Home Office

Retention of Communications Data
Code of Practice

Pursuant to regulation 10 of the Data Retention Regulations 2014 and section 71 of the Regulation of Investigatory Powers Act 2000

Draft for public consultation
9 December 2014

Contents

1. Introduction

1.1. This code of practice, issued pursuant to section 71 of RIPA, relates to the powers and duties conferred or imposed under Part 1 of the Data Retention and Investigatory Powers Act 2014 ('DRIPA') and the Data Retention Regulations 2014 ('DRR 2014'). It provides guidance on the procedures to be followed when communications data is retained under those provisions.

1.2. This code applies to Communication Service Providers ('CSPs')[1] who have been issued with a data retention notice under DRIPA. Chapters 6, 7 and 8 also apply to those who retain data under the voluntary code of practice under the Anti-terrorism, Crime and Security Act 2001 ('ATCSA').

1.3. This code should be readily available to employees of a CSP involved in the retention of communications data, and be used in conjunction with the Acquisition and Disclosure of Communications Data Code of Practice by public authorities involved in the acquisition of communications data under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA').

1.4. A data retention notice under DRIPA may only require the retention of relevant communications data. Relevant communications data is defined in DRIPA and is limited to data falling within that definition that is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying a telecommunications service[2].

1.5. The categories of data that can be retained under DRIPA are set out in the Schedule to the DRR 2014 and are the same as those that could be retained under the now revoked Data Retention (EC Directive) Regulations 2009.

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[3], or to one of the Commissioners responsible for overseeing the powers conferred by the DRIPA, the DRR 2014 or RIPA, it must be taken into account.

1.7. Under regulation 9 of the DRR 2014 the Information Commissioner must audit compliance with requirements or restrictions imposed in relation to the security, integrity and destruction of the communications data retained under DRIPA.

1.8. This code is confined to procedures relating to the retention of communications data. The codes of practice on the acquisition and disclosure of communications data and on the interception of communications issued pursuant to section 71 of RIPA provide guidance on procedures to be followed in relation to the acquisition of communications data and the interception of communications.

---

1 See paragraph 2.2

2 See paragraphs 2.10 to 2.15

3 See paragraph 9.5

1.9. The Home Office does not publish or release identities of CSPs subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of CSPs under a notice.

1.10. This code extends to the United Kingdom[4].

1.11. The Home Office may issue further advice directly to CSPs as necessary.

[4] This code and the provisions of DRIPA do not extend to the Crown Dependencies and British Overseas Territories

2. General extent of powers

Necessity and proportionality

2.1. Section 1(1) of DRIPA gives the Secretary of State the power to issue a data retention notice to a CSP, requiring them to retain relevant communications data, if she considers it necessary and proportionate for data to be retained for one or more of the purposes in section 22(2) of RIPA[5]. These are:

- in the interests of national security;
- for the purpose of preventing or detecting crime[6] 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;
- in the interests of public safety;
- for the purpose of protecting public health;
- 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;
- to assist investigations into alleged miscarriages of justice;[7]
- 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),[8] and
- 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 his death or condition.[9]

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

6 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.

7 See article 2 (a), SI 2010/1480

8 See article 2 (b) (i), SI 2010/1480

9 See article 2 (b) (ii) SI 2010/1480

Scope and Definitions

Communications service provider

2.2. Throughout this code, an operator who controls or provides a public telecommunication system or provides a public telecommunications service is described as a communications service provider ('CSP'). The meanings of telecommunications service and telecommunication system are defined in RIPA[10].

2.3. Where a company uses the physical network (this includes the network bandwidth and phone lines) belonging to another in order to provide their services to the public, a retention notice can be imposed on whichever company holds the relevant communications data (which will depend on how they design and operate their systems).

2.4. Where two companies hold similar or identical data the Home Office will agree an approach with the providers concerned to ensure that the relevant data is not retained more than once.

2.5. Section 2(8A) of RIPA, as inserted by DRIPA, clarifies the definition of telecommunications service to make clear that it includes companies who provide internet-based services, such as webmail.

Communications data

2.6. Communications data is defined in section 21(4) of RIPA. It can be used to demonstrate who was communicating; when; from where; how; and with whom. It does not include the content of any communication: for example the text of an email or a conversation on a telephone. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It can include 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. Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services.

2.7. The definition of communications data in RIPA is divided into three different types of data:

- Traffic data (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;
- Service Use information (section 21(4)(b) of RIPA) – this is the data relating to the use made by a person of a communications service; and

[10] Sections 2(1) and 81(1) of the RIPA define '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 'telecommunication 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.

- Subscriber information (section 21(4)(c) of RIPA) – this relates to information held or obtained by a CSP about persons[11] to whom the CSP provides or has provided 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.

2.8. The definition of communications data in section 2(1) of DRIPA excludes communications data in relation to the provision of a postal service.

2.9. More detailed descriptions of these definitions and examples of the type of data that they may cover are included in the Acquisition and Disclosure of Communications Data Code of Practice.

Relevant communications data

2.10. A retention notice can be given to a CSP to require the retention of relevant communications data.

2.11. Relevant communications data is defined in section 2(1) of DRIPA. It is limited to data of the kind mentioned in the Schedule to the DRR 2014 (which is identical to the Schedule to the now revoked Data Retention (EC Directive) Regulations 2009), that is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying a telecommunications service. A notice may not be issued to a company that does not generate or process data within the UK.

2.12. This definition covers data relating to the use of fixed network telephony, mobile telephony, and internet access, internet e-Mail or internet telephony. The Home Office can provide further guidance to a CSP on whether a category of data falls within this definition.

2.13. Section 2(2) of DRIPA provides that the definition of relevant communications data includes 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 or where there has been a network management intervention. 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. Messages should be treated as successful communications unless logged as otherwise by the CSP's business systems.

2.14. This provision covers all types of electronics communications, as opposed to simply relating to voice telephony.

2.15. DRIPA provides explicitly that relevant communications data does not include the content of a communication.

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

Internet email

2.16. Internet email under DRIPA is considered to be any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service.

Applicability to the ATCSA

2.17. CSPs may also retain data under the voluntary code of practice under the ATCSA. Part 3 of the DRR 2014 applies to data retained in accordance with the voluntary code. It applies equivalent measures to those in the sections of DRIPA and the DRR 2014[12] relating to data security and access to retained data. Accordingly, chapters 6, 7 and 8 of this code apply equally to data retained under the ATCSA code. This ensures that all data which CSPs retain for longer than existing business purposes, whether on the basis of ATCSA or a data retention notice under DRIPA, is subject to the same controls and safeguards.

2.18. In practice CSPs who retain data voluntarily under the ATCSA code will often do so in conjunction with data retained under DRIPA, in systems which are subject to the security and safeguards contained with the DRIPA regime.

[12] Section 1(6) of DRIPA and regulations 7, 8, 9 and 12 of the DRR 2014.

3. Giving of data retention notices

Process for giving a data retention notice

3.1. The Home Office and key operational agencies (including law enforcement agencies and security and intelligence agencies) maintain governance arrangements in order to identify operational requirements, including the potential requirement to issue a data retention notice.

3.2. Once a potential requirement is identified, the Home Office will consult the relevant CSP(s) and, if appropriate, the Secretary of State will consider giving a notice.

Criteria for issuing a data retention notice

3.3. When considering whether to issue a notice a number of factors are taken into account. These include, but are not limited, to:

- The size of a CSP – a CSP with a larger customer base is more likely to receive a data retention notice;
- The speed of growth of a CSP – small CSPs with rapid prospective growth may receive notices in anticipation of future law enforcement requirements;
- The number of requests a CSP receives annually for communications data – this, and the CSP's ability to meet the volume of requests they receive, will be a key determinant of whether there is benefit in serving a notice on a CSP (noting that the giving of a notice may increase the number of requests received by a CSP);
- Whether a CSP operates a niche service – a CSP which is the sole or key provider of a type of service may receive a notice regardless of the size of the company; or
- Whether a CSP operates in a specific geographical area – a CSP which is a key provider of services in a limited geographical area is more likely to receive a notice.

3.4. Ultimately, however, a notice can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and proportionate to do so.

3.5. The timescale for such processes will depend on operational need but will always follow the same steps to ensure that the Secretary of State is making an informed decision, based on the relevant information.

Criteria for giving a notice to categories of providers

3.6. There may be circumstances where there are a number of CSPs providing similar services in a specific limited area. An example of this could be Wi-Fi providers in a particular location.

3.7. It is possible that the Secretary of State could place the same obligations on all such CSPs through one notice, but only if it was considered necessary and proportionate to do so.

3.8. While this may be appropriate for a relatively small number of providers providing the same or a similar service, this provision cannot be used to place blanket requirements across a large number of companies operating a service or companies providing a range of different services, not least because the requirements in a notice need to reflect the particular nature of each business.

Consultation with service providers

3.9. Before giving a notice to a company the Secretary of State must take reasonable steps to consult any CSP(s) which will be covered by the notice.

3.10. In practice, consultation is likely to take place long before giving a notice to a company. The Home Office will engage with companies who may possibly be subject to a notice in the future to provide advice and guidance and prepare them for the possibility of receiving a notice should it be considered necessary and proportionate to do so.

3.11. Should the giving of a notice to a CSP be deemed appropriate, the Home Office will take steps to consult the company formally before giving a notice, in order to ensure that it accurately reflects the services and data types processed by that CSP.

3.12. Should a CSP have concerns about whether the requirements of a notice are appropriate or technically feasible, these should be raised during this consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

3.13. Should it be considered appropriate to place the same obligations on a number of companies through one notice, the Home Office will take steps to consult all CSPs who would or could be affected by the notice. However, it is recognised that there may be cases where this will not be possible, for example where a new CSP enters the market after a notice is served and therefore will not have been formally consulted.

Matters to be considered by the Secretary of State

3.14. Following the conclusion of consultation with CSPs, the Secretary of State will consider whether to give a data retention notice. This consideration should include all the aspects of the proposed data retention notice. It is an essential means of ensuring that the data retention notice is justified and that proper processes have been followed.

3.15. As part of the decision the Secretary of State must take into account a number of factors:

- The likely benefits of the notice – the extent to which the data to be retained may be of use to public authorities. This may take into account projected as well as existing benefits.
- The likely number of users of the services to be covered by the notice – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the data being retained.
- The technical feasibility of complying with the notice – taking into account any representations made by the CSP(s).
- The likely cost of complying with the notice – this will include the costs of both the retention, and any other requirements and restrictions placed on CSPs, such as ensuring the security of the retained data. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.[13]
- Any other impact of the notice on the CSP – again taking into account any representations made by the CSP(s).

3.16. The Secretary of State will also consider the contents of the proposed notice, including the data to be retained and the period or periods for which that data is to be retained up to a maximum of 12 months from the giving of the notice.[14]

3.17. In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision.

3.18. If the Secretary of State agrees with the recommendation to give a notice, they will then sign the notice.

Once a notice has been agreed

3.19. Once a notice has been signed by the Secretary of State, arrangements will be made for this to be given to a CSP. During consultation with the CSP, it will be agreed who in the company should receive the notice and how it should be issued (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be issued to a senior executive within the company.

3.20. A data retention notice comes into force from the point it is given to the CSP, unless otherwise specified in the notice.

3.21. It will often be the case that dedicated systems will be constructed within a CSP for the retention of communications data, and the time taken to design and construct such a system will be taken into account. Accordingly, different elements of the notice may take effect at different times.

---

[13] See paragraph 5.8

[14] See paragraphs 3.26 to 3.28

3.22. Once a notice has been given to a CSP, a copy of the notice and any other relevant information will be sent to the Information Commissioner, who is responsible for the oversight of the security, integrity and destruction of retained data (see chapter 5 for further details).

The content of a data retention notice

3.23. A notice will set out:

- The CSP(s) to which it relates – where a company owns a number of subsidiary companies that operate under different trading names, the notice might additionally list these details for the sake of clarity;
- Which services data is to be retained for – it may not be necessary and proportionate to retain data in relation to all communication services provided by a company;
- The data to be retained and the period for which it is retained – these will relate to the list of data types in the Schedule to the DRR 2014 and will make clear whether certain categories of data should be retained for less than 12 months; and
- Any additional requirements or restrictions in relation to the retention of the data – this may include requirements in relation to the security of retained data.

3.24. A template notice is included at annex A.

3.25. A notice will not necessarily represent the full range of services and data types which a CSP could retain. This does not mean that additional data types or services could not be included in a future version of the notice, should a pressing operational requirement arise, provided that it would be necessary and proportionate to do so (see chapter 4 for further details).

Retention period

3.26. Data retained under DRIPA may be retained for a maximum period of 12 months. A notice will only require data to be retained for as long as is considered necessary and proportionate, up to that maximum period. If, once a data retention notice is given, further evidence demonstrates that a retention period specified in the notice is no longer appropriate, the Secretary of State will set a different retention period, up to a maximum of 12 months, ensuring the period reflects what is necessary and proportionate.

3.27. A data retention notice covers relevant data already in existence at the point at which a notice is given. The starting point for the retention period for such data is determined by the date of the communication (in relation to traffic and service usage data) and the date at which the customer leaves the company or the data is changed (for subscriber data)[15].

[15] Regulation 4(2)

3.28. A data retention notice may require the retention, for up to 12 months, of data which a CSP already holds for 12 months or longer for business purposes. This ensures that the data will not be deleted before the end of the required retention period – for example in response to a change in the business retention period.

4. Review, variation and revocation of notices

Review

4.1. The Secretary of State must keep notices under review. This helps to ensure that a notice itself, or the retention of categories of data specified in a notice, remains necessary and proportionate.

4.2. It is recognised that, after being served with a notice, a CSP is likely to require time to put the necessary capabilities in place to meet their obligations. As such, the first review should not take place until after these capabilities have been put in place. Without these capabilities being fully operational, it will not generally be possible to assess the benefits of a notice.

4.3. Reviews will take place at least once every two years once capabilities are in place. However, the exact timing of the review is at the Secretary of State's discretion.

4.4. A review may be initiated earlier than scheduled for a number of reasons. These include:

- a significant change in demands by law enforcement agencies that calls into question the necessity and proportionality of the notice as a whole, or a subset of data being retained under a notice;
- a significant change in CSP activities or services; or
- a significant refresh or update of CSP systems.

4.5. The process for reviewing a notice is similar to the process for giving a notice, with the Home Office consulting operational agencies, CSPs and the Information Commissioner as part of the review.

4.6. The review will also take into account the number of law enforcement requests made and the age of the data obtained. An absence – or low volume – of law enforcement requests will not necessary mean that it is no longer necessary and proportionate to maintain a data retention notice.

4.7. Once this process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate.

4.8. A review may recommend the continuation, variation or revocation of a notice. Details of the variation of and revocation of data retention notices follow below.

4.9. The relevant CSP, the operational agencies and the Information Commissioner will be notified of the outcome of the review.

Variation

4.10. The communications market is constantly evolving and CSPs subject to data retention notices will often launch new services or generate new data that law enforcement may require.

4.11. CSPs subject to a data retention notice must notify the Home Office of new products and services in advance of their launch, in order to allow consideration of whether it is necessary and proportionate to require data generated or processed in the course of providing those services to be retained.

4.12. Small changes, such as upgrades of systems or changes to data which are already covered by the existing notice, can be agreed between the Home Office and CSP in question. However, significant changes will require a variation of the data retention notice.

4.13. Regulation 11 of the DRR 2014 provides that data retention notices under section 1(1) of DRIPA can be varied by the Secretary of State. There are a number of reasons why a notice might be varied. These include:

- a CSP launching new services or generating new categories of communications data which may be of interest to law enforcement;
- changing law enforcement demands and priorities;
- a recommendation following a review under regulation 6 of the DRR 2014 (see section above); or
- to amend or enhance the security requirements – for example following a review of security by the ICO.

4.14. Where a company has changed names, for example as part of a rebranding exercise or due to a change of ownership, the Home Office and the company will need to consider whether the existing notice is sufficient.

4.15. The process for varying a notice is similar to the process for giving a notice. The Home Office will consult operational agencies, to understand the operational impact of any change to the notice, and CSPs to understand the impact on them, including any technical implications. Once this consultation is complete, the Secretary of State will consider whether to vary the notice.

4.16. Further detail on the process for consultation with CSPs and consideration by the Secretary of State can be found in Chapter 3.

4.17. Once a variation has been agreed by the Secretary of State, arrangements will be made for this to be given to a CSP. As with a data retention notice, a variation of a notice comes into force from the point it is given unless otherwise specified in the notice and different elements of the variation may take effect at different times.

4.18. Once a variation has been given to a CSP a copy will be sent to the Information Commissioner.

4.19. A data retention notice may be varied to reduce, or extend, the period for which data can be retained. No retention notice, or such variation, can result in data being retained for longer than 12 months.

Revocation

4.20. A data retention notice must be revoked (in whole or in part) if it is no longer necessary to require a CSP to retain communications data, or certain types of communications data.

4.21. Circumstances where it may be appropriate to revoke a notice include where a CSP no longer operates or provides the services to which the notice relates, where operational requirements no longer include the data covered by the notice, or where such requirements would no longer be necessary or proportionate.

4.22. The revocation of a data retention notice does not prevent the Secretary of State issuing a new data retention notice, covering the same, or different, data and services, to the same CSP in the future should it be considered necessary and proportionate to do so (regulation 11(10)).

4.23. Once notice of revocation has been given to a CSP a copy will be sent to the Information Commissioner

5. Making of contributions towards the costs incurred by communications service providers

5.1. The DRR 2014[16] recognise that CSPs incur expenses in complying with notices to retain communications data, and allow for appropriate payments to be made to them to cover these costs.

5.2. CSPs are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a data retention notice and the DRR 2014.

5.3. Any contribution towards these costs must be agreed by the Home Office before work is commenced by a CSP[17] and will be subject to the Home Office considering, and agreeing, the solution proposed by the CSP.

5.4. These costs may include the procurement or design of systems required to retain communications data, their testing, implementation, continued operation and where appropriate sanitisation and decommissioning. Some overheads may be covered if they directly relate to costs incurred by CSPs in complying with their obligations outlined above.

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

5.6. Contributions may also be appropriate towards the costs incurred by a CSP to update its systems to maintain, or make more efficient, its retention 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 retention of communications data relating to the use of such services.

5.7. 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.

5.8. As costs are reimbursed from public funds, CSPs should take into account value for money when procuring, operating and maintaining the infrastructure required to comply with a notice. As changes to business systems may necessitate changes to data retention and disclosure systems, CSPs should take this into account when making any changes to business systems.

[16] Regulation 13

[17] Regulation 13(2)

5.9. Any CSP that has claimed contributions towards costs may be required to undergo a Home Office audit to ensure that a CSP has incurred expenditure for the stated purpose before those contributions are made. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

6. Security of retained data

6.1. All data retained under DRIPA is subject to a range of safeguards, in order to ensure effective protection of the data against the risk of abuse and any unlawful access to and use of that data. Regulation 7 of the DRR 2014 requires CSPs under a notice to take steps to ensure that the data is adequately protected while it is being retained. These requirements relate to three broad areas – data security, data integrity and deletion of data.

6.2. Further detail on the security arrangements to be put in place by CSPs may be included in the data retention notices served on a CSP which, in accordance with regulation 4(1)(d), must specify any other requirements or restriction in relation to the retention of data.

6.3. In most cases data retained under a notice is stored in dedicated data retention and disclosure systems, which are securely separated by technical security measures (e.g. a firewall) from a CSP's business systems. Where data is retained by CSPs for business purposes for some, but not all, of the period specified in the notice, the data retention and disclosure system may hold a duplicate of that business data so that it can be accessed without undue delay[18].

6.4. However, in some cases it will not be practical to create a duplicate of that data and CSPs will retain information in business or shared systems.

6.5. The scope of the security controls defined within this section apply to all dedicated IT systems that are used to retain or disclose communications data, and any other dedicated systems which are used to access, support or manage dedicated retention and disclosure systems. It also applies to all CSP (or 3rd party) operational and support staff who have access to such systems. Additional security considerations relating solely to systems for the disclosure of communications data can be found in the Acquisition and Disclosure of Communications Data Code of Practice.

6.6. Where data is retained in business or shared systems, or where business systems are used to access, support or manage retention and disclosure systems, these will be subject to specific security controls and safeguards, similar to those defined within this section, where appropriate and as agreed with the Home Office.

Data security

6.7. The specific data security measures will depend on a number of factors including, but not limited to, the volume of data being retained, the number of customers whose data is being retained and the nature of the retained data.

6.8. When setting security standards consideration also has to be given to the threat to the data.

[18] In accordance with regulation 8(2)

6.9. The security put in place at a CSP will comprise four key areas:

- Physical security e.g. buildings, server cages, CCTV;
- Technical security e.g. firewalls and anti-virus software;
- Personnel security e.g. staff security clearances and training; and
- Procedural security e.g. processes and controls.

6.10. As each of these broad areas is complementary, the balance between these may vary e.g. a CSP with slightly lower personnel security is likely to have stricter technical and procedural controls. The specific security arrangements in place will be agreed in confidence between the Home Office and relevant CSPs and shared with the Information Commissioner for his functions under this code.

6.11. As the level of data security is based on a number of factors and is a balance of four broad areas, there is no single minimum security standard. However, all CSPs retaining data will be required to follow the key principles of data security set out below.

6.12. The Home Office will provide security advice and guidance to all CSPs who are retaining data and this will be provided to the Information Commissioner for the conduct of his functions under this code.

Data integrity

6.13. Data integrity, as required by regulation 7(1)(a), relates to a need to ensure that no inaccuracies are introduced to data when it is retained under DRIPA[19].

6.14. When relevant communications data is retained under DRIPA, it should be a faithful reproduction of the relevant business data and it should remain a faithful reproduction throughout any further processing that may occur during the period of its retention. A record of the business purpose for which the data is generated may be retained to assist law enforcement to understand the underlying quality/completeness of the business data which has then been retained. For example, data generated to assist a CSP in understanding network loading may be less accurate than data used to bill customers.

6.15. There should be no errors introduced in retaining the data, for example in the process of copying the data to a retained data store or in searching and disclosing data, that lead to discrepancies between the business and retention sets of data.

6.16. Once the data has been retained, technical security controls shall be implemented to mitigate modification of the data, and to audit any attempt to modify the data, until such time that it is deleted in accordance with the DRR 2014.

[19] This includes at the point at which it is placed into a data retention and disclosure system and during the period of its retention.

6.17. The audit capability of the data retention system shall be used to provide assurance that no unauthorised changes have been made to the retained data.

Principles of data security, integrity and deletion

Legal and regulatory compliance

6.18. All data retention systems and practices must be compliant with relevant legislation. As well as DRIPA and the DRR 2014, this includes, but is not limited to, the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003, which set out key controls in relation to the storage, use and transfer of personal data.

6.19. All systems and practices must also comply with any security policies and standards in place in relation to the retention of communications data. This may include any policies and standards issued by the Home Office, and any instruction or recommendation made by the Information Commissioner such as his published guidance on security. These further requirements are unlikely to be publicly available as they may contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information security policy & risk management

6.20. Each CSP must develop a security policy document. The policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities and policies relating to the integrity and deletion of data. Each CSP must also develop security operating procedures, including clear desk and screen policies for all systems. A CSP can determine whether this forms part of or is additional to wider company policies.

6.21. The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate to the nature of the business, the data retained and the threats to data security.

6.22. Each CSP must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources Security

6.23. CSPs must clearly identify roles and responsibilities of staff, ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when staff move roles within the organisation.

6.24. Staff with access to the data retention or disclosure systems should be subject to an appropriate level of security screening. The Home Office sponsors and manages security clearance for certain staff working within CSPs. CSPs must ensure that these staff have undergone relevant security training and have access to security awareness information.

Maintenance of Physical Security

6.25. Data retention and disclosure systems should be sited in locations that have appropriate security controls in place. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

6.26. Equipment used to retain data must be sanitised and securely disposed of at the end of its life (see the section on deletion of data for further details).

Operations management

6.27. Data retention and disclosure systems should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of retained data.

6.28. CSPs must also put in place a patching policy to ensure that regular patches and updates are applied to any data retention and disclosure system. Such patches and updates will include anti-virus, operating systems, application and firmware. The patching policy, including the timescale in which patches must be applied, must be agreed with the Home Office.

6.29. CSPs should ensure that, where encryption is in place in data retention and disclosure systems, any encryption keys are subject to appropriate controls, in accordance with the security policy.

6.30. In order to maintain the integrity of internal data processing CSPs must ensure that input data is validated against agreed input criteria.

6.31. Network infrastructure, services and system documentation must be secured and managed and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

6.32. CSPs should also ensure that removable and storage media (including the hard drives used to store retained data) are managed in accordance with the security policy, especially when in transit.

6.33. The data retention and disclosure system, and its use, should be monitored and all audit logs compiled, secured and reviewed by the CSP security manager at appropriate intervals. These should be made available for inspection by the Home Office as required.

6.34. CSPs should ensure that systems are resilient to failure and data loss by creating regular back ups of the data.

6.35. Technical vulnerabilities must be identified and assessed through an independent IT Health Check (ITHC) which must be conducted annually. The scope of the Health Check must be agreed with the Home Office.

Access Controls

6.36. CSPs must ensure that registration and access rights, passwords and privileges for access to dedicated data retention and disclosure systems are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

6.37. Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e. offsite access to CSP systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly any remote access for diagnostic, configuration and support purposes must be controlled.

Management of incidents

6.38. CSPs must put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management and the Home Office. Any breaches under relevant legislation, such as RIPA or the Privacy and Electronic Communications Regulations, should be notified in accordance with those provisions.

6.39. Measures should be implemented to prevent unauthorised disclosure or processing of data. Any suspected or actual unauthorised disclosure or processing of data or information must be reported as set out above.

6.40. System managers must ensure that data retention and disclosure systems enable the collection of evidence (e.g. audit records) to support investigation into any breach of security.

Additional requirements relating to the deletion of data

6.41. Regulation 7 makes clear that retained data must be deleted such that it is impossible to access at the end of the period for which it is required to be retained, unless its retention is otherwise authorised by law. A system must be set up such that it is verifiable that data is deleted and inaccessible at the end of the retention period. Deletions must take place at intervals no greater than monthly.

6.42. Where the physical, personnel and procedural security measures are assessed by the Home Office, or Information Commissioner, to be sufficient to prevent unauthorised physical access to the data retention and disclosure system, then data should be deleted in such a way that protects against data recovery using non-invasive attacks (i.e. attempts to retrieve data without additional assistance from physical equipment).

6.43. Where the implemented security measures are assessed by the Home Office, or Information Commissioner, to be insufficient to protect the data retention and disclosure system against physical access by unauthorised personnel, then additional requirements for the secure deletion of retained data should be agreed with the Home Office and Information Commissioner on a case-by-case basis.

Additional requirements relating to the disposal of systems

6.44. The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

6.45. If the equipment is to be re-used it must be securely sanitised by means of overwriting using a Home Office approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

6.46. If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Home Office approved supplier.

6.47. Sanitisation / destruction of data must include retained data copied for back-up and recovery, and anything else that stores duplicate data within the CSP system, unless retention of the data is otherwise authorised by law.

7. Oversight by the Information Commissioner

7.1. The DRR 2014 require that the Information Commissioner provides independent oversight of the integrity, security or destruction of data retained by virtue of DRIPA.

7.2. This code does not cover the exercise of the Information Commissioner's functions. It is the duty of any CSP subject to a notice under DRIPA to comply with any requests made by the Commissioner, in order to provide any information he requires to discharge his functions.

Records to be kept by a communications service provider

7.3. To assist the Information Commissioner carry out his statutory function in relation to DRIPA and the DRR 2014, CSPs must maintain a record of information that indicates whether and how they have complied with the provisions of this code. Such information must be provided to him on request.

7.4. Such records may include but are not limited to:

- Data Retention & Disclosure system access audit records;
- IT Health Check security reports;
- Security incident logs;
- Data Retention volumes;
- Details of retained financial records (i.e. PCI-DSS implications and required exemptions);
- Data Deletion Records;
- Hardware (storage media) destruction records; and
- Documentary evidence to demonstrate how the CSP has fulfilled its responsibilities under chapter 6.

7.5. Guidance on the maintenance of records by CSPs to assist with the Commissioner's statutory functions in relation to the DRR 2014 may be issued by or sought from him.

Reports by the Information Commissioner

7.6. Reports made by the Information Commissioner concerning the inspection of CSPs and the security, integrity and deletion of communications data retained under DRIPA or the ATCSA code of practice must be made available by the Information Commissioner to the Home Office. This can help to promulgate good practice and identify security enhancements and training requirements within CSPs. The Home Office will work with CSPs to address any recommendations made by the Information Commissioner.

7.7. Subject to discussion between the Information Commissioner and the Home Office, either may publish the inspection reports, in full or in summary, or a single overarching report to demonstrate both the oversight of the security of data and CSP's compliance with DRIPA and the DRR 2014. Because of the sensitivity of identifying which companies have received retention notices, any such report must be sufficiently redacted to protect the identities of the companies.

Enforcement of integrity, destruction and security standards

7.8. The DRR 2014 impose a duty on CSPs to comply with requirements or restrictions imposed by a retention notice, section 1(6) of DRIPA, or regulations 7 or 8 of the DRR 2014. That duty is enforceable by civil proceedings brought by the Secretary of State.

7.9. In the event of a failure to comply with the integrity, destruction and security requirements contained in the DRR 2014 or in a retention notice, the Secretary of State will consider whether enforcement action is appropriate or whether to work with CSPs to address any issues identified in the first instance.

7.10. Additionally, should the Information Commissioner establish instances of failure to comply with the Data Protection Act 1998 or other relevant data protection legislation, he may take enforcement action using powers under that legislation.

7.11. Should the Information Commissioner identify any errors or issues relating to the disclosure of communications data he may take such steps as he considers necessary to bring them to the attention of the CSP. Chapter 6 of the Acquisition and Disclosure of Communications Data Code of Practice sets out the requirements on CSPs in relation to any such errors.

8. Disclosure and use of data

Disclosure of data

8.1. As per section 1(6) of DRIPA, data that is retained subject to a data retention notice should not be disclosed except in accordance with (i) a request under Chapter 2 of Part 1 of RIPA; or (ii) a court order or other judicial authorisation or warrant[20]. Regulation 8 of the DRR 2014 requires CSPs to put in place adequate security systems (including technical and organisational measures) to protect against any other type of disclosure. This provision will ensure that retained data is only disclosed subject to appropriate safeguards, which ensure that a request is both necessary and proportionate.

8.2. Where appropriate information gathering powers exist under other pieces of legislation, these may still be used to access data that is retained by CSPs for business purposes, even if it would also be retained under a notice. They may not, however, permit access to data retained solely under notice.

8.3. The power to request personal data held by a company via a Subject Access Request under the Data Protection Act 1998 is not affected by DRIPA[21]. A disclosure in response to such a request may include data retained subject to a data retention notice or information held about the acquisition of that data by public authorities[22].

8.4. The DRR 2014 also require CSPs to retain data in such a way that it can be transmitted without undue delay in response to a request (regulation 8(2)). The Home Office will work with CSPs to ensure that the necessary secure auditable systems are in place to enable this disclosure.

8.5. Where a CSP holds data in business systems, but access to a duplicate version of that data may be facilitated more efficiently via a retention and disclosure system created in compliance with a DRIPA notice, this may be permitted subject to the agreement of the Home Office. For example, if an emergency service requests data in relation to a 999 call, it may be disclosed directly from the DRIPA retention store (where access may be facilitated via a secure, auditable disclosure system, rather than relying on manual access to business systems). The agreement of the Home Office may relate either to individual requests or categories of request.

---

20 Section 1(6)(b) of DRIPA also permits the Secretary of State to add further mechanisms for access to this data via regulations, subject to the affirmative resolution procedure in Parliament. The Data Retention Regulations 2014 contain no additional provisions of this type.

21 Section 27(5) of the Data Protection Act 1998 states that 'the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.'

22 There may be other bars to disclosure in the DPA and other legislation, for example regarding impeding an investigation.

Use of data by communications service providers

8.6. If data is held subject to a notice and would not otherwise be held by the CSP for business purposes, it should be adequately safeguarded to ensure that it can only be accessed subject to a lawful request. If data is not also being retained for existing business purposes it cannot be used by CSPs for business purposes, for example marketing, if such a requirement is subsequently identified.

8.7. In circumstances where a CSP identifies a specific purpose where access to retained data is in the interest of their customers, the company should discuss this issue with the Home Office on a case-by-case basis. This could include an investigation into fraudulent use of their services, where historical data retained under a notice might be crucial to that investigation. The agreement of the Home Office may relate either to individual requests or categories of request.

9. Contacts / complaints

General enquiries relating to communications data retention and acquisition

9.1. The Home Office is responsible for the giving and management of data retention notices. 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 CSPs in relation to their obligations under communications data legislation. Any CSP can contact the Knowledge Engagement Team at:

ketadmin@college.pnn.police.uk

Complaints

Data security

9.3. The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with these regulations. Failure to comply with this code's provisions in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
www.ico.org.uk

Acquisition of retained data

9.4. 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 the RIPA.

9.5. 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
SW1H 9ZQ
020 7035 3711
www.ipt-uk.com

Annex A – Template retention notice

DATA RETENTION AND INVESTIGATORY POWERS ACT 2014

DATA RETENTION REGULATIONS 2014

Data Retention Notice

Name: **[COMPANY NAME]**

1. In exercise of the powers conferred on her by section 1(1) of the Data Retention and Investigatory Powers Act 2014 ('the Act') the Secretary of State considers that it is necessary and proportionate, for one or more of the purposes mentioned in (or specified for the purposes of) paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000, to require [COMPANY NAME] to retain relevant communications data.

2. The duty of [COMPANY NAME] to retain communications data extends only to the communications data specified in Schedule 1 to this notice.

3. Data must be retained under this notice for the period specified in Schedule 1 to this notice.

4. Data retained under this notice is subject to the requirements and restrictions set out in the Data Retention Regulations 2014 and in Schedule 2 to this notice.

5. If [Company Name] is unable to comply with any part of this notice it should notify the Home Office immediately.

6. The obligations put in place by virtue of this notice take effect [when this notice is given to you or as otherwise agreed].

....

[Minister of State / [Parliamentary Under] Secretary of State] Date

SCHEDULE 1 – DATA TO BE RETAINED BY [COMPANY NAME] IN ACCORDANCE WITH THE REQUIREMENTS IMPOSED BY THIS DATA RETENTION NOTICE

A) Services to which data retention obligations apply (delete as appropriate)

- Fixed line telephony
- Mobile Telephony (including SMS, MMS and EMS)
- Mobile internet access
- Fixed line internet access
- Wireless (e.g. Wi-Fi) internet access
- Internet E-mail services
- Internet Telephony: Voice Over IP or other over the top voice services
- Other services where relevant

B) Categories of data to be retained (delete as appropriate)

PART 1 - FIXED NETWORK TELEPHONY

Data necessary to trace and identify the source of a communication

1.*—(1) The calling telephone number.*

(2) The name and address of the subscriber or registered user of any such telephone.

Data necessary to identify the destination of a communication

2.*—(1) The telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred.*

(2) The name and address of the subscriber or registered user of any such telephone.

Data necessary to identify the date, time and duration of a communication

3. *The date and time of the start and end of the call.*

Data necessary to identify the type of communication

4. *The telephone service used.*

PART 2 - MOBILE TELEPHONY

Data necessary to trace and identify the source of a communication

5.*—(1) The calling telephone number.*

(2) The name and address of the subscriber or registered user of any such telephone.

Data necessary to identify the destination of a communication

6.*—(1) The telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred.*

(2) The name and address of the subscriber or registered user of any such telephone.

Data necessary to identify the date, time and duration of a communication

7. *The date and time of the start and end of the call.*

Data necessary to identify the type of communication

8. *The telephone service used.*

Data necessary to identify users' communication equipment (or what purports to be their equipment)

9.*—(1) The International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made.*

(2) The IMSI and the IMEI of the telephone dialled.

(3) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

Data necessary to identify the location of mobile communication equipment

10.*—(1) The cell ID at the start of the communication.*

(2) Data identifying the geographic location of cells by reference to their cell ID.

PART 3 - INTERNET ACCESS, INTERNET E-MAIL OR INTERNET TELEPHONY

Data necessary to trace and identify the source of a communication

11.*—(1) The user ID allocated.*

(2) The user ID and telephone number allocated to the communication entering the public telephone network.

(3) The name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

Data necessary to identify the destination of a communication

12.*—(1) In the case of internet telephony, the user ID or telephone number of the intended recipient of the call.*

(2) In the case of internet e-mail or internet telephony, the name and address of the subscriber or registered user and the user ID of the intended recipient of the communication.

Data necessary to identify the date, time and duration of a communication

13.*—(1) In the case of internet access—*

(a) the date and time of the log-in to and log-off from the internet access service, based on a specified time zone,

(b) the IP address, whether dynamic or static, allocated by the internet access service provider to the communication, and

(c) the user ID of the subscriber or registered user of the internet access service.

(2) In the case of internet e-mail or internet telephony, the date and time of the log-in to and log-off from the internet e-mail or internet telephony service, based on a specified time zone.

Data necessary to identify the type of communication

14. *In the case of internet e-mail or internet telephony, the internet service used.*

Data necessary to identify users' communication equipment (or what purports to be their equipment)

15.*—(1) In the case of dial-up access, the calling telephone number.*

(2) In any other case, the digital subscriber line (DSL) or other end point of the originator of the communication.

The items of data to be retained under this notice will be agreed between the Home Office and [COMPANY NAME]. This may include other information including, but not limited to, internal customer reference numbers, that is necessary to enable [COMPANY NAME] to transmit the data in response to requests.

C) Period for which data is to be retained

Unless specified below data retained under this notice must be retained for a period of 12 months. The start point for the retention period, in accordance with regulation 4(2) of the Data Retention Regulations 2014, is:

(a) in the case of traffic data or service use data, the day of the communication concerned; and

(b) in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.

Data Retained for shorter periods:

[Specify any relevant data]

D) Groups of customers in relation to which data is to be retained

Unless specified below data retained under this notice must be retained for all customers of the relevant services specified above.

Groups of customers whose data is not subject to retention obligations:

[Specify any relevant groups of customers]

SCHEDULE 2 – REQUIREMENTS TO BE APPLIED TO DATA RETAINED BY [COMPANY NAME] IN ACCORDANCE WITH THIS DATA RETENTION NOTICE

A) Security, integrity and deletion of retained data

- A review of the risks to the data retained under this data retention notice must be carried out by [COMPANY NAME] in conjunction with the Home Office within 5 months from the date the notice is given.
- A plan to address those risks, in accordance with the principles contained in the code of practice and agreed by the Home Office, must be put in place within 7 months from the date the notice is given.

B) Oversight of retained data

- A record, which indicates whether and how the security requirements in relation to the data retained under this notice have been met, must be maintained in accordance with the requirements of the Information Commissioner.
- Such information must be provided to the Information Commissioner on request.

This code of practice relates to the powers and duties conferred or imposed under sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014, and the Data Retention Regulations 2014, relating to the retention of communications data by communications service providers. It provides guidance on the procedures to be followed for the retention of communications data and describes communications data. It sets out the security principles which must be adhered to by those retaining data and the oversight arrangements in place.

This code is aimed at communications service providers who currently, or may in future, retain data under Data Retention and Investigatory Powers Act 2014 or the voluntary code of practice under the Anti-Terrorism, Crime and Security Act 2001. This code is also relevant to members of public authorities who are involved in the acquisition of communications data.

Further details regarding the acquisition of communications data can be found in the Acquisition and Disclosure of Communications Data Code of Practice.