***This information has been gisted.***

# GCHQ Bulk Personal Datasets Closed Handling Arrangements

## 1. Introduction

1.1 These handling arrangements are made under section 4(2)(a) of the Intelligence Services Act 1994 (ISA). They come into force on 4 November 2015.

1.2 These arrangements apply to the Government Communications Headquarters (GCHQ) with respect to the obtaining, use and disclosure of the category of information identified in Part 2 below, namely "bulk personal datasets".

1.3 The rules set out in these arrangements are mandatory and must be followed by GCHQ staff. Failure by staff to comply with these arrangements may lead to disciplinary action, which can include dismissal, and potentially to criminal prosecution.

## 2. Information covered by these arrangements

2.1 The Security and Intelligence Agencies (SIA) have an agreed definition of a "Bulk Personal Dataset" (BPD). A BPD means any collection of information which:

- comprises personal data;
- relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;
- is held, or acquired for the purpose of holding, on one or more analytical systems within the SIA.

2.2 Bulk Personal Datasets will in general also share the characteristic of being too large to be manually processed (particularly given that benefit is derived from using them in conjunction with other datasets).

2.3 In this context, "personal data" has the meaning given to it in section 1(1) of the Data Protection Act 1998 (DPA), which defines "personal data" as follows:

> "data which relate to a living[1] individual who can be identified –
> - from those data; or
> - from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller [e.g. GCHQ], and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

2.4 Also in this context, "sensitive personal data" has the meaning given to it in section 2 of the DPA and so covers the following:

- Racial or ethnic origin
- Political opinions
- Religious belief or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition

[1] Whilst the DPA refers only to 'a living individual', bulk personal datasets may contain details about individuals who are dead. SIA policy and processes in relation to bulk personal data are the same for both the living and the dead.

- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

2.5 In addition, GCHQ treats a number of other categories of information as sensitive. These include – but are not limited to – areas such as legal professional privilege, journalistic material and financial data.

2.6 GCHQ acquires bulk personal datasets from a variety of sources and uses them to support the performance of its statutory functions, as defined in section 3(1) of ISA. Bulk personal datasets may be obtained under section 4(2)(a) of ISA by agreement with third-party voluntary suppliers and by other non-covert access methods, and also by the exercise of other statutory powers. These statutory powers include those exercisable under warrants and authorisations issued under section 5 and section 7 of ISA in respect of property and equipment interference, and warrants issued under section 5 of the Regulation of Investigatory Powers Act 2000 (RIPA) for the interception of communications. More information on these laws and on other relevant laws may be found in the "Overview" and "Laws" sections of GCHQ's Compliance Guide.

2.7 Although bulk personal datasets constitute only a tiny proportion of the data GCHQ obtains, its retention and use of such datasets represent a significant interference with many people's right to privacy under the European Convention on Human Rights (ECHR). This interference must be justified in terms of its necessity and proportionality, in accordance with Article 8(2) of the ECHR. The use of such data for operational purposes is also especially sensitive and carries an elevated degree of corporate risk. GCHQ has therefore established special arrangements to ensure appropriate handling of such data throughout its life-cycle, both within and, where applicable, beyond GCHQ.

2.8 This document describes these handling arrangements in detail.

## 3. Handling arrangements – general principles

3.1 The SIA recognise several stages in the life-cycle of a bulk personal dataset:

- Acquisition
- Use
- Disclosure
- Retention
- Deletion/destruction

3.2 Considerations of necessity and proportionality underpin each stage: no bulk personal dataset may be acquired, used for operational purposes, disclosed to other organisations, or retained unless it can be demonstrated to the satisfaction of the Authoriser (see paragraph 3.5 below) that it is genuinely necessary to do so for legitimate operational purposes and that doing so is a proportionate way of addressing these purposes.

3.3 In this context, "necessary" means "really needed" for the purpose of discharging one or more of GCHQ's statutory functions.

3.4 "Proportionate" means that the level of interference with the individual's right to privacy is justified when measured against the anticipated benefit to the discharge of GCHQ's statutory functions and the importance of the objective to be achieved. Staff must weigh (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest and to people of no intelligence interest whose data are included in the dataset, against (b) the

operational value they expect to derive from the data. Staff must also consider whether there is a reasonable alternative way of achieving the objective that involves less intrusion.

3.5 In accordance with the joint SIA Bulk Personal Data Policy, the following stages in a bulk personal dataset's life-cycle are subject to formal authorisation by a senior member of staff:

- acquisition and use for operational purposes;
- use for a novel or experimental purpose;
- disclosure of the dataset to another organisation; and
- continued retention and use of the dataset.

3.6 Within GCHQ, authorisations are granted (or refused) by *senior GCHQ officials who are* members of the Senior Civil Service. In the case of continued retention, authorisation is granted (or refused) by a Retention Review Panel, of which *senior GCHQ officials* are members.

3.7 Deletion of a bulk personal dataset does not require authorisation: it should in principle occur as soon as retention can no longer be justified as necessary and proportionate. It must certainly occur if the Retention Review Panel refuses authorisation to retain it or in the event of an intervention to that purpose by the Intelligence Services Commissioner or the Interception of Communications Commissioner.

3.8 The purposes of the authorisation processes described in this document are to ensure that:

- GCHQ's use of bulk personal datasets for operational purposes is genuinely necessary and is proportionate to the outcomes it seeks to achieve;
- these factors have been properly and fully considered; and
- GCHQ minimises the interference with the right to privacy caused by the use of bulk personal data for operational purposes.

3.9 The processes provide:

- a mechanism for recording details of each dataset and the decisions made at various stages throughout its life-cycle;
- objective, senior-level scrutiny and validation of the reasons for which GCHQ holds and uses each bulk personal dataset; and
- the application of consistent standards to assessments of the intrusiveness and corporate risk associated with holding and using bulk personal datasets for operational purposes.

3.10 Details of each dataset and the decisions and actions taken in relation to it are recorded on a single form, which is stored centrally and serves as a record of the dataset's entire life-cycle within GCHQ.

## 4. Acquisition

**[REDACTED]**

4.3 Whatever the means of acquisition, GCHQ gives careful consideration in advance to the value that the dataset is expected to provide to one or more of GCHQ's missions, and to whether it is genuinely necessary and proportionate for GCHQ to use bulk personal data in pursuit of that (those) mission(s).

**[REDACTED]**

4.7 The types of bulk personal datasets GCHQ acquires fall broadly into the following categories; *biographical (e.g. passport details), travel, financial (e.g. finance related activity of individuals), communications and commercial.*

## 5. The acquisition authorisation process

5.1 If it is believed that a sufficiently robust case can be made, in terms of necessity and proportionality, authorisation to acquire (or create) the dataset must be sought. The authorisation process will usually be initiated by the GCHQ operational team that expects to derive most intelligence value from the dataset's use. Ideally, authorisation will be sought and granted before GCHQ acquires (or creates) the dataset. Occasionally, this is not practicable but authorisation must certainly be obtained before a bulk personal dataset is loaded onto a GCHQ system for operational use.

5.2 Representatives of the relevant operational team must seek authorisation by completing a "Bulk Personal Dataset record of authorisation" form ("BPD form"), on which they will identify themselves as "Requester" and "Endorser".

**[REDACTED]**

*5.9/5.10 The Requester/Endorser must also make a case to justify the acquisition and retention of the dataset. The Requester and Endorser must also describe credible plans for the exploitation of the dataset. This is to avoid possession of bulk personal data by GCHQ, and the associated interference with the right to privacy, to no operational benefit.*

5.11 If no credible, short-term plans are in place, authorisation to acquire the dataset will be refused.

## 6. Authorisation to acquire

6.1 Before the acquisition request is forwarded to the Authoriser for consideration, it must be endorsed by a GCHQ Legal Adviser, to confirm that all legal criteria for the dataset's acquisition/creation and continued retention have been satisfied.

6.2 Within GCHQ, authorisations are granted (or refused) by *the relevant senior GCHQ officials*. Both are members of the Senior Civil Service.

6.3 When considering whether to approve an acquisition request, the Authoriser must consider the following factors:

- the intrusiveness of the dataset: the number of people whose information it contains, the proportion of those people who are of no probable intelligence interest, and the sensitivity of the information involved;
- the level of corporate risk incurred by GCHQ's possession and use of the dataset;
- whether the Requester and Endorser have demonstrated the necessity of using the dataset in support of an operational purpose;
- whether it is proportionate to use a bulk personal dataset of this intrusiveness and sensitivity for this purpose; and
- whether only as much information will be obtained as is necessary to achieve the objective(s).

6.4 The Authoriser's decision and his/her assessment of the dataset's levels of intrusiveness and corporate risk must be recorded on the form.

6.5 The initial period of authorisation will normally be 6 or 12 months, depending on the balance between the dataset's anticipated value and its assessed levels of intrusiveness and corporate risk. A shorter (never longer) period might be authorised, in the case of a particularly intrusive or sensitive dataset.

6.6 The Authoriser may, at his/her discretion, approve acquisition of the dataset only for a brief period, for the purpose of determining its precise contents and hence achieving a better understanding of its intrusiveness, sensitivity and potential value. **[REDACTED]**

6.7 If the acquisition request fails to make a wholly convincing case for the acquisition and use of the bulk personal dataset, the Authoriser will either reject the request or may, at his/her discretion, approve it for a short period, during which its value must be clearly demonstrated.

6.8 If the request is rejected, the dataset must not be acquired (or created), or must be deleted or returned to the provider, along with any copies that may have been made, as the case may be. **[REDACTED]**

6.9 No operational exploitation of the dataset must occur before this stage of the process.

## 7. Use

**[REDACTED]**

7.4 Access to bulk personal data on operational systems is controlled through standard GCHQ account management procedures, which ensure that system access is granted only to those with a genuine, operational requirement to access the data.

**[REDACTED]**

7.6 It is GCHQ policy to grant accounts on operational systems only to individuals who have completed appropriate Legal and Policy training, and who have passed the associated tests.

**[REDACTED]**

7.7 Individuals must also sign up to the *appropriate operating procedures*. These *procedures* make it clear that system access is granted, and must be used, only for legitimate, work-related purposes. Details of individuals' access to, and use of, GCHQ IT systems are centrally logged and regularly monitored for evidence of abuse.

7.8 In the case of systems containing operational data, specific details of individuals' activities while accessing the system are logged and are subject to audit. Such logs contain details of who was accessing the system, when, and what they did while logged in. Users are also required to provide a Necessity & Proportionality Statement ("N&P Statement") for conducting an analytical search of the data in the system; an N&P Statement consists of a statement of the operational purpose of the search and an explanation of its necessity and proportionality. These justifications are also logged and are subject to periodic audits of their legitimacy and adequacy.

7.9 GCHQ's Legal and Policy training includes a section on N&P Statements. More detailed guidance on how to formulate legitimate and adequate justifications is available to all staff via links from GCHQ's Compliance Guide.

## 8. Experimental Use

8.1 Use of bulk personal data for an experimental purpose, e.g. development of a novel analytical technique or testing a new IT system, potentially entails an elevated level of risk to the security of the data, increased corporate risk and an additional interference with the right to privacy.

8.2 Any proposed experimental use of a bulk personal dataset must be authorised in advance by the *relevant GCHQ senior officials*. A request for authorisation will be made, using the relevant section of the dataset's BPD form. It will describe the proposed activity and explain why it is necessary and proportionate to use bulk personal data for this purpose. It will also include an assessment of the impact the experimental use is expected to have on the risks and interference mentioned above.

8.3 The Authoriser will consider the necessity and proportionality of the proposed use, in particular whether it is genuinely necessary to use bulk personal data for this purpose, given its intrusiveness and the degree of corporate risk involved.

8.4 If the request to use the bulk personal dataset for the proposed experimental purpose is approved, the Authoriser may, at his/her discretion, set conditions or restrictions on its use. If the request is rejected, the dataset must not be used for that purpose. The decision and any conditions or restrictions must be recorded on the dataset's BPD form.

## 9. Disclosure

9.1 Where the results of bulk personal data analysis are disclosed to partner or customer organisations, this must be done via standard *reporting* mechanisms, which ensure release of GCHQ intelligence in a secure, accountable, legally compliant manner.

9.2 If disclosure of a bulk personal dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed:

9.3 Another SIA Agency:

9.3.1 If the proposed recipient of the dataset is another SIA Agency, that Agency will (as with any other operational data) formally request transfer of the data via the "Inter-Agency Sharing" (IAS) process. As with authorisation to acquire a bulk personal dataset, this disclosure request will be considered and authorised (or rejected) by *relevant GCHQ senior officials*. The Authoriser's decision and the reasons for it will be recorded on the dataset's BPD form, as well as on the IAS request form.

**[REDACTED]**

9.4 Other organisations:

9.4.1 For any other organisation, whether another UK partner or a *foreign partner*, the dataset's Requester or Endorser will submit a request for authorisation to disclose, by means of the dataset's BPD form. Again, such requests will be considered by *relevant GCHQ senior officials*.

9.5 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of:

- its necessity and proportionality, and

- the intelligence or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.

9.6 The Authoriser will consider:

- the content of the dataset: the nature of the personal information it contains, its intrusiveness and sensitivity;
- the nature and extent of the corporate risk the disclosure would entail;
- the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
- whether any caveats or restrictions should be applied; and
- the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary.

**[REDACTED]**

## 10. Continued Retention

10.1 The ongoing retention of every bulk personal dataset is reviewed at least every 24 months by the Bulk Personal Data Retention Review Panel (the Panel).

10.2 The Panel consists of *relevant senior GCHQ officials*:

10.3 Representatives from MI5 and SIS are normally invited to observe and contribute to discussions.

10.4 The Panel meets every 6 months, typically in March and September, to consider the datasets due for review and to review the functioning of the bulk personal dataset life-cycle management processes. Discussions, decisions and actions are minuted.

10.5 If a dataset's Requester and Endorser consider that a convincing case can be made to justify the continued retention and exploitation of that dataset, they must submit a retention request to the Panel by means of the dataset's BPD form. If they do not believe a convincing case can be made, they must arrange for the deletion of the dataset as soon as they reach this conclusion.

10.6 In the request, they must justify the interference with the right to privacy caused by GCHQ's continued retention and exploitation of the dataset. They must set out why it is genuinely necessary and proportionate to continue to retain and use the data. This rationale must be supported by concrete evidence, including specific examples, where possible, of the operational value provided by the dataset during the previously authorised period. They should explain why they expect the dataset to continue to provide similar value in future.

10.7 The Requester and Endorser will take account of a dataset's value to other GCHQ business units when considering whether to make a retention request and will reflect that value in their retention justification. If the dataset has been disclosed to another (external) organisation, they will also take account of its value to that organisation.

10.8 In the case of datasets containing older material, a specific justification must be provided to explain why the older material remains of value and should not be deleted when it ages past a certain (previously specified and context-dependent) threshold.

10.9 The Panel will consider:

- whether a persuasive case has been made;
- whether it continues to be necessary and proportionate to retain the data;
- whether the degree of intrusiveness and corporate risk associated with continuing to hold and use the data remains as previously assessed;
- whether it is now possible to obtain the data of interest (the whole dataset or a subset thereof) through less intrusive means;
- whether any caveats or restrictions should be applied; and
- whether the retention request should be approved.

10.10 If the Panel approves the request, it will authorise continued retention for a specific period, usually for 12 months (until the next-but-one Panel meeting). Where some doubt remains as to the value of a dataset, or where the dataset is particularly sensitive, the Panel may authorise a shorter retention period, typically 6 months (until the next Panel meeting), occasionally less. A 24-month retention period may be authorised if the dataset is deemed to be of low intrusiveness and to represent low corporate risk

10.11 If the Panel rejects the request, or if a convincing retention case cannot be submitted to the Panel, the dataset and any copies must be deleted from GCHQ systems as soon as practicable. **[REDACTED]**

## 11. Deletion

11.1 When a bulk personal dataset is no longer of use, or a persuasive case for its continued retention and use cannot be made, the data must be deleted. **[REDACTED]**

11.2 It may not be possible to make a persuasive case for continued retention for a variety of reasons, for example:

- GCHQ may have stopped working the mission for which the data was acquired;
- it may not be possible to demonstrate that it is genuinely necessary and proportionate to hold and exploit the data;
- the dataset has failed to provide the anticipated operational value;
- the data is old and its value has diminished beyond the point where it is essential to the mission.

11.3 In such circumstances, the dataset's Requester and Endorser should not wait for the next six-monthly BPD Panel meeting but should ensure that the dataset is deleted as soon as practicable.

11.4 Where older data is no longer essential to the mission, it may be appropriate to implement a "rolling deletion window", such that data over a certain age is deleted, or the oldest data is deleted as new data is received. Such an approach should be adopted, wherever practicable, in order to minimise corporate risk and interference with the right to privacy.

11.5 When GCHQ can no longer justify the retention of a dataset, the dataset's Endorser is responsible for ensuring that:

- the data (including any copies) is deleted,
- confirmation is sent to the *relevant GCHQ policy team*, and
- details of deletion are recorded on the dataset's BPD form.

11.6 If GCHQ is the originator ("primary acquiring Agency") of a dataset that it has disclosed to another organisation but can itself no longer justify keeping, the Endorser must agree

future responsibilities with the other organisation, with respect to ownership, further acquisition (if any), safeguarding and ultimate deletion of the dataset.

## 12. Oversight

12.1 Internal:

12.1.1 GCHQ employees' conditions of employment make it clear that "unauthorised entry to computer records" may constitute gross misconduct, subject to disciplinary measures potentially including dismissal. Users of GCHQ IT systems *are also made aware through the applicable security policies* of their responsibilities regarding the proper use of corporate IT systems.

12.1.2 All staff, contractors and integrees across the extended GCHQ enterprise are required to complete the *relevant legalities training*, which reiterates that GCHQ IT systems are to be used only for legitimate, necessary, work-related purposes and that access and use are subject to monitoring. It also contains a brief section specifically devoted to Bulk Personal Data.

12.1.3 Additionally, anyone requiring access to systems containing "operational data" (which includes bulk personal data) must successfully complete Advanced Legal & Policy training before accounts will be granted. This Advanced training contains detailed sections on necessity and proportionality and on N&P Statements (including audit – see below).

12.1.4 Activity on IT systems holding bulk personal datasets is subject to audit, both from a security perspective (to ensure that there is no inappropriate access) and to verify that legitimate access is used only for properly authorised, necessary and proportionate purposes.

12.1.5 The latter is termed "N&P audit" and looks specifically at the reasons and justifications for running queries and searches in data held on the systems in question. Before submitting a query, the analyst is required to enter into the system a clear explanation of:

- the operational requirement in connection with which the query is made;
- how the query relates to the requirement;
- why it is necessary to run that particular query; and
- how the interference with the right to privacy the query will cause is proportionate to the outcome it is expected to achieve.

12.1.6 These justifications are centrally logged and are subject to N&P audit.

12.1.7 The *relevant senior GCHQ official*, who is a member of the BPD Retention Review Panel, will keep GCHQ's Executive Committee, of which she is also a member, apprised of any pertinent issues relating to Bulk Personal Data.

12.2 External:

12.2.1 The majority of the bulk personal datasets held by GCHQ are acquired by means other than interception under RIPA warrant; they therefore fall within the oversight purview of the Intelligence Services Commissioner (ISComm). The remaining few datasets, formed from intercepted material (see the section on Acquisition above), are overseen by the Interception of Communications Commissioner (IOCC).

12.2.2 The Commissioners each visit GCHQ at least twice a year for formal inspections and will typically inspect a sample of bulk personal datasets of their choice on each occasion. They will examine records (including the BPD forms) and interview officers responsible for the acquisition and management of the datasets; they may also request information on how data is handled and used. GCHQ must be able to demonstrate to the Commissioners that proper judgements have been made on the necessity and proportionality of acquiring, using, disclosing and retaining bulk personal datasets.

12.2.3 The ISComm also reviews the adequacy and effectiveness of GCHQ's policies and procedures for managing bulk personal datasets, and oversees controls to prevent and detect misuse of bulk personal data. Any reports on investigations arising out of auditing activity (see paragraph 12.1.4 above) will be drawn to the attention of the ISComm. The IOCC reviews the adequacy and effectiveness of GCHQ's arrangements to minimise the retention and dissemination of intercepted material ("RIPA Safeguards").

12.2.4 The Commissioners provide independent oversight of GCHQ's compliance arrangements and report their findings to the Prime Minister: the ISComm annually, the IOCC biannually.

12.2.5 From time to time, GCHQ may additionally report significant issues relating to BPD to the Foreign Secretary.