Home Office

The Data Protection Act 2018

National Security Certificates

August 2020

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at HONSdataqueries@homeoffice.gov.uk.

Contents

Introduction

1. This guidance is intended to provide for a common approach for obtaining national security certificates under the Data Protection Act 2018. It is intended to assist controllers considering whether to apply for a national security certificate under the Data Protection Act. This guidance is not legally binding and nothing in this guidance is intended to restrict the discretion of a Minister of the Crown[1].

[1] As set out in s205 of the Data Protection Act 2018, “Minister of the Crown” has the same meaning as in the Ministers of the Crown Act 1975, however, the ability to issue a national security certificate under the Act is limited to a Minister who is a member of the Cabinet or The Attorney General or the Advocate General for Scotland.

National Security and Data Protection Act

1. On 25th May 2018, new data protection legislation came into force, replacing the Data Protection Act 1998. The new legislation consists of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). The new legislation contains three distinct regimes for (1) general processing[2], (2) law enforcement; and (3) processing by the intelligence services. Each regime includes its own provisions which may be applicable when processing personal data for national security purposes. The approach taken to national security in the Act closely reflects the previous provisions for national security provided at s.28 of the Data Protection Act 1998. A table of the relevant sections of the Data Protection Act 2018 can be found at **Annex A**.

2. There are two key things for data controllers to consider when processing personal data for national security purposes:

    a. Whether it is necessary to exempt from provisions of the data protection legislation on grounds of national security?

    b. Whether it is appropriate to apply to a Minister of the Crown for a national security certificate to be issued?

3. It is important to note from the outset that a certificate is not required in order to rely on the national security exemption; in fact, in most cases, controllers will determine for themselves whether the national security exemption is applicable. For example, if a controller is processing data for national security purposes and receives a subject access request, they may feel content to apply the national security exemption (for example, preventing disclosure of information to a data subject by providing an NCND response) in the absence of a certificate, as it could be clear that national security is engaged.

4. National security certificates are meant to give a controller greater legal certainty that national security is applicable for specified data processing (para.11 below sets out the factors that may be relevant when deciding whether to apply for a certificate). This is because certificates certify that an exemption is required in respect of specified personal data that is processed for the purpose of safeguarding national security. A certificate signed by a Minister of the Crown, certifying that limitations to data subject

[2] The Data Protection Act 2018 does not include a national security exemption from the General Data Protection Regulation (GDPR). This is because the GDPR is European legislation and national security is out of scope of European law. When data is processed under GDPR and exemptions on the basis of national security are required, the processing is no longer in scope of GDPR and the 'applied GDPR' is applicable. When national security is relevant for general processing, reference should be made to sections 26 and 27 of the Data Protection Act 2018.

rights is required to safeguard/protect national security, will be conclusive evidence of the fact that national security is applicable.

5. National security certificates may apply to personal data which can be specifically identified or cover a broader category of personal data. They may be pre-emptive as well as retrospective.

National Security Certificates issued under the DPA 1998

6. The transitional provisions[3] make a clear distinction between processing of personal data under the Data Protection Act 1998 and the processing of personal data under the Data Protection Act 2018.

7. A National security certificate issued under the Data Protection Act 1998 ('old certificate') had an extended effect for the processing of personal data under the Data Protection Act 2018 until 25th May 2019[4]. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the 2018 Act for processing done under that Act. Controllers that previously relied on a certificate issued under the Data Protection Act 1998 should consider whether they will need to rely upon a certificate to protect personal data processed under the Data Protection Act 2018. If so, they should apply to the relevant Minister for a certificate issued under the Data Protection Act 2018.

8. Where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, it will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed[5]. The protection provided by these 'old certificates' is limited to the processing of personal data under the Data Protection Act 1998. New national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998[6].

.

[3] This is provided at Part 5 of Schedule 20 to the DPA 2018 for National Security Certificates

[4] This is provided at paragraph 18(5) of Schedule 20 to the DPA 2018

[5] This is provided at paragraph 17(3) of Schedule 20 to the DPA 2018

[6] This is provided at paragraph 17(1) of Schedule 20 to the DPA 2018

Applying for a National Security Certificate

Is a National Security Certificate Appropriate?

9. The controller should assess whether the processing undertaken requires exemption from provisions of the data protection legislation, such as limitations on the data subject's rights, in order to safeguard/protect national security. Any limitations must be proportionate and necessary.

10. Once the controller has determined that the national security exemption is applicable, they should consider whether a certificate would be beneficial. While this will depend on the specific data processing taking place or being proposed, the controller should consider the following factors:

    - the volume of data;
    - frequency of data;
    - specific complexities that would benefit from the additional clarity a certificate may provide

    Retrospective certificates may also be sought if it is determined that a certificate would be beneficial in circumstances where the processing of personal data has already taken place. As already set out at para 4 above, it is not necessary to have a national security certificate in place to rely on the national security provisions, so the absence of a certificate should not attract criticism.

11. Before making an application for a certificate, controllers should consider consulting their Data Protection Officer (where applicable), legal advisors, and the relevant Government department that will receive the request. The Data Protection Policy team in the Home Office should also be consulted (details provided at paragraph 29 of this note) to ensure the approach taken is consistent with other certificates which have been issued.

Requesting the Certificate

12. The controller should submit a formal application addressed to the relevant Minister of the Crown that clearly justifies why exemption from data protection provisions is required for the purposes of safeguarding national security and why it is considered that a national security certificate is required. In circumstances in which the certificate

is aimed at capturing a set of incoming data, the request for the certificate may be made by the recipient controller.

13. The request should include details of the data protection regime(s) the certificate should apply to if authorised; the duration of the certificate; the reasons why exemption from data protection provisions is required for the purposes of safeguarding national security; and an explanation as to why a national security certificate is considered necessary. The controller should consider the rationale for exempting each data protection provision under a certificate. Where applicable, the certificate may apply to more than one regime (i.e. Parts 2, 3 and 4 of the Data Protection Act), for example where a controller is processing data for national security purposes under both Parts 2 and 3 of the Act.

14. A draft certificate should be included for the Minister's consideration (see example at **Annex B**). The certificate should be drafted at the OFFICIAL classification. In exceptional circumstances, where this is not possible, this should be clearly stated and explained to enable the Minister to determine whether publication of the text of the certificate (in full or in part) is not possible (see para 21 below for more information).

Duration of Certificate

15. It is recommended that certificates should be for a fixed duration of no more than five years from the date of signature to ensure they are regularly reviewed by the Executive. The controller applying for the certificate should make clear how long they consider it should last for. When the certificate is intended to apply retrospectively, it may capture any period prior to the date of signature.

16. A certificate may be renewed or revoked at any time by a Minister of the Crown. The expiry of a certificate does not preclude the controller from relying on the national security provisions, however an expired certificate cannot be relied on as conclusive evidence of national security.

Contents of the Certificate

17. An example skeleton of a certificate can be found at **Annex B**. When submitting a draft certificate for approval and signature, it should include:

    a. The applicable data protection regime governing the processing under which the certificate will be issued;

    b. details of the processing which the certificate applies to; where appropriate by describing broad categories of types of processing;

    c. details of the processing which the certificate applies to; where appropriate by describing broad categories of types of processing;

d. whether the certificate is retrospective; and

e. an expiry date of no more than five years in future.

Approval and publication of the Certificate

18. If the Minister considers the application and is satisfied that exemption from data protection provisions is required for the purposes of safeguarding national security, then they can take the decision to issue a certificate and should sign the certificate provided to them.

19. A signed version of the certificate should be returned to the controller with a copy sent to the Information Commissioner for their records. The Commissioner is required to keep a public record of the certificate[7], which must include the name of the Minister who issued the certificate, the date on which the certificate was issued and in most circumstances the text of the certificate. There is a presumption in favour of publication of a certificate in full. Where the Minister of the Crown determines that publication of the text of the certificate (in full or in part) is not possible for one of the grounds provided for in the Act[8], publication of the text of the certificate may be restricted. As a result, applicants for a certificate should clearly set out whether they are content for the text of the certificate to be published, and if they are not content, they should provide clear reasoning in their application. In such circumstances, the Minister will be required to consider and agree to any publication restriction and the Commissioner should be notified of any restrictions on publication.

20. A copy of a signed certificate at a government security classification level of **OFFICIAL SENSITIVE**, should be submitted to the ICO at the following email address: nationalsecuritycertificates@ico.org.uk. Certificates at a government security classification level of **SECRET** or above should be delivered to the Information Commissioner in **hard copy only**, arranged via established ICO contact channels. A Ministerial notification setting out any restrictions to the publication of a certificate should also be delivered in **hard copy only** on the assumption that the restricted material will be SECRET or above.

[7] S130(3) of the Data Protection Act 2018

[8] S130(4) provides that publication of the text may be restricted if publication would be against the interests of national security, would be contrary to the public interest or might jeopardise the safety of any person.

Amendment, renewal and revocation of a National Security Certificate

21. A national security certificate may be renewed or revoked by a Minister of the Crown at any time. Data controllers should notify the Minister when they want to renew a certificate, following the same process outlined above, providing an updated version of the certificate. Controllers should notify the Minister if they become aware that the certificate is no longer needed or appropriate, so the Minister can revoke it.

22. Where it is necessary to amend a national security certificate, the appropriate way to do this is to make an application for a renewal, enclosing a copy of the amended certificate and making clear why any changes are required.

23. Where a Minister of the Crown revokes a certificate, they must notify the Information Commissioner to ensure the record of certificates published by the Commissioner remains accurate.[9] Similarly, when a Minister issues a new certificate as a result of an application for renewal or amendment of an existing certificate, the Commissioner should be provided with the 'new' updated certificate as outlined in para. 20 above.

[9] S130(6) of the Data Protection Act 2018

Challenges to National Security Certificates

24. Applicants seeking certificates and Ministers approving them should be aware that any person directly affected by the issuing of a certificate may appeal the decision to issue the certificate or, where in proceedings under the applied GDPR or Data protection Act 2018, a controller claims that a certificate applies to certain personal data, any other party to the proceedings may appeal the certificate on the basis that the certificate does not apply to the personal data.

25. Appeals are to the Upper Tribunal and judicial review principles will be applied when determining the appeal. In applying such principles, the Upper Tribunal can consider a wide range of issues, including necessity, proportionality and lawfulness. This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security. If the Tribunal allows the appeal, concluding that there were not reasonable grounds for issuing the certificate, they can quash the certificate. Where a certificate provides a general description of the personal data to which it applies, the Tribunal may determine that the certificate does not apply to specific personal data which is the subject of the appeal.

26. As a result, applicants should carefully consider the possible risks of legal challenge against a certificate when making any application.

Further information on National Security Certificates

27. If you have any further questions about applying for a national security certificate, you should consult your Data Protection Officer (where applicable) and/or your legal advisor.

28. If you require further information on this guidance, you should contact the Home Office Data Protection Policy Team: HONSdataqueries@homeoffice.gov.uk

Annex A

Data Protection Act 2018: Table of National Security Provisions

Regime	Section	Exemption/Restriction
Part 2 – Chapter 3 (applied GDPR)	s.26	National security exemption: General processing
	s.27	National security certificate: General processing
Part 3 (law enforcement processing)	s.44(4)	Restricts data subject's right to additional information for the purpose of exercising rights.
	s.45(4)	Restriction on Subject Access Rights
	s.48(3)	Restricts the need to inform the data subject of the reasons for refusing to rectify or erase data.
	s.68(7)	Restricts the need to inform the data subject without delay of a data breach
	s.79	National security certificate: Law enforcement
Part 4 (intelligence services processing)	s.110	National security Exemption: Intelligence Services
	s.111	National security certificate: Intelligence Services

Annex B

National Security Certificate example

The certificate should be drafted at the OFFICIAL classification. In exceptional circumstances, where this is not possible, this should be clearly stated to prevent publication and the Minister should be made aware of the reasons why the certificate cannot be published.

Certificate reference:- DPA/XXX

SECTION X [*27/79/111*] DATA PROTECTION ACT 2018

CERTIFICATE OF THE SECRETARY OF STATE

---

1. **Whereas:**

    a. by section/subsection X of the Data Protection Act 2018 ("the Act ") it is provided that the processing of personal data is exempt from certain provisions of the Act if the exemption from that provision is required for the purpose of safeguarding national security. For information, a full list of these provisions is provided at Annex A.

    b. by subsection X [*27(1)/79(3)/111(1)*] it is provided that a certificate signed by a Minister of the Crown, certifying that the exemption from all or any of the provisions referred to above at paragraph X, 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;

    c. by subsection X [*27(2)/79(4)/111(2)*], it is provided that a certificate under subsection X [*27(1)/79(1)/111(1)*] 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 hereinafter identified were not available.

3. **And for the reasons** set out below:

    3.1 *[set out a summary of the key reasons for seeking the certificate]*

4. **Now, therefore**, I, the Right Hon XX, being a Minister of the Crown who is a member of the Cabinet, in exercise of the powers conferred by section XX do issue this certificate and certify as follows:-

    a. That any personal data that are processed by X *[name of data controller/applicant]* as described in Column 1 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;
    b. That any personal data that are processed by any other person or body ("third party"), as described in Column 1 in the table below, are and shall continue to be exempt in the circumstances specified below from the provisions of the Act set out in Column 2 below. *[NOTE – this para may not be relevant for all applications, only where a controller is seeking to provide cover for third party as well]*

Column 1	**Column 2**
List any personal data/processing to which this certificate applies	*List the provisions from which exemption is sought – note, this should only be the provisions from which exemption is necessary – which may not be all of the provisions from which the Act enable exemptions (i.e. there may be some provisions which can be complied with regardless of national security considerations)*

……..

[Insert name of Minister]

……

Dated

…….

Expires

Provision	**Notes**
List the provisions that can be exempt under the certificate [as specified under s.110(2)/s26(2)/Part3 restrictions	*What does the provision relate to; e.g. First data protection principle, duty to be fair and transparent*