;
- provide assurance to CSPs that authorisations and notices are authentic and lawful;

---

58 For those authorities that do not use the Government Security Classifications, details can be found at https://www.gov.uk/government/publications/government-security-classifications. Those who do not use these classifications should treat information in the appropriately equivalent manner under their data security rules.

59 Please see Chapter 7 for further details of data protection safeguards.

60 Advice and consideration given by the SPoC in respect of any application may be recorded in the same document as the application and/or authorisation.

61 In the event that the required data is inextricably linked to, or inseparable from, other traffic data or service use data, the designated person must take that into account in their consideration of necessity, proportionality, collateral intrusion and unintended consequences.

- assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;
- assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation; and
- assess any cost and resource implications to both the public authority and the CSP of data requirements.

3.23 The SPoC would normally be the person who takes receipt of any communications data acquired from a CSP (see paragraphs 3.33 and 3.49) and would normally be responsible for its dissemination to the applicant.

3.24 Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data. Nonetheless, in the course of a joint investigation between authority A with no SPoC and authority B with RIPA communications data acquisition powers, authority B may, where necessary and proportionate, acquire communications data under RIPA to further the joint investigation.

3.25 In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of RIPA, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of both the person's accreditation and their SPoC authentication identifier is obtained from the Home Office.

3.26 For each individual application, the roles of SPoC and designated persons will normally be carried out by two persons. In exceptional cases,[62] such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPoC or the designated person.

3.27 For each individual application, the roles of SPOC and Applicant will also normally be carried out by two persons. In exceptional cases,[63] such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPOC or the Applicant.

3.28 The same person must never be both the applicant and the designated person. Clearly, therefore, the same person should never be an applicant, a designated person and a SPoC.

3.29 Where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of RIPA) or using statutory powers conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

---

[62] Where specific, specialist units, particularly those involved in sensitive work, have undertaken streamlining to ensure better application of the principles of this code, these will generally be considered to be exceptional cases.

[63] See previous footnote.

3.30 Occasionally public authorities will wish to request data from CSPs that is neither communications data nor the content of communications. Given the training undertaken by a SPoC and the on-going nature of a SPoC's engagement with CSPs, it is good practice to engage the SPoC to liaise with the CSP on such requests.

The senior responsible officer

3.31 Within every relevant public authority a senior responsible officer[64] must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of RIPA and with this code;
- oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

Authorisations

3.32 An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data.

3.33 Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems.[65] This will normally be the public authority's SPoC, though local authorities must now use the National Anti-Fraud Network (see later in this chapter for more details).

3.34 The decision of a designated person whether to grant an authorisation shall be based upon information presented to them in an application.

[64] The senior responsible officer should be a person holding the office, rank or position of a designated person within the public authority who may authorise communications falling within section 21(4)(a) and or 21(4)(b).

[65] If there is a collaboration agreement between police forces under the Police Act 1996, as amended by the Policing and Crime Act 2009, a designated person from another force under the agreement may authorise the relevant conduct.

3.35 An authorisation may be appropriate where:

- a CSP is not capable of obtaining or disclosing the communications data;[66]
- there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data;[67] or
- a designated person considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

3.36 An authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself.

3.37 An authorisation[68] – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be granted in writing or, if not, in a manner that produces a record of it having been granted;
- describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 22(2) of RIPA;
- specify the office, rank or position held by the designated person granting the authorisation. The designated person should also record their name (or designation) on any authorisation they grant; and
- record the date and, when appropriate to do so, the time[69] when the authorisation was granted by the designated person.

3.38 SPoCs should be mindful, when drafting authorisations within the meaning of section 23(1) of RIPA, to ensure the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in authorisations, particularly via communications data acquisition systems.[70]

---

66 Where possible, this assessment will be based upon information provided by the CSP.

67 In order to facilitate the secure and swift disclosure of communications data many CSPs have systems in place to ensure accurate and timely acquisition to communications data, while maintaining security and an audit trail. Increasing the speed of communications data responses is a key objective of the Home Office.

68 Where the grant of an authorisation is recorded separately from the relevant application they should be cross-referenced to each other.

69 Recording of the time an authorisation is granted (or a notice is given) will be appropriate in urgent and time critical circumstances.

70 The College of Policing Knowledge and Engagement Team (KET) can provide advice to SPoCs on how best to ensure up-to-date knowledge of data types. Contact details for the KET are in Chapter 9.

3.39 Requirements to identify a person to whom a service is, or has been, provided – for example telephone number subscriber checks – account for the vast majority of disclosures under RIPA. As a consequence of these requirements, some CSPs permit the lawful acquisition of this data by SPoCs, via secure auditable communications data acquisition systems. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data.[71]

3.40 At the time of giving a notice or granting an authorisation to obtain specific traffic data or service use data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific subscriber information relating to the traffic data or service use data to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

- to identify with whom a victim was in contact, within a specified period, prior to their murder;
- to identify, where the target of an investigation or operation has been observed to make several calls from a public pay phone, the recipient of those calls;
- to identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence); and
- where a victim or a witness has identified a specific communication or communications and corroboration of facts may reveal a potential offender or other witness.

3.41 At the time of giving a notice or granting an authorisation to obtain specific traffic data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of traffic data or service use information. This is relevant where there is a necessary and proportionate requirement to identify a person from the traffic data to be acquired, and the means to do so requires the CSP or another CSP to query their traffic data or service use information, for example:

- the CSP does not collect information about the customer within their customer information system but retains it in its original form as traffic data (such as a MAC or IMEI or an IP address); or
- where evidence or intelligence indicates there are several CSPs involved in routing a communication and there is a requirement to establish the recipient of the communication.

[71] Where details of an authorisation are provided to a CSP in writing, electronically or orally, those details must additionally specify the manner in which the data should be disclosed and, where appropriate, provide an indication of any urgency or time within which the data need to be obtained.

3.42 It is the duty of the senior responsible officer to ensure that the designated person, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of subscriber information to be obtained directly upon the acquisition or disclosure of any traffic data or service use data, and their compliance with Chapter II and with this code.[72]

Notices

3.43 The giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, unless the grant of an authorisation is more appropriate. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.[73]

3.44 The decision of a designated person whether to give a notice shall be based on information presented to them in an application.

3.45 The 'giving of a notice' means the point at which a designated person determines that a notice should be given to a CSP. In practice, once the designated person has determined that a notice should be given, it will be served upon a CSP in writing[74] or, in an urgent situation, communicated to the CSP orally.[75]

3.46 The notice should contain enough information to allow the CSP to comply with the requirements of the notice.

3.47 A notice – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be given in writing[76] or, if not, in a manner that produces a record, within the public authority, of its having been given;
- include a unique reference number and also identify the public authority;[77]
- specify the purpose for which the notice has been given, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s)and, where appropriate, time period(s);
- include an explanation that compliance with the notice is a requirement of RIPA;

---

[72] Ordinarily the applicant or other person within the investigation or operation will prepare a schedule of data, for example telephone numbers, to enable the SPoC to undertake the acquisition of subscriber information. The schedule will include details of the person who prepared it, cross reference it to the relevant notice or authorisation and specify the traffic data or service use information from which the data are derived.

[73] Please see also paragraphs 3.46-3.48 below that provide further detail on what is entailed here.

[74] 'In writing' can include, but is not limited to, letter, fax, email, and via a secure portal operated by the CSP.

[75] Further detail on 'Urgent oral giving of notice or grant of authorisation' begins at paragraph 3.65.

[76] The preparation and format of a notice must take into account that, when served on a CSP by the use of a facsimile machine or other means, the notice must remain legible.

[77] This can be a code or an abbreviation. It could be that part of a public authority's name which appears in its e-mail address. For police services it will be appropriate to use the Police National Computer (PNC) force coding.

- specify the office, rank or position held by the designated person giving the notice. The name (or designation) of the designated person giving the notice should also be recorded;
- specify the manner in which the data should be disclosed. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;
- record the date and, when appropriate to do so, the time when the notice was given by the designated person; and
- where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice.[78]

3.48 A notice must not place a CSP under a duty to do anything which it is not reasonably practicable for the CSP to do.[79] SPoCs should be mindful of the need to draft notices to ensure the description of the required data corresponds with the ways in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in notices.

3.49 In giving notice a designated person may only require a CSP to disclose the communications data to the designated person or to a specified person working within the same public authority. This will normally be the public authority's SPoC.

3.50 Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a notice relates not later than the end of the period of ten working days from the date the notice is served upon the CSP.

Duration of authorisations and notices

3.51 An authorisation or notice becomes valid on the date upon which authorisation is granted or notice given. It is then valid for a maximum of one month.[80] This means the conduct authorised should have been commenced or the notice served within that month.

[78] See footnote 52.

[79] See section 22(7) of RIPA. SPoCs, Designated Persons or CSPs may contact the KET if they require further advice on what is reasonably practicable in a particular circumstance.

[80] Throughout this code, a month means a period of time extending from a date in one calendar month to the date one day before the corresponding or nearest date in the following month. For example, a month beginning on 7 June ends on 6 July; a month beginning on 30 January ends on 28 February or 29 February in a leap year.

3.52 All authorisations and notices should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s).[81] Any period should be clearly indicated in the authorisation or notice. The start date and end date should be given, and where a precise start and end time are relevant these must be specified.[82] Where the data to be acquired or disclosed is specified as 'current', the relevant date should be taken to be the date on which the authorisation was granted or the notice given by the designated person. There can be circumstances when the relevant date or period cannot be specified other than 'the last transaction' or 'the most recent use of the service'.

3.53 Where an authorisation or a notice relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted or the notice given.

3.54 Designated persons should specify the shortest possible period of time for any authorisation or notice. To do otherwise would impact on the proportionality of the authorisation or notice and impose an unnecessary burden upon the relevant CSP(s).

Renewal of authorisations and notices

3.55 Any valid authorisation or notice may be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

3.56 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation or notice being renewed was granted or given.

3.57 Where a designated person is granting a further authorisation or giving a further notice to renew an earlier authorisation or notice,[83] the designated person should:

- have considered the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and
- record the date and, when appropriate to do so, the time when the authorisation or notice is renewed.

[81] For example, details of traffic data or service use on a specific date or for a specific period or the details of a subscriber on a specific date or for a specific period.

[82] In the case of Internet Protocol data, any timings should include an explicit indication of which time zone applies to those timings.

[83] This can include an authorisation or notice that has been renewed previously.

Cancellation of notices and withdrawal of authorisations

3.58 A designated person who has given notice to a CSP under section 22(4) of RIPA shall cancel the notice if, at any time after giving the notice,[84] it is no longer necessary for the CSP to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

3.59 Reporting the cancellation of a notice to a CSP shall be undertaken by the designated person directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated person or the SPoC will notify the CSP.[85]

3.60 Cancellation of a notice reported to a CSP must:

- be undertaken in writing or, if not, in a manner that produces a record of the notice having been cancelled;
- identify, by reference to its unique reference number, the notice being cancelled; and
- record the date and, when appropriate to do so, the time when the notice was cancelled.

3.61 In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the designated person must confirm the decision in writing for the SPoC or, if not, in a manner that produces a record of the notice having been cancelled by the designated person. Where the designated person who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the designated person.

3.62 Similarly where a designated person considers an authorisation[86] should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation must be withdrawn. It may be the case that it is the SPoC or the applicant who is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant, where appropriate) may cease the authorised conduct, and then inform the designated person who granted the authorisation.

---

[84] This can include a renewed notice.

[85] If the notice being cancelled relates to an urgent operational situation that has been resolved, or has changed, it may be appropriate for the senior officer dealing with the situation, on the ground or in a control room, to notify the CSP that the notice is cancelled where that person has the earliest opportunity to do so.

[86] This can include a renewed authorisation.

3.63 Withdrawal of an authorisation should:

- be undertaken in writing or, if not, in a manner that produces a record of it having been withdrawn;
- identify, by reference to its unique reference number, the authorisation being withdrawn;
- record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- record the name and the office, rank or position held by the designated person informed of the withdrawal of the authorisation.

3.64 When it is appropriate to do so, a CSP should be advised of the withdrawal of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

Urgent oral giving of notice or grant of authorisation

3.65 In exceptionally urgent circumstances,[87] an application for the giving of a notice or the grant of an authorisation may be made by an applicant, approved by a designated person and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate include:

- an immediate threat of loss of human life, or for the protection of human life, such that a person's life might be endangered if the application procedure were undertaken in writing from the outset;[88]
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime[89] and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset; or
- a credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

3.66 The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process. It must be clear in each case why it was not possible, in the circumstances, to use the standard, written process.

---

87 There is a general undertaking by CSPs to respond outside of normal office hours where there is an immediate threat to life.

88 This may include safeguarding the welfare of vulnerable people, including children at imminent risk of being abused or otherwise harmed.

89 See section 81(2) of RIPA.

3.67 When, in a matter of urgency, a designated person decides, having consulted the SPoC, that the oral giving of a notice or grant of an authorisation is appropriate, that notice should be given or the authorised conduct undertaken as soon as practicable after the making of that decision.

3.68 Particular care must be given to the use of the urgent oral process. When notice or authorisation is given orally, the SPoC, when relaying service of the oral notice or authorisation to the CSP, must make a note of the time, provide a unique reference number for the notice, provide the name (or designation) of the designated person and the name and contact details of the SPoC and, if required by the CSP, their authentication identifier.[90] Where telephone numbers (or other identifiers) are being relayed, the relevant number must be read twice and repeated back by the CSP to confirm the correct details have been taken.

3.69 Written notice[91] must be given to the CSP retrospectively within one working day[92] of the oral notice being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority (see the section on errors in Chapter 6, Keeping of Records, for more details).

3.70 After the period of urgency,[93] a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated person and the actions taken in respect of the decision(s).

3.71 In all cases where urgent oral notice is given or authorisation granted, an explanation of why the urgent process was undertaken must be recorded.

---

90 At the time of writing, this is the SPoC PIN.

91 Likewise where details of an authorisation are provided to a CSP orally in a matter of urgency, they should be confirmed in writing within one working day.

92 Working day means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in that part of the United Kingdom where the relevant public authority is located.

93 In some instances where life is at risk, for example in kidnap investigations, the period of urgency may be prolonged.

Communications data involving certain professions

3.72 Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.

3.73 However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament,[94] or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

3.74 Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

3.75 Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see section 6 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner.

3.76 Issues surrounding the infringement of the right to freedom of expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where an application is intended to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest, and the guidance at paragraphs 3.78–3.84 should be followed.

3.77 Where the application is for communications data of a journalist, but is not intended to determine the source of journalistic information (for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation), there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. The necessity and proportionality assessment also needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought. The application should draw attention to these matters.

[94] References to a Member of Parliament include references to a Member of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

Applications to determine the source of journalistic information

3.78 In the specific case of an application for communications data, which is made in order to identify a journalist's source, and until such time as there is specific legislation to provide judicial authorisation for such applications, those law enforcement agencies, including the police, National Crime Agency and Her Majesty's Revenue and Customs, in England and Wales with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data. Relevant law enforcement agencies in Northern Ireland must apply for a production order under the PACE (Northern Ireland Order) 1989. Law enforcement agencies in Scotland must use the appropriate legislation or common law powers to ensure judicial authorisation for communications data applications to determine journalistic sources.

3.79 Communications data that may be considered to determine journalistic sources includes data relating to:

- journalists' communications addresses;
- the communications addresses of those persons suspected to be a source; and
- communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

3.80 Each authority must keep a central record of all occasions when such an application has been made, including a record of the considerations.

3.81 This includes that, where the police suspect wrong-doing that includes communications with a journalist, the application must consider properly whether that conduct is criminal and of a sufficiently serious nature for rights to freedom of expression to be interfered with where communications data is to be acquired for the purpose of identifying a journalist's source.

3.82 As described in paragraph 3.29 above, the SPoC should be engaged in this process, to ensure appropriate engagement with the CSPs.

3.83 If and only if there is a believed to be an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, law enforcement agencies may continue to use the existing internal authorisation process under RIPA. Such applications must be flagged to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. If additional communications data is later sought as part of the same investigation, but where a threat to life no longer exists, judicial authorisation must be sought.

3.84 The requirement for judicial oversight does not apply where applications are made for the communications data of those known to be journalists but where the application is not to determine the source of journalistic information. This includes, for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

Local authority authorisation procedure

3.85 Local authorities must fulfil two additional requirements when acquiring communications data that differ from other public authorities. Firstly, the request must be made through a SPoC at the National Anti-Fraud Network ('NAFN'). Secondly, the request must receive prior judicial approval.

3.86 NAFN provides shared SPoC services to local authorities. Local government legislation allows for NAFN to act on behalf of local authorities within England and Wales, Scotland and Northern Ireland for certain functions.[95] From 1 December 2014 all local authorities who wish to acquire communications data under RIPA are required to become members of NAFN and use their shared SPoC services. This means that applicants within local authorities are required to consult a NAFN SPoC throughout the authorisation process, including before referring the case to a designated person for approval. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to applicants and designated persons ensuring the local authority acts in an informed and lawful manner.

3.87 Under sections 23A and 23B of RIPA judicial approval must also be granted for all local authority requests for communications data.[96] Judicial approval must be requested once all the internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. In England, Wales and Northern Ireland the authorisation must be provided by a magistrate; in Scotland a sheriff. The local authority, rather than NAFN, is responsible for submitting the application for judicial authorisation. It is for the local authority to decide on the most appropriate representative to present their RIPA application to the magistrate or sheriff. The judicial application must include relevant documentation, including the original RIPA authorisation or notice. Once the case has been heard, the magistrate or sheriff will complete a judicial order outlining their decision. Should authorisation be granted, the local authority will provide the judicial order to the NAFN SPoC.

[95] The Local Government Act 1972; Local Government Act (Scotland) 1973; and Local Government Act (Northern Ireland) 2014.

[96] RIPA as amended by the Protection of Freedoms Act 2012.

4 Making of contributions towards the costs incurred by communications service providers

4.1 RIPA[97] recognises that CSPs incur costs in complying with notices to disclose communications data, and allows for arrangements for making appropriate payments to them to facilitate the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a CSP should disclose data within ten working days of being required to do so. Similar arrangements are appropriate where a CSP incurs costs in making provision for the acquisition of communications data upon the grant of an authorisation under RIPA.

4.2 Significant public funding is made available to CSPs to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate and lawful requirements for the disclosure and acquisition of communications data in support of their investigations and operations to protect the public and to bring to justice those who commit crime.

4.3 It is legitimate for a CSP to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to comply with notices or to provide for the acquisition and timely disclosure of communications data.

4.4 This is especially relevant for CSPs which employ staff specifically to manage compliance with the requirements made under RIPA, supported by bespoke information systems.

4.5 Contributions may also be appropriate towards costs incurred by a CSP which needs to update its systems to maintain, or make more efficient, its disclosure process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the disclosure and acquisition of communications data relating to the use of such services.

4.6 Any CSP seeking to recover appropriate contributions towards its costs should make available to the Home Office such information as the Home Office requires, in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the CSP.

4.7 As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure.

[97] Section 24 of RIPA.

5 Special rules on the granting of Authorisations and giving of Notices in specific matters of public interest

Sudden deaths, serious injuries, vulnerable and missing persons

5.1 There are circumstances when the police undertake enquiries in relation to specific matters of public interest where the disclosure of communications data may be necessary and proportionate. Section 22 (2)(g) of RIPA and article 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 specify certain purposes for which the acquisition and disclosure of communications data may be necessary. These purposes assist the police in carrying out its functions. For example:

- identifying any person who has died or who is unable to identify himself, because of a physical or mental condition, other than as a resulting from crime (such as a natural disaster or an accident);
- obtaining information about the reason for a person's death or condition;
- locating and notifying next of kin following a sudden or unexpected death;
- locating and notifying next of kin of a seriously injured person; and
- locating and notifying the next of kin or responsible adult of a child or other vulnerable person where there is a concern for the child's or the vulnerable person's welfare.

5.2 Often a telephone, telephone number or other communications details may be the only information available to identify a person or to identify their next of kin or a person responsible for their welfare.

5.3 Equally communications data can help establish the facts relevant to a person's death or serious injury, where no crime has occurred. For example, where the police undertake an investigation to assist Her Majesty's Coroner, communications data can indicate the activity of a deceased person prior to their death, such as in a fatal accident, or identify a person who may assist the Coroner to establish the facts of a person's death.

5.4 Under RIPA communications data may also be obtained and disclosed in serious and urgent welfare cases where it is necessary within the meaning of section 22(2)(g) and the conduct authorised or required is proportionate to what is sought to be achieved by obtaining the data.

Public Emergency Call Service (999/112 calls)

5.5 RIPA regulates the acquisition and disclosure of communications data for the statutory purposes in that Act, whereas, the Communications Act 2003 requires certain CSPs to provide communications data to the emergency services following an emergency call made to 999 and 112 emergency numbers.

5.6 The Communications Act 2003 requires CSPs to comply with obligations contained within the General Conditions of Entitlement, specifically, in the case of calls to 999 and 112 numbers, the General Condition 4 (GC4). To assist the emergency services and emergency operator further details in relation to handling 999 and 112 calls are contained within the Public Emergency Communications Service Code of Practice.

5.7 Handling of an emergency call involves four phases:

- connection of the caller to the Emergency Operator using the 999/112 number;
- selection by the emergency operator of the required Emergency Authority Control Room (police, fire, ambulance or coastguard) ('the emergency service');
- connection of the caller to the Emergency Authority Control Room; and
- listening by the Emergency Operator for a short while to ensure the caller is connected to the correct emergency service and to provide further assistance to the caller or the emergency service when required.[98]

5.8 This code is not intended to regulate those activities but to ensure the boundary between this code and the Public Emergency Communications Services Code of Practice is clear. In so doing this code recognises an emergency period of one hour after the termination of the emergency call in which disclosure of communications data to emergency services will largely fall outside the provisions of RIPA.

5.9 CSPs must ensure that any service user can access the emergency authorities by using the emergency numbers and, to the extent technically feasible, make caller location information available to the emergency authorities for all 999/112 calls. In practice this means sufficient detail to identify the origin of the emergency call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency.

5.10 It is usual for CSPs to disclose, at the time of the call, some identity (caller line identity) and caller location information data (fixed or mobile) to the emergency services in order to facilitate a rapid response to the emergency call. Caller location information, which provides the geographic position of the apparatus being used by the person making the emergency call, facilitates a fast response in emergency situations where the caller is unable to give their position (for example because the caller does not know, is panicking or is incapacitated).

5.11 For the purposes of GC4, 'caller location information' also means any data or information processed in an electronic communications network indicating the geographic position of the terminal apparatus of a person initiating a call.

---

[98] This can also include silent emergency calls where the call is connected but the caller, for whatever reason, is unable to speak to the emergency operator or the emergency service.

5.12 Where a CSP provides an electronic communication service at a fixed location, the caller location information must, at least, accurately reflect the fixed location of the end-user's terminal apparatus including the full postal address. In relation to the emergency calls made using a mobile network, the caller location information must include, at least, the cell identification of the cell from which the call is being made, or in exceptional circumstances the zone code.

5.13 CSPs should take steps to assure themselves of the accuracy of the information they may be called upon to disclose. Any known limitations in this accuracy, particularly for location, should be proactively disclosed to the emergency services.

5.14 The caller identity and location data information provided automatically at the start of the call might not be sufficient to enable the emergency services to respond effectively or efficiently to the emergency. An example is where emergency calls are 'dropped' or incomplete. There are a number of reasons for these 'dropped' or incomplete emergency calls, which cannot be reconnected. For example:

- there is a fault on the line;
- the emergency service requests to be reconnected where the caller was incapacitated or unable to maintain the call and reconnection is tried and fails;
- the emergency service considers that safety of the person making the call may be put at risk if the Emergency Operator seeks to reconnect the call, particularly in cases where a crime is in progress, for example domestic violence or a robbery; and
- the Emergency Operator diagnoses a problem with the call or the strength of a mobile phone signal.

5.15 The emergency service can call upon an Emergency Operator or relevant service provider to disclose data about the maker of an emergency call within the emergency period within one hour of the 999/112 call.[99]

5.16 It is appropriate for the emergency service or emergency operator to require the CSP to disclose any further caller location information that might indicate the location of the caller at the time of the emergency call. Within one hour of the 999/112 call, it is also appropriate for the CSP, acting in the belief that information might assist the emergency service to respond effectively or efficiently to the emergency, to proactively disclose to the emergency service or emergency operator any further Caller Location Information about the location of the caller at the time of the emergency call.

5.17 It is possible the emergency service might require additional assistance in locating the scene of an emergency. This might be where a caller is unsure of their exact location. In some emergency situations the location of the caller might change before the emergency services can provide assistance. This might occur where a crime is in progress, for example, an assault where the caller is fleeing from violent pursuer, or during a flood where the caller is moving to avoid rising water. It is also appropriate for the emergency services to request updated caller location information from the CSP and for this information to have been generated after and be unrelated to the original emergency call.

[99] For the sake of clarity, it is not intended that this emergency call related activity is regulated by RIPA.

5.18 If an emergency call is disconnected prematurely for any reason, technical or otherwise, and the Emergency Operator is aware or is made aware of this, then the Emergency Operator can elect to represent the data disclosed when the call was put to the emergency service initially. This voluntary disclosure would fall outside the scope of RIPA.

5.19 There are circumstances where the Emergency Operator cannot automatically present the emergency service with communications data about the maker of an emergency call. For example, because the emergency service does not have apparatus to receive the data automatically or the data is held by a third party service provider and not readily available to the Emergency Operator. In those circumstances, and in order to provide an effective emergency service, the Emergency Operator may disclose the data it has orally.

5.20 Some CSPs have provided secure auditable communications data acquisition systems for the disclosure of communication data under RIPA. Where these exist, it is appropriate for emergency services to be provided with accreditation details to use them for acquiring data about the maker of an emergency call or caller location information, as appropriate, during the emergency period. The emergency service should ensure:

- each emergency service operator using an secure auditable system is appropriately trained and has knowledge of the system and its limitations;
- the accreditation details provided are unique to an individual;,
- the emergency service operator provides a unique reference number for each emergency call;
- the emergency service operator provides the name of the designated person and sufficient detail to link the disclosure to the originator of the request; and
- records of compliance are retained and are available for inspection by the relevant oversight bodies as appropriate. Records should be retained for two years or as otherwise notified.

5.21 The CSP should ensure:

- the secure auditable communications data acquisition system is capable of recording all actions performed by an individual using the system; and
- records of compliance are retained and are available for inspection by the relevant oversight bodies as appropriate. Records should be retained for two years or as otherwise notified.

5.22 When a secure auditable system is not available, a manual request for data can be made. The Public Emergency Communications Service Code of Practice contains the process to be followed.[100]

[100] To be used with the Public Emergency Communications Service Code of Practice, there is a guide specifically for Emergency Operators and Emergency Authority Control Room staff about when it is appropriate to contact CSPs.

5.23 If the emergency call is clearly a hoax, there is no emergency. Where an emergency service concludes that an emergency call is a hoax and the reason for acquiring data in relation to that call is to detect the crime of making a hoax call – and not to provide an emergency service – then the application process under RIPA must be undertaken.

5.24 Should an emergency service require communications data relating to the making of any emergency call after the expiry of the emergency period of one hour from the termination of the call, that data must be acquired or obtained under the provisions of RIPA.

5.25 Where communications data about a third party (other than the maker of an emergency call) is required to deal effectively with an emergency call, the emergency service may make an urgent oral application for the data. Disclosure of that data would also fall within under the provisions of RIPA.

5.26 The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('the Privacy Regulations') allow telephone users the choice whether or not their telephone number is displayed or can be accessed by the recipient of a call they make. However when an emergency call using 999 or 112 is made, the option to withhold the number making the call is not available.

5.27 In view of the obligations contained within GC4 and the further assistance which might be necessary, CSPs should ensure that adequate provision is available around the clock to liaise with the emergency services as necessary. This provision can be satisfactorily achieved through a third party, as long as the contact information and process is declared to the emergency services in advance.

5.28 Increasingly, members of the public are using non emergency numbers to request assistance. Non emergency numbers such as 101 (for the police) and 111 (for NHS services) have been established to enable the public to contact the relevant authorities for routine enquiries. This might be to report a stolen car or to seek general health advice or information. The call will be answered by a call handler for the relevant service.

5.29 A caller might dial either 101 or 111 to seek non emergency assistance (or Crimestoppers on 0800 555 111 should they wish to report crime anonymously). In the case of calls to 101, 111 and other relevant non emergency assistance services, the call handler might believe it is more appropriate that an emergency response is made.[101] If insufficient details are available to provide an emergency response it is appropriate for the call handler to seek assistance using the 999/112 numbers if that act would speed up the provision of emergency assistance. If necessary, it is also appropriate for the call handler to contact a CSP to seek sufficient subscriber or other communications data, as are necessary and appropriate to assist with the provision of an emergency response.

5.30 RIPA does not seek to regulate either the actions of the call handler or the provision of data by the CSP.

Malicious and nuisance communications

5.31 Many CSPs offer services to their customers to deal with complaints concerning malicious and nuisance communications. Although these services vary, all CSPs believe that such calls can be very distressing for their customers and that every effort should be made to resolve such situations as efficiently and effectively as possible.

5.32 The victim of malicious or nuisance communications may, in the first instance, bring it to the attention of their CSP or report it to the police.

5.33 When contacted directly by a customer, the CSP may consider the circumstances of the complaint are such that the customer should be advised to report the matter without delay to the police for investigation.

5.34 Additionally the CSP can offer practical advice on how to deal with nuisance communications and may, for example, arrange a change of telephone number. The advice given by the CSP may indicate that the circumstances could constitute a criminal offence. The CSP may choose to disclose data to its customer relating to the source of the malicious or nuisance communications, but must ensure that the disclosure complies with the provisions of both the DPA and the Privacy Regulations.

[101] For example, when the health of the enquirer suddenly deteriorates or a suspect returns unexpectedly to the scene of a crime. A guide has been produced to ensure the request and disclosure of communications data between the CSP and the 101/111 call handlers in emergency situations is effective and efficient. This guide has been agreed between participating CSPs and has been distributed to the 101 and 111 call handlers – if operators of other non emergency numbers feel this guide would be relevant to them, they should contact the KET (ketadmin@college.pnn.police.uk). It sets out what records need to be retained in order that audit and oversight activities can take place. This emergency process is not to be used in support of activity to investigate hoax or malicious callers or for other situations where the call handler does not have a belief that an emergency situation has arisen. Where a call starts as a non-emergency but develops into an emergency call then paragraphs 5.16 and 5.17 would apply.

5.35 Upon receipt of a complaint a CSP may retrieve and retain relevant specific data that, if appropriate, can be disclosed to the police later. If the complainant wishes the matter to be investigated, it is essential for the CSP and the police[102] to liaise with one another to ensure the lawful disclosure of data to enable any offence to be effectively investigated.

5.36 Where the complainant reports a matter to the police that has been previously raised with the CSP, any data already collated by the CSP may be disclosed to the police SPoC under the provisions of the DPA or the Privacy Regulations.[103] Subsequent police investigation may require the acquisition or disclosure of additional communications data from the complainant's CSP or other CSPs under the provisions of RIPA.

5.37 Whether the initial complaint is reported to the CSP or directly to the police, careful consideration should be given to whether the occurrence of malicious or nuisance communications are, or may be, related to other incidents or events. Specifically, this could be where the complainant is a victim of another crime or is a witness or a member of a trial jury in ongoing or forthcoming criminal proceedings.

[102] Ordinarily this will be overseen and coordinated by the police force's SPoC.

[103] Regulation 15 concerns tracing of malicious or nuisance calls.

6 Keeping of records

Records to be kept by a relevant public authority

6.1 Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the relevant public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner.

6.2 These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions.[104]

6.3 Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant, those records must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.[105]

6.4 This code does not affect any other statutory obligations placed on public authorities to keep records under any other enactment. For example, where applicable in England and Wales, the relevant test given in the Criminal Procedure and Investigations Act 1996 ('the CPIA') as amended and the code of practice under that Act. This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

6.5 Each relevant public authority must also keep a record of the following information:

A. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally);

B. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;

C. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were approved after due consideration;

D. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

---

[104] The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is satisfied it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates. See section 67(5) of RIPA.

[105] Under section 15 of RIPA and the statutory code of practice on Interception of Communications.

E. the number of notices requiring disclosure of communications data (not including urgent oral applications);

F. the number of authorisations for conduct to acquire communications data (not including urgent oral applications);

G. the number of times an urgent application is approved orally;

H. the number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;

I. the priority grading of the application for communications data, as set out at paragraph 3.5 and footnote 52 of this code;

J. whether any part of the application relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion) (and if so, which profession);[106] and

K. the number of items of communications data sought, for each notice given, or authorisation granted (including orally).[107]

6.6 For each **item** of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following:

A. the Unique Reference Number (URN) allocated to the application, notice and/or authorisation;

B. the statutory purpose for which the item of communications data is being requested, as set out at section 22 (2) of RIPA;

C. where the item of communications data is being requested for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 22 (2) (b) of RIPA, the crime type being investigated;

D. whether the item of communications data is traffic data, service use information, or subscriber information, as described at section 21 (4) of RIPA, and Chapter 2 of this code;

E. a description of the type of each item of communications data included in the notice or authorisation;[108]

F. whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

G. the age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

H. where an item of data is service use information or traffic data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation;[109] and

---

[106] See paragraphs 3.72 – 3.74 on communications data involving certain professions for more information.

[107] One item of communications data is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of communications data.

[108] The data type is to include whether the data is telephone data, whether fixed line or mobile, or Internet data. It will also include a further breakdown of the data type, such as, in the case of fixed line telephone data, whether the item of communications data relates to incoming call data, outgoing call data, or both. Guidance on specific data types to be collected may be issued by, or sought from, IOCCO.

I. the CSP from whom the data is being acquired.

6.7 These records must be sent in written or electronic form to the Commissioner, as determined by him. Guidance on record keeping will be issued by IOCCO. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

6.8 The Interception of Communications Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a Communications Service Provider

6.9 To assist the Commissioner to carry out his statutory function in relation to Chapter II, CSPs should maintain a record of the disclosures it has made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from IOCCO.

6.10 The records to be kept by a CSP, in respect of each notice or authorisation, should include:

- the name of the public authority;
- the URN of the notice or authorisation;
- the date the notice was served upon the CSP or the authorisation disclosed to the CSP;
- a description of any communications data required where no disclosure took place or could have taken place;
- the date when the communications data was made available to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken; and
- sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court.[110]

Errors

6.11 Proper application of RIPA and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

[109] In the case of a forward facing notice or authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. This is because a forward facing notice or authorisation will often be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the notice or authorisation may be withdrawn subsequent to that communication being made.

[110] A digital signature would assist the court in verification of the origin and integrity of the data throughout the acquisition, investigation and prosecution process and would streamline record keeping.

6.12 An error can only occur after a designated person:

- has granted an authorisation and the acquisition of data has been initiated; or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

6.13 Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

6.14 Where any error occurs in the grant of an authorisation, the giving of a notice or as a consequence of any authorised conduct, or any conduct undertaken to comply with a notice, a record should be kept.

6.15 Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

6.16 In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

6.17 This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under RIPA;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- disclosure of the wrong data by a CSP when complying with a notice; and
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation.

Recordable errors

- a notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation;[111]

[111] In this context seeking the disclosure of communications data unnecessarily means any failure to collate or record information already obtained which results in repeatedly obtaining the same data within the same investigation or operation. This does not restrict a relevant public authority undertaking the acquisition of communications data where necessary and proportionate, for example to extend the time frame of communications data already obtained, which may include elements of data previously obtained, or as a consequence of new evidence.

- the requirement to acquire or obtain the data is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted; and
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

6.18 Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

6.19 When a reportable error has been made, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO within no more than five working days of the error being discovered. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and IOCCO of the report in written or electronic form. This will enable the CSP and IOCCO to investigate the cause or causes of the reported error.

6.20 The report sent to the IOCCO by a public authority in relation to a reportable error must include details of the error, identified by the public authority's unique reference number of the relevant authorisation or notice, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When a public authority reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the public authority must explain why the CSP has not been informed of the report).

6.21 Where a CSP discloses communications data in error, it must report each error to the IOCCO within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority. [112]

6.22 In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 9).

[112] This does not affect a CSP's statutory duty under regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 to notify the Information Commissioner of a personal data breach. Further guidance is available from the Information Commissioner's website, ico.org.uk

6.23 The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

6.24 Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

6.25 Communications identifiers can be readily transferred, or 'ported', between CSPs. When a correctly completed authorisation or notice results in a CSP indicating to a public authority that, for example, a telephone number has been 'ported' to another CSP, that authorisation or notice will not constitute an error – unless the fact of the porting was already known to the public authority.

Excess Data

6.26 Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

6.27 Where a public authority is bound by the CPIA and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid notice or authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

6.28 If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated person will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data (see next section).

7 Data Protection Safeguards

7.1 Communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the DPA[113] and its data protection principles must be adhered to.

7.2 Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

Disclosure of communications data and subject access rights

7.3 This section of the code provides guidance on the relationship between disclosure of communications data under RIPA and the provisions for subject access requests under the DPA, and the balance between CSPs' obligations to comply with a notice to disclose data and individuals' right of access under section 7 of the DPA to personal data held about them.

7.4 There is no provision in RIPA preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request[114] made under section 7 of the DPA.[115] However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.[116]

7.5 Section 28[117] of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

7.6 Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

[113] Guidance is available from www.justice.gov.uk/information-access-rights/data-protection *or* www.ico.org.uk.

[114] The Information Commissioner has produced a Subject Access Code of Practice to assist organisations adopt good practice when handling subject access requests, which is available at: ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

[115] This also applies to data retained under the Data Retention and Investigatory Powers Act 2014 and the Data Retention Regulations 2014 – see the Data Retention Code of Practice for more information.

[116] There may be other bars to disclosure in other legislation, for example regarding impeding an investigation.

[117] Section 28(2) makes clear that a certificate from a Minister of the Crown is conclusive evidence, though this can be challenged through appeal to a Tribunal.

7.7 The exemption to subject access rights possible under section 29 does not automatically apply to the disclosure of the existence of notices given under RIPA. In the event that a CSP receives a subject access request where the fact of a disclosure under RIPA might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the notice would be likely to prejudice the prevention or detection of crime.

7.8 Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29.[118]

7.9 Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

7.10 CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

Acquisition of communication data on behalf of overseas authorities

7.11 While the majority of public authorities which obtain communications data under RIPA have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.

7.12 There are two methods by which communications data, whether obtained under RIPA or not, can be acquired and disclosed to overseas public authorities:[119]

- judicial co-operation; or
- non-judicial co-operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

[118] The SPoC must provide a response which will enable the CSP to comply with its obligations to respond to the subject access request within 40 days.

[119] This includes public authorities within the Crown Dependencies and the British Overseas Territories.

Judicial co-operation

7.13 A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes a request for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the request for communications data included must be capable of satisfying the requirements of Part I Chapter II of RIPA.

7.14 If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 22 of RIPA and in line with the guidance in this code of practice.

7.15 In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

7.16 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of RIPA.

7.17 The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.18 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that.[120] Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

[120] The eighth data protection principle is: 'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.' (Paragraph 8, Schedule 1, DPA 1998). The Information Commissioner has produced guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

7.19 If the proposed transfer of data is to an authority within the European Union, that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.20 If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.[121]

7.21 In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle,[122] and, if necessary, his office can provide guidance.

7.22 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'.[123] There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis.

[121] The relevant Commission webpage is at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[122] See footnote 120.

[123] Paragraph 4, Schedule 4, DPA.

8 Oversight

8.1 RIPA provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of RIPA. The Commissioner is supported by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).[124]

8.2 This code does not cover the exercise of the Commissioner's functions. It is the duty of any person who uses the powers conferred by Chapter II, or on whom duties are conferred, to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

8.3 Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under RIPA in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable them to engage the Tribunal effectively.

8.4 Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available by the Commissioner to the Home Office to promulgate good practice and help identify training requirements within public authorities and CSPs.

8.5 Subject to the approval of the Commissioner, public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Chapter II of RIPA and this code. Approval should be sought on a case by case basis at least ten working days prior to intended publication, stating whether the report is to be published in full, and, if not, stating which parts are to be published or how it is to be summarised.

[124] The IOCCO website is http://www.iocco-uk.info.

9 Contacts / Complaints

General enquiries relating to Communications Data Retention & Acquisition

9.1 The Home Office is responsible for policy and legislation regarding communications data acquisition and disclosure. Any queries should be raised by contacting:

Communications Data Policy Team
Home Office
2 Marsham Street
London
SW1P 4DF

commsdata@homeoffice.x.gsi.gov.uk

9.2 The Knowledge Engagement Team within the College of Policing can provide advice and guidance to police and other public authorities in relation to their obligations under communications data legislation. The Knowledge Engagement Team can be contacted at:

ketadmin@college.pnn.police.uk

Complaints

9.3 RIPA established an independent Tribunal ('the Investigatory Powers Tribunal'). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under RIPA.

9.4 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW 1H 9ZQ

☎ 020 7035 3711

www.ipt-uk.com

ISBN 978-1-4741-1565-0