*All gists in the following extract have been double-underlined

SECRET
INTELLIGENCE
SERVICE

AUTHORISATION OF BULK PERSONAL DATASET

1. Definition

This Authorisation Form records the justification for SIS' handling and usage of specific bulk personal datasets. Bulk personal datasets are acquired under Section 2(2)(a) of the Security Service Act 1989 or Sections 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994 and have the following characteristics:

- They comprise personal data as defined by section 1(1) of the Data Protection Act 1998;
- They relate to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;
- They are held, or are acquired for the purpose of holding, on one or more analytical systems within SIS.

2. Acquisition Case *to be completed by the Acquiring Officer*

Dataset Codename and File Reference	
Data Owner **NB: A senior SIS official will be the data owner unless specified. This means a senior SIS official will have devolved responsibility for 'Action On'.**	
Description of Dataset Content **NB: This description will be used in lists of datasets presented to oversight bodies (e.g. the Foreign Secretary, the ISC, the Intelligence Services Commissioner) and will be seen by staff in the relevant directorate who manage the Service's bulk data records.**	
Sanitised Description of Dataset Content **NB: This description will be used on the database.**	
Source **[redacted]**	
Date of Acquisition (DD/MM/YYYY)	
Proposed frequency of update	<select>
Protective Markings	<select> <select>
National Caveat	<select> Other:
Who is responsible for Action On? (Designation/Organisation) **NB: Please specify only if different from the data owner or if data is not owned by SIS [redacted]. The Officer stated will be expected to respond to enquiries from HO teams, [redacted] and Duty Officer when required**	
Any special Action On handling requirements **[redacted]**	
Can this Dataset be Shared in bulk?	SIA: Yes ☐ No ☐ [redacted]
Media Serial Number	

Necessity

Please explain why it was necessary for SIS to acquire this data covering the following points:

- Which NSC strategic intelligence priorities does this acquisition meet?
- What results or benefit do you expect it to provide in relation to SIS's functions and the purposes of UK national security, economic wellbeing of the UK and the detection/prevention of serious crime?

Risks of holding this data to SIS and to wider HMG

NB: The operational risks around acquisition of this data should have been dealt with elsewhere (e.g. KD, submission etc)

Please comment on the following:

- What are the risks of holding this dataset that might have the potential to cause political or reputational embarrassment? Consider also if there could be economic impact on the UK or the risk of litigation.
- What is the damage to SIS' operational equities should SIS possession of this dataset become known? What impact could there be on our capabilities and operations?

Overall classification of Risk	<select>
Designation/Staff Number	
Date	

3. Data Intrusiveness *(to be completed by the Transformation Officer)*

Contains Data on UK Nationals?	Yes ☐	Reasonably Likely ☐	Unlikely ☐	No ☐
How have you reached this assessment?				
Contains Data on Minors (under 16s)?	Yes ☐	Reasonably Likely ☐	Unlikely ☐	No ☐
How have you reached this assessment?				

Does the dataset contain any categories of personal data deemed to be particularly intrusive? Yes No		
	Yes	No
Financial	☐	☐

Religion	☐	☐	Criminal Activity	☐	☐
Political (including trade union membership)	☐	☐	Legally Privileged Info	☐	☐
Racial/Ethnic Origin	☐	☐	Journalist Info	☐	☐
Disability/Medical Condition	☐	☐	Medical Info	☐	☐
Sexual Orientation	☐	☐	Spiritual Counselling	☐	☐

If 'Yes' is ticked for any of the above, please provide further details	
Designation/Staff Number	
Date	

4. Exploitation Case *(to be completed by the Exploitation Officer)*

Proposed exploitation system(s) for the dataset (the SIS database, [redacted] etc)	
If section 3 above indicates that information on minors is present or is reasonably likely to be present, is this to be exploited?	Yes, it will be exploited ☐ **(NB: ensure a specific justification for this is included below)** No, it will not be exploited ☐ **(NB: state below if the information will be deleted)**

If section 3 above indicates that there are categories of personal data present that are deemed to be particularly intrusive, please indicate whether these will be exploited and on which systems they will be available (please tick all that apply)

NB: If any category is to be exploited, a specific justification must be included below. If a category is not to be exploited, state below if the information will be deleted.

	Will not be exploited	[redacted] only	The database & [redacted]	[redacted]	Standalone system	Other (please specify)
Religion	☐	☐	☐	☐	☐	
Political (including trade union membership)	☐	☐	☐	☐	☐	
Racial/Ethnic Origin	☐	☐	☐	☐	☐	
Disability/Medical Condition	☐	☐	☐	☐	☐	
Sexual Orientation	☐	☐	☐	☐	☐	
Financial	☐	☐	☐	☐	☐	
Criminal Activity	☐	☐	☐	☐	☐	
Legally Privileged Info	☐	☐	☐	☐	☐	
Journalist Info	☐	☐	☐	☐	☐	

Medical Info	☐	☐	☐	☐	☐
Spiritual Counselling	☐	☐	☐	☐	☐

Intrusion of Exploitation

What is the assessment of the level of actual and collateral intrusion?

- Actual: the intrusion of (or interference with) privacy caused by accessing personal data as a result of analysis to identify and investigate intelligence targets;
- Collateral: the intrusion or interference with privacy of individuals who are not of intelligence interest, which happens as a consequence of the analytical process.

Classification of Actual Intrusion	<select>
Classification of Collateral Intrusion	<select>

Justification

- How will SIS make use of this data? What intelligence benefits are to be derived from exploitation of the data?
- If the dataset contains information on minors or categories of personal data deemed to be particularly intrusive, ensure you make a specific justification for holding and/or using each of these categories.
- Given the potential to intrude into the privacy of individuals contained in this dataset, explain why the continued retention and/or exploitation of the dataset is necessary and proportionate.

[redacted]

Given all of the above, I judge that it is necessary and proportionate to retain/retain and exploit [delete as appropriate] this dataset. Retention of this dataset will be reviewed regularly by SIS's Data Retention Review Panel.

Designation/Staff Number	
Date	

5. Legal Advice *(to be completed by a legal adviser)*

Having regard to (i) the information set out in this form and (ii) the legal considerations document attached to the IW, I am satisfied that holding this data complies with the Intelligence Services Act 1994 (ISA 1994), Data Protection Act 1998 (DPA 1998) and Human Rights Act 1998 (HRA 1998).

Designation/Staff Number	

Date	

6. Data Authorisation *(to be completed by a senior SIS official)*

I am satisfied that it is necessary and proportionate for SIS to retain and/or exploit this data set as described above, and that satisfactory arrangements exist for ensuring proper management and protection of the data. I authorise the retention and/or exploitation of this dataset.	
Designation/Staff Number	
Date	

LEGAL CONSIDERATIONS IN RESPECT OF THE AUTHORISATION OF BPD

Intelligence Services Act 1994 (ISA 1994)

Does it fall within SIS functions and purposes to obtain data under section 1(1)(a) of ISA 1994? Section 1(1)(a) provides that one of SIS's functions shall be to obtain information relating to actions of persons outside the British Islands. These functions are exercisable in the interests of national security (with particular reference to the defence and foreign policies of Her Majesty's Government in the UK), the economic well-being of the UK or in support of the prevention or detection of serious crime (section 1(2) ISA 1994). No information should be obtained by SIS except so far as is necessary for the proper discharge of its functions (see s2(2) ISA).

Data Protection Act 1998 (DPA 1998)

Is processing this data necessary for the exercise of functions conferred by an enactment (i.e. ISA section 1)? If yes, processing this data will be lawful as provided for by DPA 1998 Schedule 2 para 5(b) and, to the extent that it may apply in this case, Schedule 3 para 7(1)(b). Where necessary for the purpose of safeguarding UK national security, consideration may be given to whether SIS may rely on the exemption under section 28 of the DPA 1998.

Human Rights Act 1998 (HRA 1998)

Holding and exploiting this data may amount to an interference with Article 8 of the ECHR. Interference may only be justifiable if it is both necessary and proportionate. The case for both necessity and proportionality should be made clearly in the authorisation form.

The interference may be necessary if it is necessary for one or more of the legitimate functions of SIS (acting to protect national security in the UK; acting in the interest of the economic well-being of the UK; acting in support of the prevention or detection of serious crime). The interference may be proportionate if there is a reasonable balance between the degree of intrusion into privacy (as set out in the authorisation form, both actual and collateral) and the intelligence to be gained.

Any steps taken to reduce intrusiveness (including, but not limited to, the extent of access, the systems onto which the data will be loaded, a decision to limit the fields of data loaded) will be relevant to the decision on proportionality and must be considered.

The nature of the dataset will also be relevant to the decision on proportionality. Where data that SIS deems to be particularly intrusive is included in the dataset, specific justification for why it is necessary and proportionate to acquire, retain and exploit (if applicable) the particularly intrusive data should be set out. If it is clear that the dataset contains records for minors, specific justification should be given for acquiring, retaining and exploiting those records.