ANNEX A

Certificate reference:- DPA/s28/TSS/2

SECTION 28 DATA PROTECTION ACT 1998

CERTIFICATE OF THE SECRETARY OF STATE

1. Whereas:

(i) by section 28(1) of the Data Protection Act 1998 ("the Act ") it is provided that personal data are exempt from any of the provisions of :-

(a) the data protection principles;

(b) Parts II, III and V; and

(c) section 55

of the Act if the exemption from that provision is required for the purpose of safeguarding national security;

(ii) by subsection 28(2) it is provided that a certificate signed by a Minister of the Crown certifying that the exemption from all or any of the provisions mentioned in subsection 28(1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact;

(iii) by subsection 28(3), it is provided that a certificate under subsection 28(2) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.

2. **And considering** the potentially serious adverse repercussions for the national security of the United Kingdom if the exemptions hereafter identified were not available.

And for the reasons set out in document referenced **DPA/S28/TSS/2-REASONS**, in summary that:

2.1 The work of the security and intelligence agencies of the Crown requires secrecy.

2.2 The general principle of neither confirming nor denying whether the Security Service processes data about an individual, or whether others are processing personal data for, on behalf of with a view to assist or in relation to the functions of the Security Service, is an essential part of that secrecy.

2.3 In dealing with subject access requests under the Data Protection Act 1998, the Security Service will examine each individual request to determine:

i) whether adherence to that general principle is required for the purpose of safeguarding national security; and

ii) in the event that such adherence is not required, whether and to what extent the non-communication of any data or any description of data is required for the purpose of safeguarding national security.

2.4 The very nature of the work of the Security Service requires exemption on national security grounds from those parts of the Act that would prevent it, for example, passing data outside the European Economic Area and that would allow access to the Security Service's premises by third parties.

3. Now, therefore, I, the Right Honourable David Blunkett MP, being a Minister of the Crown who is a member of the Cabinet, in exercise of the powers conferred by the said section 28(2) do issue this certificate and certify as follows:-

3.1 that any personal data that are processed by the Security Service as described in Column 1 of Part A in the table below are and shall continue to be required to be exempt from those provisions of the Act that are set out in Column 2 of Part A;

3.2 that any personal data that are processed by any other person or body (in circumstances where that data processing comprises or includes the retention or disclosure of data by that other person or body for or to the Security Service) in the course of data processing operations carried out for, on behalf of or at the request of the Security Service or in relation to the functions of the Security Service of the Security Service Act 1989 as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act that are set out in Column 2 of Part B;

3.3 that any personal data that are processed by any other person or body (other than a government department, agency or non-departmental public body) in the course of data processing operations following the data's disclosure to that person or body by the Security Service in accordance with section 2(2)(a) of the Security Service Act 1989 as described in Column 1 of Part B in the table below are and shall continue to be exempt from those provisions of the Act that are set out in Column 2 of Part B;

3.4. that any personal data that are processed by the Security Service for the purposes set out in Column 1 of Part C in the table below are and shall continue to be required to be exempt from those provisions of the Act that are set out in Column 2 of Part C below; and

3.5. that any personal data that are processed by the Security Service as described in Column 1 of Part D of the table below are and shall continue to be required to be exempt from those provisions of the Act that are set out in Column 2 of Part D below

all for the purpose of safeguarding national security, provided that:

(i) no data shall be exempt from the provisions of section 7(1)(a) of the Data Protection Act 1998 if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that adherence to the principle of neither confirming nor denying whether the Security Service holds data about an individual is not required for the purpose of safeguarding national security;

(ii) no data shall be exempt from the provisions of section 7(1)(b), (c) or (d) of the Data Protection Act 1998 if the Security Service, after considering any request by a data subject for access to relevant personal data, determines that non-communication of such data or any description of such data is not required for the purpose of safeguarding national security.

4. This certificate gives notice that I require the Security Service, by virtue of my authority arising from s1(1) of the Security Service Act 1989, to report to me on the operation of the exemptions described in this certificate

PART A	
Column 1	**Column 2**
Personal data processing in performance of the functions of the Security Service described in Section 1 of the Security Service Act 1989 as amended by the Security Service Act 1996, including recruitment of staff of the Security Service and assisting with the recruitment of staff of the Secret Intelligence Service and GCHQ and vetting of the Security Service's candidates, staff, contractors, agents and others in accordance with the government's vetting policy	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(1)(c), 16(1)(d), 16(1)(e), 16(1)(f), 17, 21, 22, and 24 of Part III; (iii) Part V; (iv) the first data protection principle; (v) the second data protection principle; (vi) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate; and (vi) the eighth data protection principle.

Part B	
Column 1	**Column 2**
Personal data processing for, on behalf of or at the request of the Security Service or in relation to the functions of the Security Service described in section 1 of the Security Service Act 1989 as amended by the Security Service Act 1996 or following the data's disclosure to that person or body by the Security Service in accordance with section 2(2)(a) of the Security Service Act 1989, including recruitment of staff of the Security Service and assisting with the recruitment of staff of the Secret Intelligence Service and GCHQ and vetting of the Security Service's candidates, staff, contractors, agents and others in accordance with the government's vetting policy	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(1)(c), 16(1)(d), 16(1)(e), 16(1)(f), 17, 21, 22, and 24 of Part III to the extent that those provisions require any reference to the Security Service or data processing operations carried out by or in support of the Security Service or in consequence of a lawful disclosure by the Security Service ; (iii) Part V; (iv) section 55; (v) the first data protection principle; (vi) the second data protection principle; and (vii) the sixth data protection principle to the extent necessary to be consistent with the exemptions contained in this certificate.

PART C	
Column 1	**Column 2**
1. Personal data processed by the Security Service for the purposes of administration of human resources (including data relating to former members of staff but excluding the contents of the filing system containing confidential data as described in Part D of this table) and staff pay, tax and national insurance contributions	1. Sections 16 (1) (f), 47 and 50 and Schedule 9.
2. Personal data processed by the Security Service for the purposes of maintaining CCTV coverage of Thames House, 12 Millbank, London in relation to the security and integrity of the building	2. Sections 47 and 50 and Schedule 9.
3. Personal data processed by the Security Service for the purpose of commercial agreements (whether concluded or otherwise) or other arrangements with 3rd parties, in relation to which the Security Service supplies goods or services or under which the Security Service receives goods or services, whether the goods or services are supplied or received under those agreements, arrangements or otherwise (and to the extent that the data do not comprise data to which Parts A or B of this certificate apply)	3. Sections 16 (1) (f), 47 and 50 and Schedule 9

Part D	
Column 1	**Column 2**
Personal data processed by the Security Service for the purpose of maintaining and consulting a filing system containing confidential data about current and former members of its staff, the purpose of which is to provide personnel officers and managers with information considered necessary to make informed decisions as to the suitability of individuals for any task, appointment, posting or any other matter, with particular regard to the security implications of those decisions	(i) Sections 7(1), 7(8), 10, 12 of Part II; (ii) Section 16(c), 16(e), 16(f), 17, 21, 22, and 24 of Part III; (iii) Part V; and (iv) The eighth data protection principle

David Blunkett

.....

The Right Hon. David Blunkett, MP

10 / 12 / 01

.....

Dated

I confirm that the Home Secretary approved this certificate and it was signed with his personal stamp.

Name .....

Signed .....

Dated 10 / 12 / 01

Annex C

Document Reference **DPA/S28/TSS/2-REASONS**

REASONS FOR THE HOME SECRETARY SIGNING THE DATA PROTECTION ACT 1998 s28 (NATIONAL SECURITY) EXEMPTION CERTIFICATE COVERING PERSONAL DATA PROCESSED BY THE SECURITY SERVICE – REFERENCE DPA/S28/TSS/2

1. Introduction

1.1. The section 28 certificate, document reference **DPA/S28/TSS/2,** was signed by the Home Secretary following a request made to him by the Security Service. This document explains the reasons he did so. It is made public to allay concerns that anyone may have about the use by the Security Service of the data protection national security exemption that exists under section 28 of the Data Protection Act 1998.

1.2. Before signing the certificate the Home Secretary considered the following factors:

i. The Data Protection Act 1998 (DPA), its national security exemptions, and role of the National Security Panel of the Information Tribunal (the "Tribunal").

ii. The functions of the Security Service and its primary role in the protection of national security.

iii. Why secrecy is essential to the work of the Security Service and the damage or potential damage that can be done to national security when secrecy is compromised.

iv. The need and use of the neither-confirm-nor-deny policy.

v. The Tribunal determination in the appeal by Norman Baker MP against a s28 certificate signed by the previous Home Secretary covering personal data that the Security Service may have processed.

vi. The safeguards and statutory controls that exist on the activities of the Security Service.

vii. The non-DPA remedies open to anyone who feels aggrieved by anything which he or she believes the Service has done in relation to them or their property.

viii. The test that should be used to balance the need to safeguard national security and purposes of the DPA.

ix. The form and scope of the certificate.

x. The checks, procedures and reporting obligations placed on the Security Service as conditions of their use of the certificate.

xi. Other points on the Security Service's need for use of exemptions under the Data Protection Act 1998.

These factors are explained below.

1.3. While this document gives as full as possible account of the reasons why the Home Secretary signed the certificate, it must be remembered that there are other considerations not set out here. These considerations arise from the Home Secretary's personal detailed knowledge of the secret work of the Security Service. Obviously, these considerations cannot be made public.

1.4. This document focuses on the use of the national security exemption from the entitlement of an individual, under section 7 of the DPA, to be told by a data controller whether or not that data controller holds personal data on that individual and, if held, provide information on the data being held. Almost inevitably, a subject access request will be the first step for anyone concerned by the possibility of the Security Service processing personal data on them. The Security Service is seen to be a data controller.

2. The Data Protection Act 1998, its national security exemptions, and role of the Tribunal.

2.1. The Data Protection Act 1998 (DPA) came into force on 1 March 2000. The DPA made new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

2.2. Section 7 of the DPA, created a general entitlement for an individual to ask and be told by anyone who decides on purposes of processing personal data whether personal data on

them is being processed, which includes being held, and if it is, be told certain information about that data. The entitlement to ask and be told in this way is known as "subject access". The main rationale for subject access is so an individual can satisfy himself or herself as to what, if any, personal data is being processed about them, that any processing is done for a proper purpose, that the data is accurate, and to whom the data may be disclosed. If dissatisfied with the outcome of their request, the individual can then take corrective action.

2.3. The DPA recognises that there are certain circumstances when it would be inappropriate to comply with certain of the DPA's provisions, and so provides several exemptions. One, at DPA section 28, exempts personal data from a number of provisions, including those of subject access, if the exemption is required for the purpose of safeguarding national security.

2.4. DPA section 28 also provides that a Cabinet Minister may sign a certificate as conclusive evidence of the need for the use of the national security exemption. The certificate may identify the personal data to which it applies by means of a general description and may cover personal data processed after the date the certificate came into effect. Such a certificate will channel appeals against that certificate or its coverage to the National Security Panel of the Information Tribunal (the Tribunal) for consideration and determination.

2.5. The Tribunal considers appeals against a section 28 certificate by applying the principles used by the court on a judicial review. If the Tribunal determines the Minister did not have reasonable grounds for issuing the certificate or the actions in issuing the certificate were not proportionate for the purpose, the Tribunal may quash the certificate.

3. The functions of the Security Service and its primary role in the protection of national security.

3.1. The functions of the Security Service are set down in law – the Security Service Acts 1989 and 1996. It has three functions: protect national security, safeguard the economic well-being of the United Kingdom against threats posed outside of the British Islands, and - following the 1996 Act – support law enforcement agencies in the prevention and detection of serious crime. The 1996 Act defines such crime. The 1989 Act places the Security Service under the authority of the Secretary of State.

3.2. A booklet – *MI5, The Security Service* – explains in some detail the work of the Security Service. As the Service's Director General summarised in his introduction to the

booklet, the Security Service's tasks are both to investigate and to counter covertly organised threats to the UK such as terrorism and espionage. The booklet explains that the Government decided that the Service should use its know-how, gained from their national security work, in support of law enforcement agencies in combating serious crime. This led to the 1996 Act. The booklet is available from the HMSO. Similar information is also available on the Security Service's Internet web site. The address is http://www.securityservice.gov.uk.

3.3. The work of the Security Service is vital in safeguarding the national security of the United Kingdom. Intelligence successes relating to national security can, and have:

- saved the lives of British nationals and other persons;
- prevented the spread of weapons of mass destruction;
- thwarted those who would overthrow or undermine the United Kingdom's parliamentary democracy through terrorism and other means; and
- countered the actions of foreign powers intent in damaging the interests of the country.

3.4. Members of the Security Service have no powers to question or arrest anyone, or demand entry into premises or demand to search anyone or anything. They are not like police or customs officers.

4. Why secrecy is essential to the work of the Security Service and damage and potential damage that can be done to national security when secrecy is compromised.

4.1. Secrecy is essential to the work of the Security Service. Many individuals who co-operate with the Service –such as agents - only do so under guarantee of complete confidentiality and anonymity. If their identity became known not only would it jeopardise the work in hand and their future co-operation but also it would put them at personal risk. Such a risk is not fanciful, as a large part of the Security Service's work comprises the investigation of terrorists. Clearly, the same risks apply to members of the Security Service itself.

4.2. Secrecy is also essential because the Security Service undertakes investigations covertly. The Service's effectiveness lies in its ability to obtain and exploit secret

intelligence, which those under investigation may go to some lengths to keep hidden. As well as the use of agents mentioned above, sources of secret intelligence include:

a. the interception of communications,

b. eavesdropping, and

c. surveillance.

Clearly, such techniques lose much if not all of their effectiveness if it is known when and how they are used.

4.3. So, if an individual were to become aware that they were subject to a Security Service investigation, they could not only take steps to thwart it but also attempt to discover, and perhaps reveal, the methods of investigation used, or the identities of the Security Service officers, or agents involved in such methods of investigation. Compromise of methods or personnel affects both the individual investigation and potentially all other such investigations as the risk of deploying such methods and personnel is increased. Similarly, increased knowledge of methods of investigation deployed by the Security Service, and other agencies, would greatly assist those such as terrorists, spies, and serious criminals in planning their activities, so as to the reduce the likelihood of detection or interference.

4.4. Ultimately, the undermining of the effectiveness of the Security Service could result in the loss of, or a reduction in, the deterrence of those who may be tempted to damage national security. In addition, it could also result in the loss of, or a reduction in, the reputation of the Security Service itself. This could lead to a reduction in the co-operation that the Security Service actively receives from individuals and organisations both at home and abroad and also to an impairment of the ability of the Security Service itself to recruit staff. Anything that weakens the effectiveness of the Security Service weakens the UK's ability to safeguard national security.

5. The need for and use of the "neither confirm nor deny" policy.

5.1. It has been the policy of successive governments neither to confirm nor to deny suggestions put to them on the work of the intelligence and security agencies including the Security Service. Put simply, the policy is a way to preserve the secrecy described above by giving a vague and non-committal answer.

5.2. The need for such a policy and Parliament's acceptance of this is reflected in legislation. Such legislation includes the Security Service Act 1989, which places a duty on the Director General to ensure that no information is disclosed by the Service except so far as necessary for the proper discharge of its functions. It also includes the Official Secrets Acts 1911 to 1989. The 1989 Act makes it unlawful for a member of the Security Service to make any unauthorised disclosure of information held by virtue of their work, or make any such disclosure purporting to be on such information or one intended to be take as such. It also includes the predecessor to the current Data Protection Act, namely the Data Protection Act 1984. The Code of Practice on Access to Government Information, Second Edition 1997, gives "information whose disclosure would harm national security" as a category of information that is exempt from the provisions of the Code.

5.3. The Government applies the policy to Security Service investigations and to suggestions of whether a particular individual or group is or has been under investigation. To ask whether the Security Service holds personal data on an individual often amounts to asking whether there is or has been an investigation.

5.4. By logical extension, the policy must apply even if no investigation has taken place. If the Security Service said when it did not hold information on a particular person, inevitably over time those on whom it did hold information would be able incrementally to deduce that fact. Not least because they would not receive the same assurance given to others.

5.5. If individuals intent on damaging national security could confirm that they were not subjects of interest to the Security Service, then they could undertake their activities with increased confidence and vigour. Another complexity would be the handling of cases where the Service had confirmed no interest in an individual or group but subsequently it took an interest. Would the Security Service be obliged to tell the earlier enquirer that the circumstances had changed? In any event, the response to repeat requests would reveal the change in circumstances. In either case, damage is done not only in the way described in section 4, but also the timing of the change would be helpful to those under investigation. For example, a terrorist may work out what he or she had done at that time to give themselves away. If so, they, and others they told, could avoid such actions in the future - ultimately, this would help them in carrying out their acts of terror.

5.6. Conversely, confirmation to individuals that they are subjects of interest may create or fuel suspicions that associates of theirs are assisting the Security Service. The consequences

of this could be harm to those who are in fact providing assistance, harm to those wrongly suspected of such assistance; and eventually in either case harm to the work of the Security Service in that the potential of personal harm to such persons would act as a strong deterrent to anyone assisting the Security Service, both in the investigation in question and in any other.

5.7. There are circumstances when the neither confirm nor deny policy is not used. Usually when it has been officially confirmed that the Security Service had undertaken an investigation, for example when a terrorist had been prosecuted, or when the interests of national security require a disclosure.

6. The safeguards and statutory controls that exist on the activities of the Security Service.

6.1. By their very nature, the Security Service's covert investigations are intrusive into the privacy of individuals. For this reason, there a number of constraints, oversight arrangements and safeguards placed on the Security Service. These include:

6.1.1. Legal constraints placed on the Security Service and its work, or its Director General, by Parliament through:

i. The Security Service Acts 1989 and 1996,

ii. the Intelligence Services Act 1994, and

iii. the Regulation of Investigatory Powers Act 2000. This law governs the interception of communications, the carrying out of surveillance and the use of "covert human intelligence sources", eg undercover officers or agents.

6.1.2. Oversight by the Home Secretary. This in turn includes :

i. regular meetings with the Director General;

ii. visits to Thames House to talk with staff there;

iii. advice from officials who are in daily contact with the Security Service;

iv. personal authorisation of warranted activity under the Regulation of Investigatory Powers Act 2000, and Intelligence Services Act 1994;

v. scrutiny of the Director-General's statutory Annual Report;

vi. scrutiny of the Security Service Annual Performance and Priority Report;

vii. calling for other reports where necessary;

viii. giving evidence to the Intelligence and Security Committee, considering their reports, and participating in Commons' debates on their reports;

ix. scrutiny of the reports of the independent Interception and Intelligence Services Commissioners who see everything relevant to their function.

6.1.3. Oversight by the Intelligence and Security Committee. This is an independent committee of members of both Houses of Parliament established under the Intelligence Services Act 1994. Its terms of reference are the same as most parliamentary departmental select committees. The Committee has its own Investigator who can look into and expand on the detail of evidence given to the Committee.

6.1.4. Oversight by the independent Intelligence Services Commissioner. This role was created by the Regulation of Investigatory Powers Act 2000 and combines the previous roles of the Security Service Act Commissioner and the Intelligence Services Act Commissioner. The Commissioner must hold or have held a high judicial office. As stated above, the Commissioner sees all information relevant to his or her functions.

6.1.5. Oversight by the independent Interception Commissioner. The Regulation of Investigatory Powers Act 2000 created this role although there had been a previous Commissioner under the Interception of Communications Act 1985. The Commissioner must hold or have held a high judicial office. He or she too sees all information relevant to his or her functions.

6.1.6. The Security Service's performance, plans and priorities are subject to external scrutiny by a senior Whitehall Committee known as JIC (the Joint Intelligence Committee). The resultant report is subject to approval by senior Ministers.

6.1.7. Oversight, in financial matters, by the National Audit Office.

6.1.8. Significantly in the context of data protection, the Security Service Act 1989 places duties on the Security Service's Director General concerning the obtaining and disclosure of information. The Director General must "ensure that arrangements are in place for securing that no information is obtained by the Service except so far as

necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of preventing or detecting serious crime".

6.1.9. The Regulation of Investigatory Powers Act 2000 also set up the Investigatory Powers Tribunal. This is described below.

7. Non-Data-Protection-Act Remedies

7.1. Anyone who feels aggrieved by anything which he or she believes the Security Service has done in relation to them or their property may complain to the independent Investigatory Powers Tribunal. The Tribunal will also hear claims relating to the Security Service under the Human Rights Act. Created under the Regulation of Investigatory Powers Act 2000, the Tribunal replaces the earlier Security Service Tribunal. Members of the Tribunal must qualify as lawyers. A duty to co-operate with the Tribunal is placed on everyone holding office under the Crown – this includes all members of the Security Service. There is no bar to what Tribunal members can see when looking into a complaint. If the Tribunal upholds the complaint, it can award compensation or make any other order that it sees fit. The address of the Tribunal is: PO Box 33220, LONDON SW1H 9ZQ.

8. The test that should be used to balance the need to safeguard national security and purposes of the Data Protection Act 1998.

8.1. The DPA section 28 states "personal data are exempt ... if the exemption ... is required for the purpose for safeguarding national security". However, the term national security is not defined. Both domestic and European courts have accepted that the Government has significant discretion in what constitutes national security. In addition, when considering safeguarding national security the courts have accepted [1] that it is proper to take a precautionary approach. That is, it is not necessary only to consider circumstances where actual harm has or will occur to national security, but also to consider preventing harm occurring and avoiding the risk of harm occurring.

8.2. Even so, the Home Secretary has balanced the need to safeguard national security against the purposes and entitlements conferred by the DPA. The risk to national security through the compromise of the work of the Security Service has been covered above. This was balanced against the factors below:

---

[1] The House of Lord's Judgement of 11 October in the appeal of Shafiq Ur Rehman against deportation, Secretary of State for the Home Department (11 October 2001 [2001] UKHL47).

i. the consequences of an individual not knowing whether the Security Service processes personal data on them arising from a covert investigation;

ii. if processed, an individual not knowing the purpose why it is processed;

iii. if processed, an individual not knowing whether the data is accurate;

iv. if processed, to whom the data may be disclosed;

v. the consequences of, for practical purposes, denying an individual of the opportunity to challenge the purpose for processing, the accuracy of data and opportunity to challenge to whom the data may be disclosed;

vi. the consequences to national security of the individual not correcting inaccurate personal data on him or her; and

vii. the consequences of the Information Commissioner or the courts not having a role in examining the use of the national security exemption in regard to DPA provisions.

8.3. In weighing the above factors, the Home Secretary took account of legal constraints and controls placed on the Security Service, the lack of Security Service executive powers and that their investigations in all but rare cases are kept secret.

9. The form and scope of the certificate.

9.1. The certificate has taken account of the determination of the National Security Panel of the Information in the appeal by Norman Baker MP against the previous certificate signed on behalf of the Security Service.

9.2. As expressly permitted by the DPA, the certificate identifies personal data by general description and it covers personal data processed after the date the certificate came into effect. A general description certificate reflects the primary function of the Security Service, set out in law, to protect national security. Otherwise, an individual certificate would be required for every appeal against the Security Service's use of the national security exemption. It should be noted that in the vast majority of cases the Service will need to use the exemption to preserve the neither confirm nor deny policy or to limit the extent of disclosure. The administrative burden of ad hoc certificates, taken together with

the fact that only Cabinet Ministers may sign such certificates, were also factors taken into consideration for the form and scope of the certificate.

9.3. The terms of the certificate were drafted to reflect the functions of the Security Service and the terms of the Data Protection Act 1998. A proportionate approach was adopted; careful consideration was given to the range of exemptions truly required in respect of each of the different categories of personal data, so that only the necessary exemptions were certified in respect of each category.

9.4. In particular, in line with the comments of the Tribunal, the neither confirm nor deny principle is preserved, subject to some exceptions. For example, it is not to possible to sustain the principle in respect to former employees of the Security Service. Even so, it may still be necessary, to safeguard national security, to withhold information about personal data that may have been processed.

9.5. The Home Secretary was aware that the personal data covered by the certificate might have been, or might be being, processed by the Security Service in the exercise of its function to support law enforcement agencies in the prevention and detection of serious crime. However, again in line with the policy of successive governments, the Home Secretary took the view that the complete separation of the national security and serious crime functions of the Security Service was impossible. The work of the Security Service in respect of any individual may often be carried out simultaneously under both of these functions.

9.6. The methodology, operating techniques, and resources of the Security Service are common to all three of its functions. It would be impossible to maintain a "neither confirm nor deny" approach to personal data processed under the Security Service's national security function if that approach were not adopted to personal data obtained under the serious crime function. Carefully directed or persistent enquiries made by an individual in respect of the serious crime function of the Security Service would lead to a grave risk of revealing whether the Security Service processed data in respect of that individual under its national security function. Therefore, the Home Secretary considered that exemption of all such personal data was required for the purpose of safeguarding national security. The same reasoning of course applies to the Security Service's other function of safeguarding the economic well-being of the country.

9.7. The certificate gives notice of the checks, procedures and reporting obligations placed on the Security Service as condition of their use of the certificate. These obligations are linked for the first time to the certificate in light of the Tribunal's determination mentioned in paragraph 9.1 above. The obligations ensure that while its terms are widely drawn that the Security Service will only use the national security exemption when necessary.

10. The checks, procedures and reporting obligations placed on the Security Service as condition of their use of the certificate.

10.1. The checks, procedures and reporting obligations on the Security Service are set out in the certificate, document reference **DPA/S28/TSS/2.** The Home Secretary also considered the Security Service arrangements for dealing with DPA subject access requests as set out in their internal protocol document.

10.2. In summary, the obligations require the Security Service to examine each subject access application and, for the purposes of safeguarding national security,:

i. decide the whether the use of the neither confirm nor deny approach is necessary,

ii. otherwise decide to what extent the national security exemption is still necessary; and

iii. to report back to the Home Secretary on the working of these arrangements.

11. Other points on the Security Service's need for use of exemptions under the Data Protection Act 1998.

11.1. When signing the certificate, the Home Secretary noted that other DPA exemptions might well also apply to the personal data covered by the certificate.

11.2. In addition, the signing of this certificate did not exclude the possible necessity of signing other national security certificates relating to personal data processed by the Security Service.

12. Conclusion

12.1. Having considered the factors above and given his knowledge of the secret work of the Security Service, the Home Secretary decided it was right for him to sign the certificate as requested by the Security Service.