Cabinet Office

HMG Security Policy Framework

Legal Guidance

VERSION HISTORY

SPF VERSION	DATE PUBLISHED	SUMMARY OF CHANGES
V1.0	Dec 08	N/A
V2.0	1 May 09	N/A
V3.0	Oct 09	N/A
V4.0	May 2010	Minor amendments, see attached Annex A for further details.
V5.0	Oct 10	Amendments to links within the document.
V6.0	May 2011	made minor amendments to the following paragraphs: 4.25- paragraph amended because webpage has moved and been updated. 5.2- paragraph amended to update web link 5.4 (k)-amendment added for clarity 5.5- web link updated
V7.0	Oct 11	Paragraph 4.22- updated web link Paragraph 4.25- updated web link and remove reference to “Andorra”. Paragraph 4.49- updated web link.

1. Introduction

1.1 This guidance is intended to be an introduction to the main areas of law within which the HMG Security Policy Framework operates. It is not intended to be an exhaustive survey of all law that may be of relevance to the Framework. Nor is it intended to be a substitute for expert legal advice on specific issues and problems that you may face.

2. Sources of Legal Advice and Guidance

2.1 The primary source of expert legal advice must remain your departmental or agency legal advisers. In addition, guidance on the Data Protection Act 1998 and the Freedom of Information Act 2000 is available on the Ministry of Justice website (www.justice.gov.uk) and the Information Commissioner's website (www.ico.gov.uk). Note that the views of the Information Commissioner do not necessarily reflect those of the government. Links to further guidance on specific issues covered by this guidance are given below.

3. The Official Secrets Act 1989 ("OSA")

3.1 Sections 1 to 6 and 8 of the OSA contain a number of offences concerning unauthorised disclosures of information, documents or articles. The term "official information" is not used in the OSA but is commonly used, and is used in this guidance, to mean information, documents or articles which are in the possession of Crown Servants (see paragraph 3.4 below) or government contractors (see paragraph 3.6 below) by virtue of their position as such.

Application of the OSA

3.2 The offences in the OSA are capable of being committed by a range of persons: members of the security and intelligence services; Crown servants; persons notified under section 1 of the OSA; and government contractors. Certain offences under the OSA may also be committed by members of the public.

3.3 **Members of the security and intelligence services** are specifically mentioned in section 1(1) of the OSA, which applies to both present and former members.

Members of the security and intelligence services also fall within the definition of Crown servants (see paragraph 3.4 below).

3.4 **Crown servants**: the term "Crown servant" is defined in section 12 of the OSA to include not just civil servants and members of the armed forces but also Ministers, including Ministers from the devolved administrations and the police. The term also includes members or employees of certain bodies and holders of certain offices that are prescribed in the Official Secrets Act 1989 (Prescription) Order 1990[1], including British Nuclear Fuels plc, the United Kingdom Atomic Energy Authority, the Nuclear Decommissioning Authority, the Comptroller and Auditor General, and the Parliamentary Commissioner for Administration. The OSA applies to both present and former Crown servants (as defined).

3.5 **Notification under section 1 of the OSA**: a person may be notified that he is subject to section 1(1) of the OSA if, in the opinion of a Minister of the Crown, the work undertaken by that person is or includes work connected with the security and intelligence services and its nature is such that the interests of national security require that he should be subject to section 1(1). Notification lasts for five years unless revoked and may be renewed for periods of five years at a time. A notification must be revoked if, in the Minister's opinion, the notified person's work ceases to be of the type described above. Departments and agencies are reminded of the requirement to ensure that notifications are renewed every five years, to keep under review the need for continuing notification of individual posts and to maintain and keep under review the number of notifiable posts. Notified persons who are not Crown servants or government contractors nonetheless fall within the definition of Crown servant for the purpose of section 8(1) and (2) of the OSA. The offence in section 1 OSA applies both to persons who are and to persons who have been notified.

3.6 **Government contractors**: section 12 of the OSA defines the term "government contractor" to include any person who is not a Crown servant but who provides, or is employed in the provision of, goods and services for the purposes of Ministers and other Crown servants as defined in section 12 (see paragraph 3.4 above). The OSA applies to present and former government contractors.

[1] S.I. 1990/200 as amended by S.I.2007/2148, S.I.2006/362,S.I.2004/1823, S.I.2003/1918, S.I.1999/1042 and S.I. 1993/847.

Protected Interests

3.7 The offences in the OSA cover unauthorised disclosures of official information which are damaging to specified interests or that result in certain consequences.

3.8 **Security or intelligence**: the term "security or intelligence" is defined in section 1(9) of the OSA to mean the work of, or in support of, the security and intelligence services or any part of them. References in the OSA to information relating to security or intelligence include references to information held or transmitted by the security and intelligence services or by persons in support of, or of any part of, them. The unauthorised disclosure of official information relating to security or intelligence is damaging if it damages, or would be likely to damage, the work of the security and intelligence services. In the case of members of the security and intelligence services and persons notified under section 1, it is an offence simply to make an unauthorised disclosure of official information relating to security or intelligence: there is no requirement in section 1(1) that the disclosure be damaging.

3.9 **Defence**: the term "defence" is widely defined to include, among other things: the size, shape and organisation of the armed forces; the development, production and operation of weapons; defence policy and strategy; and military planning and intelligence. The unauthorised disclosure of official information relating to defence is damaging if, among other things: it damages the capabilities of the armed forces; it leads to loss of life or injury to members of the armed forces; it endangers the interests of the United Kingdom, or the safety of British citizens abroad; it seriously obstructs the promotion or protection by the United Kingdom of its interests abroad; or if it would be likely to have any of those effects.

3.10 **International Relations**: the term "international relations" includes relations between States, between international organisations and between States and international organisations. It also includes any matter relating to a foreign State or an international organisation which is capable of affecting the relations of the United Kingdom with a foreign State or international organisation. The unauthorised disclosure of official information relating to international relations is damaging if it endangers the interests of the United Kingdom, or the safety of British citizens abroad, seriously obstructs the promotion or protection by the United Kingdom of its interests abroad, or would be likely to have any of those effects.

3.11 **Foreign confidences**: the unauthorised disclosure of official information obtained in confidence from a foreign State or international organisation is damaging if it endangers the interests of the United Kingdom, or the safety of British citizens abroad, seriously obstructs the promotion or protection by the United Kingdom of its interests abroad, or would be likely to have any of those effects.

3.12 **Crime**: section 4 of the OSA covers the unauthorised disclosure of official information which, among other things, results in the commission of an offence, facilitates an escape from legal custody, impedes the prevention or detection of offences, or the apprehension or prosecution of suspected offenders or would be likely to have any of those effects.

3.13 **Special investigation powers**: section 4 of the OSA also covers the unauthorised disclosure of official information obtained by reason of ,or relating to, the interception of communications in obedience to a warrant issued under the Interception of Communications Act 1985 or the Regulation of Investigatory Powers Act 2000 or information obtained by reason of action authorised by a warrant under the Security Service Act 1989 or the Intelligence Services Act 1994.

4. The Data Protection Act 1998 ("DPA")

4.1 The DPA governs the processing of personal data, including the release of personal data, in the UK. It provides that **personal data** and **sensitive personal data** must be **processed** by **data controllers** in accordance with eight **data protection principles**. The DPA implements Directive 95/46/EC[2].

4.2 **Personal data** is data which relate to a living individual who can be identified from those data or from those data and other information which is in, or is likely to come into, the possession of the data controller. It includes expressions of opinion about the individual.

4.3 **Sensitive personal data** is personal data consisting of information relating to the data

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ No. L 281, 23.11.95, p. 31)

subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the commission of offences and criminal proceedings.

4.4 The term **'processing'** is given a very wide meaning in the DPA and includes, among other things, obtaining, recording, holding, carrying out operations on, adapting, retrieving, disclosing and destroying data.

4.5 A **data controller** is a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. Data controllers are under a duty to comply with the data protection principles.

4.6 The eight **data protection principles** are:

a. Personal data must be processed fairly **and** lawfully **and** shall not be processed unless at least one of the conditions in Schedule 2 to the DPA is met **or**, in the case of sensitive personal data, shall not be processed unless at least one of the conditions in Schedule 3 to the DPA is also met.

b. Personal data may be obtained only for specified lawful purposes and shall not be processed in a manner incompatible with those purposes.

c. Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed.

d. Personal data must be accurate and, where necessary, kept up to date.

e. Personal data must not be kept for longer than is needed for the purposes for which it is being processed.

f. Personal data must be processed in accordance with the rights of data subjects.

g. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

h. Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for personal data.

Exemptions

4.7 The DPA contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA such as the right of access to personal data (as to which, see below). The exemptions vary in their scope. For example, section 28 provides an exemption from the data protection principles, the provisions relating to the rights of data subjects, the provisions relating to the requirement of data controllers to notify the Information Commissioner, and the enforcement provisions if it is required for the purpose of safeguarding national security. A ministerial certificate stating that the exemption applies is conclusive evidence of that fact. In contrast, section 31 (regulatory activity) provides an exemption from the subject information provisions (aspects of the requirement of fair and lawful processing in the first data protection principle and section 7) if compliance with those provisions would prejudice specified regulatory activity. Other exemptions include:

a. Crime and taxation (section 29).

b. Health, education and social work (section 30).

c. Research, history and statistics (section 33).

d. Disclosures required by law or made in connection with legal proceedings (section 35).

e. Parliamentary privilege (section 35A).

Rights of data subjects

4.9 The DPA gives certain rights to data subjects and the sixth data protection principle requires that personal data must be process in accordance with those rights. These include the right of access to personal data (section 7) and the right to prevent processing likely to cause damage or distress (section 10).

4.10 **Subject access requests**: section 7 of the DPA gives individuals the right to be

informed whether their personal data is being processed by a data controller and, if so, to be given a description of that personal data, the purposes for which it is being processed and third parties to whom that personal data may have been disclosed. Individuals also have the right to be provided with their personal data that the data controller is processing and information as to the source of that data. Subject access requests must be in writing. Where complying with a subject access request would mean disclosing the personal data of another person, the data controller is not obliged to comply with the request unless either the other person consents or it is reasonable in all the circumstances to comply without the consent of the other person. The statutory time limit for complying with a subject access request is 40 days.

4.11 **Damaging or distressing processing**: data subjects have the right under section 10 of the DPA to give notice to a data controller requiring the data controller to cease processing their personal data on the ground that it is causing the data subject or another substantial damage or substantial distress and that the damage or distress is unwarranted. The time limit for complying with a section 10 notice is 21 days. The requirement to cease processing does not arise in certain circumstances. For example, where the data subject has consented to its processing; where processing is necessary for contractual performance or compliance with legal obligations; or the processing is necessary in order to protect the vital interests of the data subject.

Data Security

4.12 The seventh data protection principle (see paragraph 4.6.g) includes a number of specific obligations relating to data security. Measures taken under the seventh data protection principle must ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the data, and to the nature of the data to be protected. In addition, the data controller must take reasonable steps to ensure the reliability of any employees who have access to the personal data.

4.13 Where processing is to be carried out by a data processor on behalf of a data controller, the data controller must choose a data processor providing sufficient guarantees in respect of technical and organisational measures governing the processing and must take reasonable steps to ensure compliance with those measures. Furthermore, processing by a data processor must be carried out under a contract in writing under which the data processor is to act only on instructions from

the data controller, and the contract must require the data processor to comply the obligations in the seventh data protection principle.

4.14 In addition, government departments and agencies are required to comply with mandatory minimum measures and civil servants dealing with personal data are to undergo annual mandatory training.

4.15 For further information, see Information Assurance Standard No. 6 – Protecting Personal Data and Managing Information Risk (MR 2).

Data Sharing

4.16 Under the DPA, each government department is a separate data controller. As such, the sharing of personal data between government departments, as well as between departments and public or private sector organisations, must comply with the DPA. Departments, whether the senders or recipients of shared personal data, must also ensure that the sharing is within their public law powers, that it does not breach any restrictions on disclosure and that it complies with the Human Rights Act 1998, Article 8 of the European Convention on Human Rights ("ECHR") and the law of confidence.

4.17 **Public law powers** include both express and implied statutory powers as well as those prerogative and common law powers that are available to Ministerial departments.

4.18 **Restrictions on disclosure** may come from express or implied statutory provisions. In addition, there may be further particular restrictions in place, for example court orders prohibiting disclosure.

4.19 Under **Article 8** of the ECHR everyone has the right to respect for his private and family life, his home and his correspondence. Interference with Article 8 rights by a public authority are only justified if it is in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others. Data sharing is likely to engage Article 8, which is broad in its scope.

4.20 The **law of confidence** protects information from unauthorised disclosure if it has the

necessary quality of confidence and if it was received pursuant to an obligation to keep the information confidential. (Confidential in this context is not to be confused with the protective marking CONFIDENTIAL.) There are public interest defences to a breach of confidence. Taken with Article 8 of the ECHR, the law of confidence also protects private information from misuse: see for example the cases of Naomi Campbell v Mirror Group Newspapers[3] and Max Mosley v News Group Newspapers[4].

4.21 Data security (as to which, see above 4.12) is of key importance in the context of data sharing.

4.22 For further information on data sharing, see Public Sector Data Sharing: Guidance on theLawhttp://www.justice.gov.uk

Data Transfer

4.23 The transfer of data between countries or territories engages the eighth data protection principle. The reference to territories is important: the Channel Islands, the Isle of Man and the UK's overseas territories are separate territories for the purpose of the DPA. Transfers may be either to a third country data processor (i.e. any person, other than an employee of the data controller, who processes data on behalf of a data controller) or to a third country data controller.

4.24 Transfers between countries or territories within the European Economic Area ("EEA") (the EU member States plus Norway, Iceland and Lichtenstein) are permitted. All countries within the EEA are required to have domestic legislation implementing Directive 95/46/EC. Note that the Channel Islands and the Isle of Man are **outside** the European Economic Area.

4.25 Countries and territories outside the European Economic Area may be assessed by the EU Commission as to whether their laws provide an adequate level of protection. Switzerland, Argentina, the Isle of Man, Canada, Jersey,Guernsey, Australia, Faeroe Islands and Israel have all been assessed as adequate and so transfers to them may take place. An up to date list can be found at :

http://ec.europa.eu/justice/data-protection/document/international-

[3] [2004] 2 AC 457, [2004] UKHL 22

[4] [2008] EWHC 1777 (QB)

transfers/adequacy/index_en.htm
b

4.26 Some countries, e.g. Canada and the USA, have developed particular schemes such as the US Safe Harbor Scheme. The Safe Harbor Scheme is a set of principles which are similar to those in the Data Protection Act 1998 and relate to transfer of data to certain US entities. Those countries are considered to provide an adequate level of protection so long as those schemes are applied to the transfer.

4.27 For all other countries and territories, an assessment of adequacy must be carried out by the data controller prior to transfer taking place. The general criteria for assessment of adequacy include the nature of the personal data, the purposes of the transfer, the period of the intended processing, any security measures in place in the receiving country, the country of origin of the personal data and the country of final destination. In addition, there are criteria for assessing legal adequacy that must be applied in all cases, although the degree of scrutiny will depend on the level of risk that the general assessment reveals. The legal adequacy criteria include the law in force in the receiving country, the international obligations applicable to the receiving country, whether there are any relevant codes of practice or enforceable rules in the receiving country and any security measures taken in the receiving country.

4.28 Finally, there are a number of derogations from the eighth data protection principle in Schedule 4 to the DPA including that the data subject has given his consent, or that the transfer is necessary for the performance of a contract between the data controller and the data subject or for reasons of substantial public interest. However, those derogations should only be used in exceptional circumstances and only if it is impossible to obtain adequacy.

4.29 For further information, see the Information Commissioner guidance on the eighth data protection principle and international data transfers http://www.ico.gov.uk

5. The Freedom of Information Act 2000 ("FOIA")

5.1 The FOIA grants two rights to a person making a request for information to a public authorities: to be informed by the public authority whether it holds the requested information (the duty to confirm or deny); and, if that is the case, to be supplied with the information. The bodies and offices that are public authorities for the purpose of

the FOIA are specified in the FOIA. They include all government departments, both Houses of Parliament, the Northern Ireland Assembly, the National Assembly of Wales, the armed forces, local authorities, the National Health Service, maintained schools and the police. The security and intelligence agencies are **not** public authorities for the purposes of the FOIA.

5.2 A step-by-step guide to dealing with requests for information under the FOIA can be found on the Ministry of Justice website (http://www.justice.gov.uk/guidance/foi-step-by-step.htm). The Ministry of Justice also publishes a set of working assumptions to assist central government officials in considering how to handle certain types of request, including Cabinet and Cabinet committee information, policy advice, parliamentary questions, legal advice, and confidential information received from foreign states of international organisations (http://www.justice.gov.uk/guidance/foi-working-assumptions.htm).

Exemptions

5.3 The FOIA provides for a range of exemptions under which public authorities may withhold the requested information (or neither confirm nor deny whether the information is held). A "neither confirm or deny response" may be required in circumstances where to confirm or deny the existence of information would in itself communicate sensitive and potentially damaging information to the detriment of the public good. A "neither confirm nor deny response" can be used in relation to any exemption except the exemption in section 21. These exemptions are either absolute or qualified. If an absolute exemption applies, the public authority may withhold the information. If a qualified exemption applies, the public authority is required to undertake the public interest test. It is required to balance the public interest in withholding the information against the public interest in disclosing the information. Only if the public interest balance is in favour of withholding the information may the public authority withhold. The decision to confirm or deny is separate from the decision not to disclose information and needs to be taken on its own terms. Exemptions most likely to apply to information covered by the Security Policy Framework are:

a) Information supplied by, or relating to, bodies dealing with security matters (section 23) (absolute). Section 23 bodies include the security and intelligence agencies, the special forces and the

Serious Organised Crime Agency.

b) National security (section 24) (qualified).

c) Defence (section 26) (qualified).

d) International relations (section 27) (qualified).

e) The economy (section 29) (qualified).

f) Investigations and proceedings conducted by public authorities (section 30) (qualified).

g) Law enforcement (section 31) (qualified).

h) Formulation of government policy, etc (section 35) (qualified).

i) Prejudice to effective conduct of public affairs (section 36) (qualified).

j) Health and safety (section 38) (qualified).

k) Personal information (section 40) (partly qualified and partly absolute).

l) Information provided in confidence (section 41) (absolute).

m) Commercial interests (section 43) (qualified).

n) Prohibitions on disclosure (section 44) (absolute).

5.5 Detailed guidance on the exemptions is published on the Ministry of Justice website (http://www.justice.gov.uk/guidance/foi-exemptions-guidance.htm).

Access to Environmental Information

5.6 Environmental information is exempt from the FOIA by virtue of section 39 of that Act.

Instead, the regime for access to environmental information is provided by the Environmental Information Regulations 2004[5] ("EIRs"), which implement Directive 2003/4/EC[6].

5.7 The EIRs apply to "public authorities" but the meaning of that term differs from that in the FOIA. Whilst there is a considerable degree of overlap - government departments are public authorities under both the FOIA and the EIRs - some bodies are public authorities under the EIRs but not under FOIA and others are public authorities under FOIA but not under the EIRs. For example, the special forces are expressly excluded from the scope of the FOIA but not from the EIRs.

5.8 The EIRs apply to "environmental information", which is broadly defined to include information on: the state of the elements of the environment; factors affecting or likely to affect the elements of the environment; measures designed to protect those elements; reports on the implementation of environmental legislation; cost-benefit and other economic analyses and assumptions; and the state of human health and safety.

5.9 The EIRs contain a range of exceptions which, whilst in different terms to those in the FOIA exemptions, cover similar ground. For example, a public authority may refuse to disclose information to the extent that the would adversely affect:

a) International relations, defence, national security or public safety (regulation 12(5)(a)).

b) The course of justice, the ability of a person to receive a fair trial or the ability of a public authority to conduct an inquiry into a criminal or disciplinary nature (regulation 12(5)(b)).

c) The confidentiality of the proceedings of a public authority where such confidentiality is provided by law (regulation 12(5)(d)).

d) The confidentiality of commercial or industrial information where

[5] S.I. 2004/3391

[6] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (OJ No. L 41, 14.2.2003, p. 26)

such confidentiality is provided by law to protect a legitimate economic interest (regulation 12(5)(e)).

5.10 Note that all of the exceptions set out above, and the other exceptions contained in regulation 12(4) and (5), are subject to the public interest test. Furthermore, there is no equivalent in the EIRs of the exemption for security bodies in section 23 of the FOIA.

5.11 Environmental information which is also personal data must be dealt with in accordance with regulations 5(3) and 13.

5.12 Detailed guidance on the EIRs, including on handling requests, is published on the Department for the Environment, Food and Rural Affairs website:

http://www.defra.gov.uk/corporate/policy/opengov/eir/guidance/full-guidance/index.htm

Annex A

VERSION HISTORY – SPF V.4.0

TITLE OF CHAPTER / SECTION	PARA REFERENCE	SUMMARY OF CHANGES
Legal Guidance	3.4	Amendment made for greater clarity
	3.4 footnote	Amendment added for completeness
	3.5	Amendment made for greater clarity
	3.6	Amendment made for greater clarity
	3.9	Stray comma removed
	3.11	Stray comma removed
	3.12	Amendment made for greater clarity
	3.13	Amendment made for greater clarity
	4.3	Words added for clarity
	4.4	Words added to make it clear that the list is not exhaustive
	4.6	Words added for clarification
	4.7	Words inserted for completeness.
	4.11	Amended for greater clarity
	4.12	Words added for completeness
	4.13	Amended for greater clarity
	4.16	Words added for completeness
	4.19	Words added for completeness
	4.25	List updated and internet link added
	4.26	Words added for completeness
	4.27	Words added for clarification
	4.29	Up to date link to webpage added
	5.1	Amendment made for greater clarity
	5.3	Amendment made for clarity
	5.9	Amendment made for greater clarity
	5.10	Amendment made for greater clarity
	5.12	Up dated web link