Compliance Guide 2010-2014

This documents all pre-existing versions of the relevant extracts of the on-line Compliance Guide, 2010-2014.

Double underline indicates gisted for OPEN.

'Overview' section of the Compliance Guide

No previous versions.

'Analysis' section of the Compliance Guide

Extracts from 'Analysis' section of the Compliance Guide April 2014.

Principles

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

The individuals whose communications you examine have a right to privacy. Your queries and analysis must be necessary in order to meet a valid intelligence requirement and proportionate. You usually have to demonstrate this through an HRA justification that is logged for audit.

It is your responsibility to obtain additional authorisation to query and examine the content of communications, if this is required on grounds of location (eg if you discover that a target has entered the UK) or nationality, and to make relevant analysts aware of any significant changes that may affect the legality of the targeting of selectors.

No additional authorisation is needed for querying and examining events data.

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.

HRA justification

You are interfering with 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. It is GCHQ policy to apply the same legal and policy handling rules to all operational data, whether it is acquired by an interception warrant or by any other means. 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 operational purposes:
    - national security (NS)
    - economic well-being (EWB) of the UK (provided that there is also a link to NS)
    - prevention or detection of serious crime (SC)

  and
- proportionate.

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

- Purpose and JIC Priority 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.

Your HRA justification should provide enough information about the individual or organisation so that an uninformed observer e.g. an auditor can understand why it is necessary and proportionate to intrude on an individual's right to privacy - it should not be merely a repetition of the *requirement* number description and should not use abbreviations which would not be understood by an uninformed observer..

Systems that contain communications content may also ask you to provide a legal or policy authorisation reference number if your target is sensitive on grounds of location or nationality, or if your query is intentionally seeking to select data to, from or about person(s) who are sensitive on these grounds. Further detail is in location and nationality.

Some areas have produced local guidance to help staff to understand what constitutes a good HRA justification. Please contact your *relevant policy contact* for more detail.

The 'analysis' glossary at the end of this section of the Compliance Guide provides a list of terms that refer to an individual or organisation.

All queries are logged for audit.

Communications about targets

Bulk personal data

GCHQ acquires and stores some data sets that contain a high proportion of information relating to individuals. This data is either acquired lawfully from GCHQ's own collection operations, or from other parties. In the latter case, acquisition is authorised and recorded by obtaining a Data Acquisition Authorisation (DAA). Some of these data sets are classed as targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but there is something about the data that implies a reasonable expectation that much of it will contain information of intelligence value to GCHQ. Some of these data sets are classed as non-targeted bulk personal data sets i.e. they are personal because each record contains at least the name of an individual, but the majority of the data is not believed to relate to probable intelligence targets. *The relevant policy team* makes the decision about what is targeted and non-targeted bulk personal data, in consultation with data owners. The following types of data include both.

Relevant extract from the 'Analysis' section of the Compliance Guide January 2010 to April 2014.

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 **<1>** 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 an 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 **<2>** for examination of the content of their communications.
If your target is otherwise sensitive on grounds of nationality or location, you need an STA 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 under 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)

  and
- proportionate.

To demonstrate the necessity and proportionality of your search, you must supply an 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' **<1>** 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 extracts from the 'Audit' section of the Compliance Guide November 2010.

Details
All operational query-based systems that make Sigint data available to GCHQ users (including *foreign partner* systems) require HRA justification for each query and create logs of this information. The requirements for logging are stated in the *relevant requirements document*.
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 reference.

'Authorisations' section of the Compliance Guide

Relevant extracts taken from 'Authorisations' section of the Compliance Guide May 2014.

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 Sensitive Relationships Team makes use of these Directions.

Relevant extracts taken from 'Authorisations' section of the Compliance Guide August 2012 to May 2014.

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 Sensitive Relationships Team makes use of these Directions.

Relevant extracts taken from 'Authorisations' section of the Compliance Guide November 2010 to August 2012.

Telecommunications Act direction

We receive communications data from CSPs under the authority of directions under s94 of the Telecommunications Act (as amended by the Communications Act). These directions are issued by the Secretary of State, in the interests of national security

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 [link to Collection and data acquisition: Other data acquisition] and Partnerships [link to Partnerships: Receiving data].

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 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.

Further detail on the new process will be added later in 2010. In the meantime, you should contact *the relevant policy team* for guidance.

Relevant extract taken from the 'Authorisations' section of the Compliance Guide September 2010 to November 2010.

Telecommunications Act direction

We receive communications data from CSPs under the authority of directions under s94 of the Telecommunications Act (as amended by the Communications Act). These directions are issued by the Secretary of State, in the interests of national security.

'Collection and data acquisition' section of the Compliance Guide

Relevant extract from the 'collection and data acquisition' section of the Compliance Guide January 2010

***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 partner* systems
- 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

No previous versions

'Communications data' section of the Compliance Guide

Relevant extracts from the 'Communications data' section of the Compliance Guide August 2013.

Principles

Communications data is data attached to or associated with communications - see the full definition.

The acquisition of communications data, whether through interception, a 'direction' (see below) or a partner organisation, potentially impinges 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 partner*, OGDs and various commercial organisations such as communications and internet service providers (CSPs and ISPs)

[1] In this context, 'targeting' means 'tasking'

- feeds requested from service providers
- ad hoc elements such as billing data or subscriber details for a communications address required 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. Ad hoc elements may be made available in the same way, but this is not normally practical.

Authorisations

GCHQ's acquisition of communications data is authorised in four different ways according to the category above:

- collection of communications data as part of interception 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 considerations of necessity and proportionality
- 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 regularly review with each relevant CSP/ISP exactly what types of communications data we wish to receive. Some are regular feeds, others one-off requests
- if you need ad hoc elements of communications data from a CSP or ISP, you must follow the procedure below, which is designed to comply 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, including guidance for DPs.

'Errors' section of the Compliance Guide

Extracts from 'Errors' section of the Compliance Guide April 2011

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 policy team* straight away. *The relevant policy 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 policy team* and the Legal Advisers determine exactly what constitutes an error.

Reporting potential errors

You should not hesitate to report to *the relevant policy team* any activity that appears to be erroneous or unauthorised

'Oversight' section of the Compliance Guide

Relevant extract from the 'Oversight' section of the Compliance Guide August 2011.

Each commissioner discharges his functions by making regular visits to the SoS, to those agencies (such as GCHQ) which are acting under the authority of warrants issued by the SoS and to relevant government departments (such as FCO WLD which deals with warrant applications on behalf of GCHQ), and by carrying out inspections to ensure that operations are authorised and carried out in accordance with the relevant act.

If a commissioner is informed of or finds any breach of the provisions of the relevant act, other than one that has already been reported on by the Investigatory Powers Tribunal (IPT) <1>, or determines that any of the safeguards required by law are inadequate, he will report this to the PM.

Each commissioner is required to make an annual report to the PM, which is laid before parliament and published. The PM may, after consultation with the relevant commissioner, exclude any sensitive material from the relevant report to be laid before parliament. This typically forms the basis of a highly classified annex, which is not published or made available to parliament.

'Partnerships' section of the Compliance Guide

Relevant extracts from the 'Partnerships' section of the Compliance Guide January 2010

Receiving data

GCHQ receives data from partner organisations under formal and informal agreements. Operational data received this way must be handled in accordance with HRA and is treated as if it were intercepted under RIPA. In particular, it is handled in accordance with RIPA 15 regarding access, review and retention.

Sharing data

GCHQ may share warranted data, such as the results of Sigint analysis, with another organisation, subject to legal safeguards. The safeguards provide that the sharing must be necessary for one of GCHQ's purposes.

In the context of GCHQ's customers, this is the basis of *intelligence* reporting). Safeguards are provided by *a number of processes as well as the STRAP handling regime.*

Selected information from *intelligence reporting* may be released to NATO in accordance with reporting policy.

If you wish to share data other than *intelligence reporting* with a government department, you must do so in an accountable way. You must first consult *the relevant policy team*, who will consider legal and policy requirements, for example relating to disclosure.

[REDACTED]

Relevant extracts from the 'Partnerships' section of the Compliance Guide August 2011

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 may share operational data, such as the results of Sigint analysis, with another organisation, subject to legal safeguards. The safeguards provide that the sharing must be necessary for one of GCHQ's purposes.

In the context of GCHQ's customers, this is the basis of *intelligence reporting*). Safeguards are provided by *a number of processes as well as the STRAP handling regime.*

Selected information from *intelligence reporting* may be released to NATO in accordance with reporting policy.

If you wish to share operational data other than *intelligence reporting* with a government department, you must do so in an accountable way. You must first consult *the relevant policy team* who will consider legal and policy requirements, for example relating to disclosure.

[REDACTED]

Relevant extracts from the 'Partnerships' section of the Compliance Guide February 2013

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 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 policy 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 by *a number of processes as well as the STRAP handling regime.*

Intelligence reporting is not necessary when sharing with *foreign partner* Sigint agencies, although *intelligence reporting* will be 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 Reporting Policy and, when appropriate, International Relations policy and guidance.

If you wish to share operational data with a company, for example to help it develop software for GCHQ, or to share raw operational data with government customers, you should read and apply the published policy and guidance and consult *the relevant team* accordingly.

'Review and retention' section of the Compliance Guide

Extracts taken from the 'Review and retention' section of the Compliance Guide 20 November 2009.

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 May 2010.

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, specially 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 is controlled by procedures described in Authorisation; see also Collection 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 Sigint** must be necessary and proportionate; see particularly *intelligence reporting and foreign partners*, Disclosure and Partnerships.

The mandatory *Legalities* training programme reminds operations 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, eg 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. These ensure that any selection of a UK individual's communications is specifically authorised, usually by a Secretary of State. RIPA section 16 authorisations and processes are described in Authorisation and Targeting.

Additional safeguards

Some safeguards additional to those set out in law are required as a matter of policy because of agreements with the Foreign Office. The following is a list of the safeguards that affect operational activity most directly:

- the internal approval regimes under ISA s7 class authorisations
- the arrangements for designating a subset of senior officials in GCHQ who may approve some RIPA or ISA authorisations, specially in case of urgency; further detail is in Authorisations
- the annual reporting to the Secretary of State on our activities conducted under our WTA authorisation.

'Sharing' section of the Compliance Guide

Relevant extracts from the 'sharing' section of the Compliance Guide January 2010

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 of 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 teams.* Their 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.

You must handle any operational data from partners in accordance with HRA and as if it were intercepted under RIPA. In particular, you must follow RIPA s15 safeguards regarding access, review and retention. There is further detail in *foreign partners* and Partnerships.

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 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 policy team*.

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.

Some further guidance is in Partnerships.

'Sigint development' section of the Compliance Guide

Extracts from the 'Sigint development' section of the Compliance Guide September 2010.

Principles

When you perform SD you need to take special care, as your work may give you or others the possibility of 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 necessity and proportionality by:

- minimising any intrusion into 'innocent' people's communications
- 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* on the *operational concept* and before any operational usage.

'Targeting' section of the Compliance Guide

Relevant extracts from the 'Targeting' section of the Compliance Guide January 2010.

What is targeting?

Targeting is usually the use of a selector intended to identify and select the communications of a target individual or organisation. Selectors may also be targeted to identify other types of communications eg electronic attack – further detail is in Types of targeting.

Sustained targeting is the use of a selector that you know or believe to be used by your target. This targeting is authorised for a maximum of one year before a review <3> is necessary.

Targeting for development purposes is the use of new selectors to establish whether they meet an intelligence requirement. This targeting is authorised for a maximum of three months before a review <3> is necessary.

You may conduct targeting using selectors that do not refer explicitly to a target, such as content keywords<1> to select communications for examination.

The location or nationality <8> of your target determines whether you require any further authorisation.

Using a term that is referable to an individual repeatedly to search and extract stored communications content for a purpose other than the initial reason for selecting and storing that data is also targeting. It is a form of datamining and is covered in Analysis.

Legal basis for targeting

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

- **specifically authorised**, if that is required by law on the grounds of location
- **necessary** for one of GCHQ's Sigint 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)

  in addition to meeting a specific intelligence requirement on the certificate and
- **proportionate**

A policy authorisation is required if your target is sensitive on grounds of location or nationality.

...

<6> **Demonstrating proportionality**

You must demonstrate that your targeting is proportionate. This concept is explained generally in Overview. When targeting selectors you should specifically apply your judgement to:

- targeting the minimum number of individuals to meet the requirement
- considering whether other less intrusive means could achieve the desired result
- balancing the expected intelligence gain against the intrusion into the individual's right to privacy
- targeting only those selectors that you believe will meet the intelligence requirement
- considering whether collateral intrusion into other individuals' communications is likely and whether this can be justified to meet the requirement.

For every selector, you must record your judgement (HRA justification) that clearly explains the reason for the targeting. Please follow this link <9> for further details of how to achieve this in the *relevant database*. You should keep the proportionality of the targeting under review <3> and amend the justification or cease targeting if the activity no longer meets an intelligence requirement.

...

Demonstrating legal compliance in targeting databases

You must use the following fields 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. If multiple selectors used by the same target can be covered by this justification, it may be cascaded to them. But justification remains at selector level so you must ensure that the justification that is cascaded to each selector is sufficiently strong to demonstrate the necessity and proportionality of targeting that selector, and amend it if necessary.

A random sample of records in *the relevant databases are* audited each year to provide assurance of the legal compliance of GCHQ's targeting. Please refer to audit <link to sub-section on **[REDACTED]** audit> for further details.

<7> *Requirement* number for target development selectors

You should use the *Requirement* number that equates to the intelligence requirement that the targeting seeks to meet. In *the relevant database*, you should tick the 'Sigint Devt' box, which sets the HRA expiry date to three months.

...

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.