Extracts from GCHQ's Compliance Guide, in force from June 2014 onwards

Double underlined sections have been gisted for OPEN.

'Overview' section of the Compliance Guide

Relevant extracts from the 'Overview' section of the Compliance Guide in force from October 2014 until the present

Principles

GCHQ relies upon three core principles to demonstrate the legal compliance of our operational activities. The principles are that all operational activity must be:

- authorised (legal or policy authorisation)
- necessary for one of GCHQ's operational purposes: national security economic well-being of the UK or the prevention or detection of serious crime (further detail)
- proportionate (further detail)

The principles recur throughout this guidance, where their implications are explained in context.

We show that our actions are necessary and proportionate by producing an accountable record for oversight and audit. In many cases this takes the form of a HRA justification.

...

'Analysis' section of the Compliance Guide

Relevant extracts from the 'Analysis' section of the Compliance Guide as at June 2014 until the present

Principles

You can assume the data you analyse has been legally obtained, as long as policies on collection and targeting have been properly followed.

It is your responsibility to make relevant analysts aware of any significant changes that may affect the legality of the targeting of selectors, or mean that additional authorisation is required to examine the content of communications (for example, if you discover that a target has entered the UK).

The individuals whose communications you examine have a right to privacy, so your work must conform to the standards of HRA. Your queries and analysis must be necessary for an intelligence requirement and proportionate. You usually have to demonstrate this through a HRA justification that is logged for audit.

If you are examining the content of individuals' communications, the standard of your HRA justification must be higher than if you are examining events data. No additional authorisation is needed for querying and examining events data.

If your target is in the UK, you must have additional authorisation for examination of the content of their communications. If your target is otherwise sensitive on grounds of nationality or location, you need a COPA before you may examine the content of their communications.
Governmental and military communications do not attract human rights protections. If within these communications you come across the individuals' private communications, you must respect the human rights of those individuals.
It is GCHQ policy to apply the same legal and policy handling rules to all operational data, whether it is acquired by interception warrant or by any other means.

Analyst responsibility
You are intruding on an individual's right to privacy every time you search for their communications or communications about them in a database that contains raw traffic, or material derived from it. To conduct analysis in a way that is fully compliant with the law, every search that you carry out must be:

- authorised
- necessary for one of GCHQ's purposes:
  - national security (NS)
  - economic well-being (EWB) of the UK (provided it also meets the NS purpose)
  - prevention and detection of serious crime (SC)
- proportionate

To demonstrate the necessity and proportionality of your search, you must supply a HRA justification. This consists of three parts:

- JIC purpose eg 1NS
- *Requirement* number that equates to the intelligence requirement that your search seeks to meet
- free-flow explicit textual justification that explains why you are carrying out this search

If you own scheduled queries on content or events databases, it is your responsibility to ensure that the HRA justification and query terms are up to date. 'Querying and analysis of targets' communications content: analyst responsibility' provides more detail. The audit section provides guidance on standards of HRA compliance for queries on raw traffic and other databases.

...

'Audit' section of the Compliance Guide

Relevant extract from the 'Audit' section of the Compliance Guide as at June 2014 until the present

Details
All operational query-based systems that make Sigint data available to GCHQ users **[REDACTED]** require a HRA justification for each query and create logs of this information. The requirements for logging are stated in the Requirements for Systems. The log includes at least:

- JIC purpose and priority
- *Requirement* number
- textual HRA justification
- user's *identifier*, date and time.

These fields of a log or database entry will be checked by an audit. Depending on the nature of the database, auditors may check additional fields, such as query terms or the legal authorisation.

...

'Authorisation' section of the Compliance Guide

Relevant extracts of the 'Authorisations' section of the Compliance Guide from January 2015 until the present

...

Direction under s.94 of the Telecommunications Act

A Direction under s.94 of the Telecommunications Act may be issued by the Secretary of State and served upon a CSP. The Direction cannot direct the CSP to disclose communications content; it can, however, direct the CSP to disclose other information i.e. communications data in the interests of national security and where SoS judges it proportionate. GCHQ's *relevant team* makes use of these Directions.

Acquisition of data from partners

GCHQ receives operational data from various sources other than its own collection operations. Further information is in Collection and data acquisition and Partnerships.

Particular sensitivity attaches to any such data that includes details of non-targets as well as targets (i.e. is bulk in nature) and relates to identifiable individuals. You need to obtain a Bulk Personal Data Acquisition Request (BPDAR) before you receive any operational data meeting these criteria from a partner. By following this process you will help to ensure that GCHQ's acquisition of the data is demonstrably necessary and proportionate.

When the Investigatory Powers Bill was published on 4 November 2015, new open arrangements covering the handling of Bulk Personal Data (BPD) and section 94 data across the SIA were published at the same time.

Complementing these open handling arrangements (which are unclassified) are sets of closed handling arrangements (classified SECRET) for BPD and Section 94 for each of the Security and Intelligence agencies (SIA) which took effect on 27 November 2015.

The introduction of these handling arrangements reflects the intention of the SIA to make the acquisition and use of BPD and section 94 data more transparent and subject to clearly articulated safeguards. It also responds to recommendations made by the Intelligence & Security Committee in its Privacy and Security Report and by David Anderson QC in his review of investigatory powers. The closed handling arrangements for GCHQ largely reflect current practices and policy although there are some minor changes.

All staff involved in work that involves the acquisition of BPD and/or section 94 material, or the handling of such material, must follow these new handling arrangements.

If you have any questions you should contact the *relevant team* for guidance.

...

Relevant extracts from the 'Authorisations' section of the Compliance Guide as at June 2014 to January 2015.

...

Direction under s.94 of the Telecommunications Act

A Direction under s.94 of the Telecommunications Act may be issued by the Secretary of State and served upon a CSP. The Direction cannot direct the CSP to disclosure of

communications content; it can, however, direct the CSP to disclose other information i.e. communications data in the interests of national security and where the SoS judges it proportionate. GCHQ's *relevant team* makes use of these Directions.

...

'Collection and data acquisition' section of the Compliance Guide

Relevant extracts from the 'Collection and data acquisition' section of the Compliance Guide from January 2015 until the present

...

Other data acquisition

GCHQ receives operational data from various sources other than its own interception. The principal sources are:

- communications data acquired under Telecommunications Act s94 directions and through partnerships (see communications data for further details).
- collateral datasets received from other intelligence agencies, other government departments or commercial organisations. (Comment: these can be particularly sensitive if they include details on non-targets as well as targets. See Compliance - Authorisations for further details).

GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently. You must ensure that there is appropriate authorisation in place to acquire data from these sources, in order to comply with the law or (in cases where no legal authorisation is needed) to demonstrate that its acquisition is necessary and proportionate. Further information is in 'Authorisations'.

...

Relevant extract from the 'collection and data acquisition' section of the Compliance Guide as at June 2014 to January 2015

...

***Partner* collection and miscellaneous data acquisition**

GCHQ receives operational data from various sources other than its own interception. Three principal sources are:

- through GCHQ targeting[1] of *Sigint* partners
- communications data acquired under Telecommunications Act s94 directions and through partnerships
- collateral databases received from sister intelligence agencies.

GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently.

...

'Communications containing confidential information' section of the Compliance Guide

[1] In this context, 'Targeting' means 'tasking'.

Relevant extracts from the 'Communications containing confidential information' section of the Compliance Guide from March 2015 until the present

Principles

The RIPA Interception of Communications Code of Practice stipulates that particular consideration should be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. GCHQ must therefore take special care to ensure that the acquisition, analysis and retention of communications in these circumstances, and the dissemination of any intelligence produced from them, is necessary and proportionate.

The Human Rights Act and the European Convention on Human Rights also protect the rights to a fair trial, free press and freedom of religion.

This section of the Compliance Guide provides guidance on the handling and dissemination of certain categories of confidential information. You must follow the stipulations laid out below and in the linked policies.

For guidance on the deliberate targeting of sensitive professions, or where you intend to, or it is likely that you will, acquire confidential information, see the Targeting section of the Compliance Guide.

What is confidential?

Four categories of material require special handling:

1. Material that is legally privileged

Legal Professional Privilege (LPP) is broadly classified under two sub-headings:

- **legal advice privilege** which attaches to communications between a professional legal adviser, acting as such, and their client where the communication is made confidentially for the purpose of legal advice.
- **litigation privilege** which attaches to communications between the client and his legal adviser or agent, or between one of them and a third party, if they come into existence for the sole or dominant purpose of either giving or getting legal advice with regard to the litigation or collecting evidence in the litigation. This second category is wider than the first since it is possible for litigation privilege to attach to communications other than those directly between a lawyer and their client, i.e. between a lawyer and a third party in connection with legal proceedings.

2. Confidential personal information

Confidential personal information is information held in confidence concerning an individual (alive or dead) who can be identified from it and where the information relates to his physical or mental health or to spiritual counselling. This could include consultations between a health professional and a patient, or information from a person's medical records. Spiritual counselling is defined as conversations between an individual and a minister of religion acting in his official capacity, and where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3. Confidential journalistic information

This includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information

being acquired for the purposes of journalism and held subject to such an undertaking. Such undertakings may be implicit or explicit.
As a matter of policy, GCHQ also includes in this category any discussions around editorial policy and management of media organisations, as analysis and dissemination of such communications may also damage the freedom of the press.

4. Communications of and with UK legislators, namely:

- Members of the House of Commons (MPs)
- Members of the House of Lords
- Members of the Scottish Parliament (MSPs)
- Members of the Northern Ireland Legislative Assembly (MLAs)
- Members of the Welsh Assembly (AMs)
- Members of the European Parliament (MEPs) representing UK constituencies.

This category includes any and all communications in which a legislator is a participant whether or not he received it. It also extends to communications to or with legislators' offices/staff in view of the likelihood that they will handle legislators' communications or communicate on behalf of legislators. The confidentiality of these communications is essential to the interests of democracy in that it protects the independence of legislators and thus their ability to hold the Executive to account.
In cases of doubt, responsibility for deciding whether target communications and reportable information contain confidential information rests with the *relevant policy team*, who will consult the Legal Advisers as necessary.

Targeting of confidential communications
If you are likely to obtain confidential information as a result of your targeting activities, you must obtain a COPA in advance. In the case of legally privileged information, the COPA must be ratified by a senior FCO official before being signed off within GCHQ - contact the *relevant policy team* to assist with this. If a practising lawyer is the target, a COPA ratified by a senior FCO official is mandatory, whether or not you anticipate obtaining legally privileged information, and whether or not such information is of intelligence value. Full details are in the Authorisations section of the Compliance Guide.

Analysis of confidential communications
You should not transcribe, gist or otherwise analyse intercept containing confidential information unless you have reasonable grounds to believe it is necessary:

- on the grounds of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the UK, so far as those interests are also relevant to the interests of national security;
- for any of the other purposes mentioned in section 15(4) of RIPA.

Reporting/dissemination of intelligence from confidential communications
Other than in exceptional circumstances, material subject to legal privilege must not be acted on or further disseminated unless a Legal Adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.
Intelligence based on the interception of confidential information may only be disseminated in accordance with the GCHQ Intelligence Sharing and Release Policy on the sensitive professions and proportionality. Any intelligence that may potentially involve confidential

information must be submitted for mandatory 'Sensi' check. *Non-Sensi-Checkers* are not empowered to release such information themselves.

Relevant extracts from the 'Communications containing confidential information' section of the Compliance Guide as at June 2014 to March 2015

Compliance Guide - Communications Containing Confidential Information

Topics

- Principles
- What is confidential?
  - Material that is legally privileged
  - Confidential personal information
  - Confidential journalistic information
  - Communications of and with UK legislators
- Analysis of confidential communications
- Reporting/dissemination of intelligence from confidential communications

Principles

The RIPA Interception of Communications Code of Practice stipulates that particular consideration should be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. GCHQ must therefore take special care to ensure that the acquisition, analysis and retention of communications in these circumstances, and the dissemination of any intelligence produced from them, is necessary and proportionate.

The Human Rights Act and the European Convention on Human Rights also protect the rights to a fair trial, free press and freedom of religion.

This section of the Compliance Guide provides guidance on the handling and dissemination of certain categories of confidential information. You must follow the stipulations laid out below and in the linked policies.
For guidance on the deliberate targeting of sensitive professions, or where you intend to, or it is likely that you will, acquire confidential information, see the Targeting section of the Compliance Guide.

What is confidential?

Four categories of material require special handling:

Material that is legally privileged. This covers the provision of legal advice by any individual, agency or organisation qualified to do so. Legal Privilege does not apply to communications made with the intention of furthering a criminal purpose. However, the privilege does apply to the provision of professional legal advice to someone suspected of having committed a criminal offence, and is not necessarily lost when this legal advice is shared by the recipient.
Legal Privilege is fundamental to the right to a fair trial and the rule of law, as it allows an individual or entity to consult a lawyer in confidence without fear that what passes between them will be later used against them in court. The interception and reporting of legally privileged communications carries the inherent risk that it may influence the conduct of legal

proceedings and adversely affect the course of justice, particularly when the Crown is party to the legal proceedings.

Confidential personal information. Confidential personal information is information held in confidence concerning an individual (alive or dead) who can be identified from it and where the information relates to his physical or mental health or to spiritual counselling. This could include consultations between a health professional and a patient, or information from a person's medical records. Spiritual counselling is defined as conversations between an individual and a minister of religion acting in his official capacity, and where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

Confidential journalistic information. This includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. Such undertakings may be implicit or explicit.
As a matter of policy, GCHQ also includes in this category any discussions around editorial policy and management of media organisations, as analysis and dissemination of such communications may also damage the freedom of the press.

Communications of and with UK legislators, namely:

- Members of the House of Commons (MPs)
- Members of the House of Lords
- Members of the Scottish Parliament (MSPs)
- Members of the Northern Ireland Legislative Assembly (MLAs)
- Members of the Welsh Assembly (AMs)
- Members of the European Parliament (MEPs) representing UK constituencies.

This category includes any and all communications in which a legislator is a participant whether or not he received it. It also extends to communications to or with legislators' offices/staff in view of the likelihood that they will handle legislators' communications or communicate on behalf of legislators. The confidentiality of these communications is essential to the interests of democracy in that it protects the independence of legislators and thus their ability to hold the Executive to account.
In cases of doubt, responsibility for deciding whether target communications and reportable information contain confidential information rests with the *relevant policy team*, who will consult the Legal Advisers as necessary.

Analysis of confidential communications
You should not transcribe, gist or otherwise analyse intercept containing confidential information unless you have reasonable grounds to believe it is necessary on the grounds of national security, economic well-being of the UK or preventing or detecting a serious crime.

Reporting/dissemination of intelligence from confidential communications
Intelligence based on the interception of confidential information may only be disseminated in accordance with the GCHQ Intelligence Sharing and Release Policy on the sensitive professions and proportionality. Any intelligence that may potentially involve confidential information must be submitted for mandatory 'Sensi'-Check. Non-Sensi-Checkers are not empowered to release such information themselves.

'Communications data' section of the Compliance Guide

Relevant extracts from the 'Communications data' section of the Compliance Guide as at June 2014 until the present

...

Principles

Communications data comprises traffic data, service use data and subscriber data:

- Traffic data is data attached to a communication for the purposes of any telecommunications system used to transmit it,
- Service use data is any non-content information about the use made of a telecommunications service by a person, and
- Subscriber data is any other information held by a provider about a person to whom it provides a telecommunications service.

See the full RIPA definition.

The acquisition of communications data, whether through interception, a 'direction' (see below) or a partner organisation, will impinge on human rights and is therefore covered by authorisation regimes that comply with RIPA and the Telecommunications Act.

GCHQ handles all communications data in accordance with RIPA 15 safeguards, irrespective of its source.

Sources

GCHQ acquires communications data from a wide range of sources that split into four categories:

- most is collected as part of the interception process
- many forms of communications data are obtained through partnerships with *foreign partners*, OGDs and various commercial organisations such as communications and internet service providers (CSPs and ISPs)
- feeds requested from service providers
- ad hoc elements such as billing data or subscriber details for a communications address requested directly from service providers

Data received through the first three of these sources is generally fed into corporate events databases, where you can query it along with all other events data. A proportion of the ad hoc elements are made available in the same way, but this is not normal practice.

Authorisations

GCHQ's acquisition of communications data is authorised in four different ways depending on which of the above categories it fits into:

- collection of communications data as part of the interception process is authorised by our RIPA interception warrants
- communications data is received from multifarious partners on the basis of exchange, warranted feeds, gifts and other supplies, all subject to consideration of HRA
- feeds are requested from CSPs and ISPs under the authority of directions under s94 of the Telecommunications Act (as amended by the Communications Act). Directions are issued by the Secretary of State in the interests of national security. Although the directions are fairly general in nature, we agree and review annually with each relevant CSP/ISP exactly what types of communications data we wish to receive. Some directions are for regular feeds, others one-off requests

- requests for ad hoc elements of communications data from a CSP or ISP are authorised under RIPA Part I Chapter II. You must follow the procedure below, which ensures compliance with RIPA Part I Chapter II; in summary it involves putting forward a request and getting it authorised by a Designated Person (DP). The majority of requests for communications data are processed by means of the *relevant* database.

The rest of this section gives further guidance on this final class of request under RIPA Part I Chapter II, including guidance for DPs.

...

'Errors' section of the Compliance Guide

Relevant extracts from the 'Errors' section of the Compliance Guide as at June 2014 until the present

Principles

GCHQ policy is to abide by all UK laws that relate to GCHQ's operations, but errors with respect to legal compliance, and to applying the safeguards do sometimes occur. This section outlines GCHQ's process for handling errors and your role.

We need to be able to recognise and detect errors of legal compliance. We are obliged to investigate them and report to our oversight authorities.

If you have any concern over legal compliance or you identify an error that could breach GCHQ's legal requirements or safeguards you should inform *the relevant team* straight away. *The relevant team* will help and advise, if necessary coordinating GCHQ's response.

GCHQ is happy to stand by those who make errors where they are inadvertent or otherwise explicable. The Department will not tolerate errors of a deliberate nature that seek to avoid or undermine the processes and systems by which GCHQ operates.

What is an error?

From time to time in the course of operational activities, mistakes are made and errors occur.

There is no simple definition of whether an incident constitutes an error. Many comprise interference with one or more individuals' right to privacy and result from an accident or a failure to observe GCHQ procedures. *The relevant team* and the Legal Advisers determine exactly what constitutes an error.

Most compliance errors involve accidental collection of data without the necessary authorisation being in place. Other errors involve activity that, with hindsight, is judged unnecessary or disproportionate, even though an authorisation is in place.

For the purpose of the oversight arrangements applying to GCHQ, the term 'errors' includes breaches of the law in the sense of committing an offence (e.g. unlawful interception), as well as breaches of safeguards. Many apparent errors turn out not to be errors, but it is important that 'near-misses' are analysed thoroughly, not least so that lessons can be learned and actual errors in the future can be avoided.

Examples of GCHQ activity that would breach the law include:

- unlawful interception, as might occur when a RIPA 8(1) warrant is cancelled but targeting of a person in the UK is not removed
- unlawful interference with a computer system, as might occur if a CNE operation is conducted without the necessary ISA authorisation being in place.

Breaches of safeguards include:

- selection under a RIPA 8(4) warrant, other than permitted under the certificate

- carrying out CNE not covered by an internal approval.

Errors may also arise in relation to GCHQ's acquisition of communications data under RIPA Part I Chapter II. See Communications data for more detail.
GCHQ procedures and systems - as well as training and this Compliance Guide - are crafted to minimise the chance of legal errors.

Reporting potential errors
You should not hesitate to report to *the relevant team* any activity that appears to be erroneous or unauthorised. This includes any activity that does not appear to comply with GCHQ's systems and processes and may therefore have resulted in unauthorised, unjustified or disproportionate interference with privacy rights or property. You may wish to consult your line management or your local *policy lead*, but do not allow this to cause unnecessary delay.

Handling of errors
If you report a possible error, *the relevant team* will work with all relevant parties to investigate the circumstances and determine, in conjunction with the Legal Advisors, whether the incident constitutes an error.
If an error does occur, *the relevant team* will:

- advise whether it is necessary to stop a task, destroy material or cancel *intelligence reporting*
- coordinate any reporting to oversight authorities - i.e. the relevant Commissioner
- help develop recommendations for preventing a recurrence, e.g. changes to procedures, processes or training, and ensure they are implemented.

In a typical year GCHQ makes between 5 and 20 errors, of which only a small number may be deemed serious.

'Foreign partner' section of the Compliance Guide

Relevant extracts from the *'foreign partner'* section of the Compliance Guide as of June 2014 to present date
[REDACTED]

'Oversight' section of the Compliance Guide

Relevant extracts from the 'Oversight' section of the Compliance Guide as at June 2015 until the present.

...
Both Commissioners also have oversight of the intelligence Agencies' activities in respect of communications containing confidential information; this includes material that is legally privileged, confidential personal information (such as material related to the subject's physical or mental health or to spiritual counselling), confidential journalistic information, or the communications of and with UK legislators (the Wilson Doctrine). Warrants and reporting that relate to communications containing confidential information will explicitly be brought to the attention of the relevant Commissioner during the next inspection visit. Any material containing confidential communications that is retained should be made available to the relevant

Commissioner if requested, including detail of whether that material has been disseminated. For more on these communications and the associated handling arrangements see communications Containing Confidential Information.

...

'Partnerships' section of the Compliance Guide

Relevant extracts from the Partnerships' section of the Compliance Guide as of June 2014 until the present.

GCHQ shares data with a wide range of partner organisations. These embrace both Sigint partners and other organisations. **[REDACTED]**

Receiving data

GCHQ receives data from partner organisations under formal and informal agreements. In order to comply with HRA, the acquisition must be necessary and proportionate, and may require legal or policy authorisation. You should familiarise yourself with the guidance in Authorisations to check whether you require authorisation. However the data is acquired, it must be treated as if it were intercepted under RIPA. In particular, it should be handled in accordance with RIPA section 15 safeguards regarding access, review and retention. When the data contains personal information and its acquisition is not authorised by some other means, a Data Acquisition Authorisation must be obtained.

Sharing data

GCHQ can only share operational data, including the results of Sigint analysis, with other organisations where this is necessary for one of GCHQ's purposes and subject to legal safeguards and in accordance with our legal obligations.

Unless specifically authorised by the *relevant team*, *intelligence reporting* must be issued to account for all operational data shared with customers *and foreign partners*. This ensures that GCHQ meets its legal obligation to maintain an accountable record and enables safeguards to be applied **[REDACTED],** as well as the STRAP handling regime.

Intelligence reporting is not necessary when sharing with *foreign partner* Sigint agencies, although *intelligence reporting* will need to be issued should those agencies need to share the data with their customers and this *intelligence reporting* may need to be issued by GCHQ.

Intelligence reporting must be issued in accordance with *the relevant policies*.

...

'Review and retention' section of the Compliance Guide

Relevant extracts from the 'Review and retention' section of the Compliance Guide from October 2015 until the present

Principles
RIPA requires GCHQ to have arrangements to minimise retention of intercepted data and any material derived from it, as a "safeguard" to minimise intrusion into people's right to privacy.
Any retention must be necessary and proportionate for genuine operational purposes.
GCHQ treats all operational data as if it were obtained under RIPA.
GCHQ implements this safeguard by specifying default maximum retention periods for categories of data.
Retention of material beyond these default periods must be formally approved. Continued retention must be reviewed and rejustified, in most cases annually.

Default retention limits
This section of the Compliance Guide sets out GCHQ's arrangements for minimising retention to meet the requirements of the RIPA safeguards. We generally achieve this by setting default maximum retention periods for different categories of Operations data (see table below).
Data that does not fit comfortably within one of these categories should be discussed with *the relevant team*.
Note that, by agreement with *the relevant team*, retention periods for data in specific systems or applications may vary from these defaults.
[REDACTED]
...

Relevant extracts from the 'Review and retention' section of the Compliance Guide as of June 2014 to October 2015.

Principles
RIPA requires GCHQ to have arrangements to minimise retention of intercepted data and any material derived from it.
GCHQ implements this safeguard through policy by specifying maximum periods of retention for categories of Sigint and IA material; the policy also caters for exceptional needs.
Material kept beyond default periods must be reviewed and rejustified, in most cases annually.
GCHQ treats all operational data as if it were obtained under RIPA.
Very little data is kept for legal purposes alone.

Retention limits
This Compliance Guide and the Operations Data Retention Policy (DRP) set out GCHQ's arrangements for minimising retention in accordance with the RIPA safeguards. The DRP achieves this by setting default maximum limits for storage of Operations data.
[REDACTED]
...

'Safeguards' section of the Compliance Guide

Relevant extracts from the 'Safeguards' section of the Compliance Guide as at June 2014 to the present.

Principles

Safeguards are principles required by ISA and RIPA that must be applied to the handling of intelligence/intercepted material to ensure HRA requirements are met. ISA requires GCHQ to have arrangements in place to ensure that it obtains or discloses information only in the proper discharge of its functions or for the purpose of any criminal proceedings.

RIPA requires GCHQ to have arrangements in place to minimise its retention and dissemination of intercepted material. RIPA also applies specific protection to the communications of people in the UK. GCHQ applies RIPA safeguards to all operational data. Compliance with these safeguards is mandatory. GCHQ's policies and procedures, including those in this Compliance Guide, are built to implement these.

ISA safeguards

You must follow the policies of this Compliance Guide, especially those that are relevant to your work. By doing that, you will be playing your role in complying with the safeguard at ISA 4(2)(a): GCHQ obtains information only as is necessary for the proper discharge of its functions and discloses information either for that purpose or for the purpose of any criminal proceedings. In practice this requirement is met operationally by ensuring that everything we do is necessary in the interests of national security, the economic wellbeing of the UK, or in support of the prevention and detection of serious crime.

Key among the processes for achieving compliance are:

- **acquisition of information** from communications and other emissions, or any cooperative partner is controlled by procedures described in Authorisations; see also Collection and acquisition and Targeting
- **creation and keeping of records** must be justified as necessary for an ISA purpose and proportionate; see also Review and retention
- **reporting and other release of operational material** must be necessary and proportionate.

The mandatory *legalities* training programme reminds relevant staff of the safeguards and their duty to follow them.

If we fail to follow these safeguards properly a breach may occur - see Errors.

RIPA section 15 safeguards

Section 15 of RIPA imposes handling, dissemination and minimisation safeguards that require:

- the copying and disclosure of intercepted material to be minimised
- intercepted material to be destroyed as soon as its retention is no longer necessary for an authorised purpose
- access to material to be limited to people who need to see it.

These safeguards are implemented through a wide range of GCHQ operational, security and personnel policies, e.g. those at Review and retention.

RIPA section 16 safeguards

Section 16 of RIPA applies extra safeguards to the interception under external warrants of communications of individuals known to be in the UK. Firstly, material may only be examined if it falls within one of the categories of intercepted material set out in the certificate issued under s 8(4), i.e. material, the examination of which the Secretary of State considers necessary. In practice, the purpose of the HRA justification for the selector or query is to ensure that the analyst provides an accountable record that this requirement has been satisfied and that all targeting and searches conducted fall within one of the 8(4) categories. Secondly,

communications may not be selected for examination using a factor referable to an individual known to be in the UK, unless that selection has been specifically authorised under RIPA s16, usually by a Secretary of State. RIPA section 16 authorisations and processes are described in Authorisations and Targeting.

...

'Foreign partner' section of the Compliance Guide

Relevant extracts from the *'foreign partner'* section of the Compliance Guide as of June 2014 to present date
[REDACTED]

'Sharing' section of the Compliance Guide

Relevant extracts from the 'Sharing' section of the Compliance Guide as of June 2014 to present date[2]

Scope

This section outlines legal issues relevant to GCHQ's sharing of operational data. It provides cross-references to more detailed guidance on individual topics.

Principles
You may share operational data only if it is necessary for one of GCHQ's operational purposes. Your sharing must be kept to the minimum necessary and must be done in an approved, accountable way, in accordance with the guidance provided in this section. The legal basis for sharing is explained in Overview.

If you wish to share a new line of data with an external organisation, you must first consult *the relevant team*. The judgement on the necessity of sharing will be taken within a broad context of policies associated with GCHQ's partnerships.

Staff and contractors seconded to or working for GCHQ are covered by the same legal requirements as GCHQ personnel, in particular ISA, HRA and RIPA. If you handle operational data you must be trained in operational legalities.
[REDACTED]

Receiving Data
GCHQ receives operational data from many partner organisations. The data includes:

- intercept resulting from targeting on Sigint partners' systems
- communications data and other feeds of Sigint and network defence raw material by data transfer
- communications content, events data and communications-related data, received through access to partners' databases
- a wide range of reports including technical, *intelligence reporting* and other forms of collateral
- collateral data received from sister intelligence agencies or other cooperative relationships

[2] This section of the Compliance Guide applies to the sharing of all types of data and not just bulk data sets. The sharing policy for specific types of data such as bulk data sets is agreed in consultation with the relevant teams.

You must handle any operational data obtained from partners in accordance with HRA and as if it were intercepted under RIPA. In particular, you must ensure that its acquisition is authorised, necessary and proportionate, and follow RIPA section 15 safeguards regarding access, review and retention. Particular sensitivity attaches to any such data that is bulk or unselected in nature (i.e. includes details of non-targets) and relates to identifiable individuals. You need to obtain a Data Acquisition Authorisation before you receive any operational data meeting these criteria from a partner. By following this process you will help to ensure that GCHQ's acquisition of the data is demonstrably necessary and proportionate.

Sharing GCHQ's Data

You may share material derived from operational activity with other organisations, but this is subject to:

- legal safeguards
- policy approval
- accountability.

The legal safeguards require that the sharing must be restricted to the minimum necessary for one of GCHQ's operational purposes and that receiving partners must accord the material a level of protection equivalent to GCHQ's safeguards. If therefore you are contemplating sharing significant new lines of material with partners, and/or if you have any concerns relating to the equivalence of the safeguards that will be applied, you should refer the matter *to the relevant team*.

Policy approval may be subject to appropriate filtering or sanitisation of the data being applied in order to protect sensitive equities or UK domestic communications.

These criteria apply to many forms of data sharing, for example through:

- data forwarded to Sigint partners as a result of their targeting on GCHQ's collection systems and other arrangements
- data provided to non-Sigint partners
- allowing access to certain databases
- *intelligence reporting*
- passing technical information and the results of analysis to partners
- sharing sets of intercepted data with industry and OGD partners.

'Sigint development' section of the Compliance Guide

Relevant extracts from the 'Sigint development' section of the Compliance Guide as at June 2014 to the present.

...

Principles

When you perform SD you need to take special care, as your work is likely to give you or others access to the communications of many individuals who are not Sigint targets. The key legal requirements are to obtain any necessary authorisation and to demonstrate HRA by:

- minimising any intrusion into '*the communications of non-subjects of interest*
- balancing this by the expected intelligence benefit

- monitoring/recording actions and outcomes in order to demonstrate compliance.

If you plan a new SD task that is not following established methods or a clear precedent then you must consult *the relevant team* for advice on how to meet these requirements. You should prepare by reading relevant parts of the guidance below. This principle also applies to a significant change to an existing task.

If you plan to develop or use a new system or database for SD then you should follow guidance on Systems & Databases. That includes legality checks with *the relevant team* before any operational usage.

...

'Targeting' section of the Compliance Guide

Relevant extracts from the 'Targeting' section of the Compliance Guide as at June 2014 until the present

...

What is targeting?

Targeting means making a person, organisation or other entity the object of our operational Sigint activities:

- by **seeking** to identify and intercept their communications for intelligence purposes,
- by **searching** for their communications in a database.

CNE and **[REDACTED]** operations can also be considered forms of targeting but are dealt with elsewhere in the Compliance Guide.

Legal basis for targeting

For targeting to be compliant with the law, the use of every selector must be:

- appropriately authorised, and
- justified, which means
  - necessary for one of the purposes in ISA for which GCHQ may exercise its monitoring function, and
  - proportionate.

Additionally, a COPA is required if your target is outside the British Islands and

- is sensitive on grounds of location or nationality, or
- especially sensitive confidential communications are involved.

Demonstrating necessity and proportionality

To demonstrate the necessity and proportionality of your targeting, you must supply a HRA justification. This consists of:

- The JIC purpose and priority, e.g. 1NS.
- The *requirement number* that equates to the intelligence requirement that your targeting seeks to meet.
- A clear free-flow textual justification that explains why you are performing this targeting and addresses any issues of proportionality.

The concept of proportionality is described in more detail in Overview.

When using selectors to target wanted communications, you should consciously:

- target only those that you believe will meet the intelligence requirement,
- consider whether other less intrusive means could achieve the desired result,
- balance the expected intelligence gain against the intrusion into the target's right to privacy, and
- consider whether collateral intrusion into other individuals communications is likely and can be justified.

You must record a clear explanation (HRA justification) for the use of each selector. Guidance on what analysts should provide in a HRA justification can be found here. Follow this link for further details of how to achieve this in the *relevant database*. You should keep the proportionality of the targeting under review and amend the justification if necessary, or cease targeting if the activity no longer meets an intelligence requirement.

...

Demonstrating legal compliance in targeting databases

You must provide the following information in approved targeting databases to demonstrate legal compliance:

- JIC Purpose – NS, EWB or SC, combined with a JIC Priority
- Requirement code - equates to the intelligence requirement that the targeting seeks to meet
- Source field – a traceable and specific source <link to **[REDACTED]** audit best-practice paper, once published on the web> that provides the origin of the targeting
- HRA justification – free-flow text that is specific to your selector and demonstrates why it is necessary and proportionate <6> to intrude on the right to privacy of the person/people whose communications will be collected by that selector; it should not repeat the *requirement* number
- HRA review by date – determines automatic deactivation of targeting if selector is not re-justified. If this selector is subject to a warrant, other legal authorisation or STA, the HRA review by date must not exceed the expiry date of the authorisation. In *the relevant database* this may be set ahead of the authorisation expiry date but targeting will cease when the earlier date is reached.
- Warrant, Legal Authorisation or Copper Ref field – you must record the reference of any legal or policy authorisation
- Warrantry, Legal Authorisation or Copper/STA Ref expiry date – you must ensure that this is correct, as in *the relevant database* this will cause targeting to cease once it has expired
- Location – you must record the current location of your target, using this guidance <8> to help you.
- Nationality – you must record the nationality of your target; please follow the guidance <8> if you do not know or if your target has more than one nationality.

...

In the *relevant database*, you are required to justify retention of target knowledge at the target level – in other words, to justify holding information, including selectors, about your target.

However, justification for placing those selectors on cover – which is a significantly greater interference with the right to privacy – is on a per selector basis in *relevant database*. You must ensure that the justification in *relevant database* adequately

demonstrates the necessity and proportionality of targeting that specific selector, and strengthen it if necessary. Similarly, use of selectors as query terms for searches in intercept databases must be adequately justified at the point of submitting the query.

If multiple selectors for the same target can be covered by the same justification, and the justification is strong enough, it may be cascaded to them from *relevant database*. Where appropriate, you should consider providing an initial justification in *relevant database* that is strong enough to justify whatever action you may wish to take against that target, so that it can be cascaded directly to other systems.

Random samples of records in *relevant database* and intercept repository query logs are audited several times each year, to provide assurance of the legal compliance of GCHQ's targeting. See the Audit section of this Compliance Guide for further details.

***Intelligence Requirement* Code**

Use the *requirement* number of the intelligence requirement that the targeting seeks to meet. For selectors targeted for target development or target discovery purposes, use the *requirement* number of the related intelligence requirement and, in *the relevant database*, tick the 'Sigint Devt' box, which sets the HRA expiry date **[REDACTED].**

If you are targeting a selector for Capability Development purposes, you should use *the relevant code*. **[REDACTED]**

Sigint partner analysts should quote the *intelligence requirement code* that best reflects the intelligence requirement they are working on, as part of their HRA justification when submitting queries to GCHQ intercept databases.

...

Database queries

If you use untargeted selectors to conduct repeated queries over a period of time for the content of an individual's communications, you are targeting them. You should put these selectors onto sustained targeting via a targeting database<17>, first seeking authorisation if necessary.