NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

## Related Links

[REDACTION]

**Do not make changes to this page. Consult the Policy Lead with any queries**

# Communications Data - Guidance on Justifications and Priorities

**Policy Lead:** ***MI5 Warrantry Official***

**Business sponsor:** ***Senior MI5 Official***

**Policy Issue Date: 21 January 2015**

**Review Date: 21 January 2016**

## Policy Aim

**To Provide applicants for Communications Data with the necessary information to draft justifications which effectively address both necessity and proportionality issues and to correctly assign National Priority Grading System (NPGS) grades to applications, as well as information for Designated Persons (DPs) to enable them to identify justifications that are incomplete or relate to sensitive professions or where NPGS priority grades have been inappropriately assigned.**

## Audience

All users of communications data.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

## Principles

- To provide simple and effective guidance to applicants for communications data on how to word justifications in requests for communications data
- To ensure the production of legally compliant justifications through the provision of comprehensive guidance
- To provide simple and effective guidance to applicants for communications data on how NPGS priority grades should be applied to applications
- To provide guidance for DPs on information a proper justification should include and how to identify when an inappropriate priority grade has been assigned to an application
- To ensure that requests for communications data are authorised at the appropriate level
- To identify what constitutes a sensitive profession

## Summary

This page provides a resource for applicants and DPs for communications data, either using ***the electronic system for processing CD requests*** or through the use of ***the relevant form***. It outlines the issues of necessity and proportionality and how both should be addressed when justifying any applications for communications data. It also details how and when the different NPGS priority grades should be assigned. This also provides details of sensitive professions and the different levels of authorisation.

Your attention is also drawn to the S94 Handling Arrangements which came into force on 4 November 2015 - also available via the links to the right of this page – and which relate to the handling acquisition of and access to bulk communications data, specifically the underlying datasets from which [REDACTION] targeted data requests are made. This bulk communications data is obtained pursuant to directions issued by the Home Secretary under section 94 of the Telecommunications Act 1984. The Handling Arrangements, which reflect our existing practice, confirm that the procedure set out in this Guidance (as now updated) must be followed in respect of all communications data requests, whether involving access to targeted communications data or bulk communications data.

It should be noted however that ***the warrantry team*** can advise only on legal compliance issues relating to communications data requests. Enquiries on how to make applications or to track the progress of existing applications should be directed to ***the relevant team***. [REDACTION]

## Table of Contents

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS



## Justifications Overview

Core things to consider in any request for communications data are necessity, proportionality and collateral intrusion. Necessity, Proportionality and Collateral Intrusion require justification in their own separate boxes.

## Necessity

Necessity can be divided into three main points that need to be considered in any communications data justification:

- A short background to the investigation - what is it that we are investigating?

- What role does the target that is associated with this request play in the investigation?

- How does the communications address that is the subject of this request relate to the target and to the investigation?

The applicant must be able to link these three points together in order to demonstrate that any request for communications data is necessary for the statutory purpose specified.

## Proportionality - General

When considering proportionality, applicants need to outline how obtaining the data will benefit the investigation and what intrusion into privacy the request will result in. The main things that need to be considered are:

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

- What are you looking for in the data to be acquired?

- If the data contains what you are looking for, how will this assist you in taking the investigation forward?

- What will be the intrusion into the privacy of the target of the request? Will there be any other intended intrusion taking place?

- Is there another, less intrusive way of obtaining the information you need?

- If a time period of data has been specified, why is this particular time period required e.g. why would a shorter time period not be sufficient?

Therefore, the applicant should explain how the communications data will be used once obtained and how this will benefit the investigation. It is also important that intrusion into the target of the request's privacy is considered.

These points form a large part of the proportionality argument, the other part being in relation to collateral intrusion.

## Proportionality - Collateral Intrusion

Identifying any meaningful collateral intrusion forms part of the proportionality argument. The key question to be asked in relation to this is:

- Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?

- If a time period of data has been specified, how will this impact on the identified collateral intrusion?

- How do you plan to manage any identified collateral intrusion? [REDACTION]

"Meaningful collateral intrusion" includes collateral intrusion that we can foresee is "highly likely" – such as family members using the landline or internet connection where they live. However, we should not speculate where possible collateral intrusion cannot be said to be "highly likely". So when considering this question, the applicant should not detail potential or hypothetical errors. [REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

Therefore, collateral intrusion should always be considered and described if it is identified. However, it may be that none can be identified. When this is the case, then this should be stated. For example, telephone subscriber checks are unlikely to result in any collateral intrusion.

## Guidance for Designated Persons

Designated Persons (DPs) are responsible for granting authorisation for communications data requests. They must ensure that the request is both necessary and proportionate for the purpose for which the data is sought. DPs should take care to scrutinise the application, particularly the justification page, before authorising any request for communications data. In particular, key points DPs should check are:

- Taking into account the guidance for applicants above, that the justification provided by the applicant is sufficient to satisfy the DP that obtaining the requested data is both necessary and proportionate
- That the individual mentioned in the justification is identical with the one for which the data is being obtained, that is that the justification has not been "copied and pasted" from another application
- That the intrusion into privacy that will result from the request has been addressed where necessary and where identified, measures to mitigate collateral intrusion have been outlined. In relation to subscriber details it is accepted that collateral intrusion is likely to be minimal or that none will be identified
- That the time period of data requested is proportionate and that the reasoning for requesting the time period listed is explained in the justification
  DPs are required to reject any application for communications data where they are not convinced of both the necessity and proportionality of the request. DPs are encouraged to consider carefully whether necessity and proportionality have been appropriately considered.

There is no obligation for DPs to comment on individual communications data requests EXCEPT when they relate to sensitive professions in which case you must use the following form of words "The user of xxx is a (Enter sensitive profession) and may use xxx to contact individuals relating to the latter's spiritual welfare/ private constituency matters/confidential medical matters /it may be possible therefore to infer an issue of sensitivity from the fact that someone has regular contact with him/her on xxx. The request may therefore involve a higher degree of interference with privacy given the users sensitive profession. I have balanced the intrusiveness of the interference against the need for it in operational terms and, given that there is no other less intrusive way in which to gather this information, I am satisfied that the higher degree of interference is necessary for the purposes of protecting national security and proportionate to that aim."

However, ***the warrantry team*** would advise DPs to consider adding comments to specific requests if these comments might add anything of value to the investigative

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

record, over and above the case made in the application. In particular, ***the warrantry team*** would recommend that DPs consider adding brief comments in the following scenarios:

- When rejecting an application, to confirm why the request has been rejected;
- when approving large applications with potential for larger collateral intrusion, [REDACTION]
- to add comments in support of the urgency of a particular application;
- to clarify or add any relevant and supportive factors not reflected in the applicant's case;
- where there is unusual interference with privacy or unusual collateral intrusion;
- where data has been requested and collected over a longer period than normal;
- when the request relates to a member of a sensitive profession.

In relation to NPGS grades, DPs should check that they agree with the urgency grade that the applicant has set for an application and if they agree, they may wish to comment on this, although it is not compulsory to do so. If DPs do not agree with the priority grading the applicant has chosen then they can downgrade or upgrade the priority as applicable. Where a DP has changed the priority they must justify the reasons for the change in the "DP justification" box in the "priority" page.

DPs are also encouraged to familiarise themselves with the RIPA Communications Data Code of Practice and the Data Communications Group (DCG) justifications guidance. These documents are available via the links to the right of this page.

DPs should also familiarise themselves with the S94 Handling Arrangements which came into force on 4 November 2015 and which relate to the handling acquisition of and access to bulk communications data [REDACTION]. The Handling Arrangements, which reflect our existing practice, confirm that the procedure set out in this guidance must be followed in respect of all communications data requests, whether involving access to targeted communications data or bulk communications data.

Click here for further guidance for Designated Persons [REDACTION]

## Sensitive professions

The new Code of Practice requires us to give special consideration to the necessity and proportionality of communications data applications that might lead to a higher than usual degree of intrusion. It is recognised that the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates

to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion) known as 'sensitive professions' or 'SPs'. Click here for a list of sensitive profession definitions. [REDACTION]

The existence of CD relating to a SP does not preclude applications being made to obtain such data. However, when making an application for CD relating to someone we know or believe [REDACTION] (please click this link for guidance you should be following prior to making an application) is a member of a SP, or you otherwise think may lead to higher than usual level of intrusion, you should consider whether the proposed conduct is necessary and proportionate and you must clearly set out those considerations in the application.

Furthermore, those CD applications must be approved by an Independent Designated Person (IDP). This have been defined as ***senior MI5 officials*** outside of the direct management chain of the investigator and reporting chain of the investigation.

You must draw attention (within the application) to the sensitivity of the request using the following form of words:

"The user of xxx is a (Enter sensitive profession) and may use xxx to contact individuals relating to the latter's spiritual welfare/ private constituency matters/confidential medical matters /it may be possible therefore to infer an issue of sensitivity from the fact that someone has regular contact with him/her on xxx. The request may therefore involve a higher degree of interference with privacy given the users sensitive profession. I have balanced the intrusiveness of the interference against the need for it in operational terms and, given that there is no other less intrusive way in which to gather this information, I am satisfied that the higher degree of interference is necessary for the purposes of protecting national security and proportionate to that aim."

IDPs must comment on the CD application if it relates to a SP or involves a higher than usual level of intrusion. The comment MUST consider and record the basis upon which they have concluded that the CD to be obtained is necessary and proportionate in the specific circumstances.

Requests for data on members of a sensitive profession will be recorded on MI5 systems; details of these requests will be provided to the Interception Commissioner.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

CD resulting from sensitive profession requests (as above) relating to lawyers may - exceptionally - be protected by legal professional privilege. When reviewing CD product that relates to a lawyer, investigators should therefore consider whether the CD may be legally privileged and if they consider that it may be, they must seek advice from a ***legal adviser***.

## Priorities Overview

Requests for communications data are graded on a nationally agreed, three point scale before being sent to the relevant Communications Service Provider (CSP). This process, which is detailed in the Communications Data code of practice, is called the National Priority Grading System (NPGS). It ensures that CSPs are able to manage their workload effectively and ensure that the most urgent requests are dealt with first.

## NPGS Priority Grades Explained

Requests for communications data can be assigned one of three NPGS priority grades, the definitions of which are provided below:

1 – Very Urgent. [REDACTION]

2 – Urgent. [REDACTION]

3 – Routine. The majority of applications will fall into this category

[REDACTION]

# ANNEX A

## Example *Electronic System for Processing CD Requests* Justifications

Listed below are a few examples of justifications for some of the most common ***the electronic system for processing CD requests*** requests:

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, UNDERLINED AND ITALICS

# ANNEX B

## Scenarios for NPGS Grades 1 and 2

Scenarios are provided below giving example of when NPGS grades 1 or 2 could be applied:

[REDACTION]

# ANNEX C

## Examples for Communications Related Data intrusion issues

[REDACTION]