

SECTION 28 DATA PROTECTION ACT 1998

CERTIFICATE OF THE FOREIGN SECRETARY AND THE HOME SECRETARY

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 2, 3 and 5; and
 - (c) section 55 of the Actif the exemption from that provision is required for the purpose of safeguarding national security;
- (ii) by subsection (2) of section 28 it is provided that a certificate signed by a Minister of the Crown certifying that the exemption mentioned in subsection (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 (3) of section 28 it is provided that a certificate under subsection (2) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect,
- (iv) data are processed by the ISC Secretariat on behalf of the Intelligence and Security Committee

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 a document dated *22 March 2002*, in summary that

1. The work of the Intelligence and Security Committee requires secrecy,
2. It is important to maintain the principle of neither confirming nor denying whether the Intelligence and Security Committee processes data about an individual
3. in dealing with subject access requests under the Act the ISC Secretariat will examine each individual case to determine :-

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

Now, therefore, we, Jack Straw and David Blunkett, in exercise of the powers conferred by the said section 28(2) do certify as follows :

personal data that are processed for the purpose of performing the Intelligence and Security Committee's functions under the Intelligence Services Act 1994 by the Intelligence and Security Committee or by the ISC Secretariat on behalf of the Intelligence and Security Committee are and shall continue to be required to be exempt from sections 7, 10, 14, 16(1)(c) and (e), 17, 21, 22, 24, 55, Part 5, the 6th data protection principle (to the extent necessary to be consistent with the exemptions contained in this certificate) and the 8th data protection principle,

for the purposes of safeguarding national security, provided that :-

- (a) no data shall be exempt from the provisions of section 7(1)(a) of the Act if the ISC Secretariat, after examining any request by a data subject for access to relevant personal data, determines that adherence to the principle of neither confirming nor denying whether data are held about an individual is not required for the purpose of safeguarding national security;
- (b) no data shall be exempt from the provisions of section 7(1)(b)(c) or (d) of the Act if the ISC Secretariat, after examining 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.

This certificate gives notice that we require the Clerk to the Intelligence and Security Committee, who heads the ISC Secretariat, to report to us on the operation of this certificate.

David Blunkett

.....

dated the 22. day of March 2002

The Right Hon. David Blunkett, MP

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

Jack Straw

.....

dated the 26 day of March 2002

The Right Hon. Jack Straw MP

REASONS FOR THE FOREIGN SECRETARY AND THE HOME SECRETARY SIGNING THE DATA PROTECTION ACT 1998 s28 (NATIONAL SECURITY) EXEMPTION CERTIFICATE COVERING PERSONAL DATA PROCESSED BY THE INTELLIGENCE AND SECURITY COMMITTEE AND ITS SECRETARIAT

1. Introduction

- 1.1 A section 28 certificate was signed by the Foreign Secretary and the Home Secretary for the Intelligence and Security Committee. This document explains the reasons they did so.
- 1.2 Before signing the certificate the Ministers considered the following factors:
 - the DPA, its national security exemptions and the role of the National Security Panel of the Information Tribunal;
 - the functions of the Intelligence and Security Committee in relation to the safeguarding of national security;
 - why secrecy is essential in the work of the Intelligence and Security Committee and the damage or potential damage that can be done to national security if compromised;
 - the need and use of the “neither confirm nor deny” policy by the Government;
 - the test that should be used to balance the need to safeguard national security and the purposes of the DPA;
 - the form and scope of the certificate;
 - the checks, procedures and reporting obligations placed on the Intelligence and Security Committee as conditions of their use of the certificate; and
 - other points on the Intelligence and Security Committee’s need for use of exemptions under the DPA.

These factors are explained below.

- 1.3 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. A subject access request will, almost inevitably, be the first step for anyone concerned by the possibility of the Intelligence and Security Committee processing personal data on them. The Intelligence and Security Committee is seen to be a data controller, with the Secretariat under the Clerk of the Committee as the data processor.

2. The DPA, its national security exemptions and the role of the National Security Panel of the Information Tribunal (“Tribunal”)

- 2.1 The 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 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 the 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. This 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 themselves 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 therefore provides a number of exemptions. One, at section 28 of the DPA, 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 Section 28 of the DPA also provides that a Minister of the Cabinet or the Attorney General or the Advocate General 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 the certificate or its coverage to 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 that the Minister did not have reasonable grounds for issuing the certificate or the actions in issuing the certificate were inappropriate for the purpose the Tribunal may quash the certificate.

3. The functions of the Intelligence and Security Committee and in relation to the safeguarding of national security

- 3.1 The Intelligence and Security Committee is a statutory body of nine parliamentarians established by the Intelligence Services Act 1994. The Committee examines the expenditure, administration and policy of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ). The Committee is required to report at least annually to the Prime Minister, although it can submit reports to him at any time. The Prime Minister is required to lay before each House of Parliament a copy of the annual report. However, after consultation with the Committee, the Prime Minister may exclude any matter in a report that would be prejudicial to the continuing discharge of the functions of the three

Intelligence and Security Agencies. The Committee is supported by a small secretariat, headed by the Clerk to the Committee, in discharging its functions.

- 3.2 In the preparation of its reports to the Prime Minister, and as part of its work under the Intelligence Services Act 1994, the Committee takes evidence and briefings from the three intelligence and security agencies, the Ministry of Defence (the Defence Intelligence Staff in particular), the Joint Intelligence Organisation of the Cabinet Office and a number of Law Enforcement Organisations.
- 3.3 Like the intelligence and security agencies, the Intelligence and Security Committee maintains its own liaison with analogous organisations in Allied countries. Such liaison arrangements allow access to information and analysis on intelligence, security and oversight matters. The Committee regards it as important to be able to have constructive discussions with Countries to enable proper and robust systems of legislature based oversight to exist for intelligence and security organisations.
- 3.4 The Committee does not investigate individuals.

4. Why secrecy is essential in the Intelligence and Security Committee and the damage or potential damage that can be done to national security when secrecy is comprised

- 4.1 It is fundamental to the integrity of intelligence and security related material information from whatever source that the information is kept in confidence and not disclosed outside the intelligence and security community. The inappropriate disclosure of such information could cause harm or distress and result in putting the continued supply from one or other of the sources at risk.
- 4.2 Where personal data features as part of the information that is used to reach a decision, whether a collective decision or otherwise, relating to national security it is essential that the decision-making process can take place without the fear of the information being disclosed in an unauthorised and inappropriate manner. The same applies to such information recorded or stored for whatever other purpose.
- 4.3 Depending on the nature and source of the personal data involved the disclosure of such information could lead to varying degrees of damage, up to and including exceptional damage, to the continuing effectiveness or security of security or intelligence operations. The same could also apply to the operational effectiveness or security of United Kingdom or allied forces.

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 or such matters in general. The policy, put simply, is a way to preserve the secrecy 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 Official Secrets Acts 1911 to 1989. The 1989 Act makes it unlawful for any member of the Intelligence and Security Committee or of the ISC Secretariat to make any unauthorised disclosure of information held by virtue of their work. It also includes the predecessor to the DPA, 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.

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

6.1 Section 28 of the DPA states that "Personal data are exempt ... if the exemption ... is required for the purpose of safeguarding national security". The term "national security", however, 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 (see the House of Lords' Judgement of 11 October 2001 in the appeal of Shafiq Ur Rehman against deportation) 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.

6.2 Even so the Foreign Secretary and the Home Secretary have balanced the need to safeguard national security against the purposes and entitlements conferred by the DPA. This was balanced against the following factors:

- the consequences of an individual not knowing whether the Intelligence and Security Committee processes personal data on them provided in the course of the Committee's work;
- if processed, an individual not knowing the purpose why it is processed, whether the data is accurate and to whom the data may be disclosed;
- the consequences of, for practical purposes, denying an individual the opportunity to challenge the purpose for processing, the accuracy of the data and to whom the data may be disclosed;
- the consequences to national security of the individual not correcting inaccurate data on him or her; and
- the consequences of the Information Commissioner or the courts not having a role in examining the use of the national security exemption in the regard to the provisions of the DPA.

7. The form and scope of the certificate

- 7.1 As expressly permitted by the DPA, the certificate identifies personal data by general description and it covers personal data processed after the date that the certificate came into effect. A general description certificate reflects the primary need for secrecy in the Intelligence and Security Committee to protect national security. Without this an individual certificate would be required for every appeal against the Intelligence and Security Committee's use of the national security exemption. In many instances the Intelligence and Security Committee 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 individual certificates, and the fact that only members of the Cabinet or the Attorney General or the Advocate General may sign such certificates, were also factors taken into consideration in the form and scope of the certificate.
- 7.2 The terms of the certificate were drafted to reflect the functions of the Intelligence and Security Committee and the terms of the DPA. A proportionate approach was adopted with careful consideration being given to the range of exemptions required in respect of each of the different categories so that only those that were absolutely necessary would be included.
- 7.3 To further ensure that as much personal data as possible is disclosed the Foreign Secretary and the Home Secretary require the ISC Secretariat to give due consideration to the:
- age of a document;
 - continued validity of any protective marking assigned to the document;
 - source of the personal data; and
 - context in which the personal data is given.

8. The checks, procedures and reporting obligations on the Intelligence and Security Committee as conditions of their use of the certificate

- 8.1 The Foreign Secretary and the Home Secretary before signing the certificate considered the Intelligence and Security Committee's handling arrangements for dealing with subject access requests made under the DPA.
- 8.2 In summary the ISC Secretariat is required to examine each subject access application and to:
- decide whether the use of the neither confirm nor deny approach is necessary;
 - decide, if not, to what extent the national security exemption is necessary;

The Clerk to the Committee is required to report back to the Foreign Secretary and the Home Secretary on the working of these arrangements.

8.3 The neither confirm nor deny approach will only be used where there is a particular and identified need to do so and there are no other alternatives. It is also relevant that there could be occasions when disclosure is required.

9. Other points on the Intelligence and Security Committee's need for use of exemptions under the DPA

9.1 When signing the certificate the Ministers noted that other exemptions under the DPA might well also apply to the personal data covered by the certificate.

9.2 It was further recognised that the signing of the certificate did not exclude the possible necessity of signing other national security certificates relating to personal data processed by the Intelligence and Security Committee.

10. Conclusion

10.1 Having considered the above factors the Foreign Secretary and the Home Secretary decided it was right to sign the certificate on behalf of the Intelligence and Security Committee.

Dated 22 day of March 2002