Ministry of Defence Access to Information

Guidance Note

Version 6 March 2009

Guidance Note B1: Access to information legislation

1. The **Freedom of Information Act 2000** came into force on 1 January 2005 a statutory right to request information held by public authorities and replaced those parts of the Public Records Act which related to access to records. It introduced the requirement for Publication Schemes and created the new role of Information Commissioner, with powers to supervise and enforce the Act. The non-statutory Code of Practice on Access to Government Information was superseded by the FOI Act.

2. The **Environmental Information Regulations 2004** came into force on 1 January 2005, replacing the previous Regulations (EIRs 1992, as amended 1998). The introduction of EIRs 2004 in England, Wales and Northern Ireland (and of similar Regulations in Scotland) enables the UK to comply with its commitments under the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental matters (the Aarhus Convention), and with EU Directive 2003/4/EC on public access to environmental information. Requests for environmental information must be considered under the EIRs 2004, not the FOI Act.

3. The **Data Protection Act 1998** created eight data protection principles and strengthened an individual's right to see data held on them by public bodies and the private sector. The definition of data includes both manual files and electronic records.

4. The **Official Secrets Act 1989** (OSA) applies to all MOD personnel. Both the FOI Act and the OSA regulate the release of information; the OSA prescribes penalties for the **unauthorised** disclosure of information in the areas of security; intelligence; defence; international relations; crime and special investigative powers. The FOI Act establishes authorised channels for release. The obligation of secrecy does not conflict with FOI Act since disclosure should always be properly authorised. More information on the OSA is given in JSP 440 Part 9, Chapter 2, paragraphs 3-18.

5. The **Public Records Act 1958 & 1967** the public records of the United Kingdom date back to the 11th century, with the current records legislation being set out in the 1958 & 1967 Acts. The latter reducing the release into the public domain to 30 years ("the 30-year rule"). This rule, which may reduce following a review in 2008, requires that by 30 years the department must have reviewed any surviving records and either transferred them to The National Archives (TNA), destroyed them or have permission to retain them. Where it is necessary to retain records in a Department beyond the 30 years, the approval of the Secretary of State for Justice is required. FOI legislation allows, subject to any necessary public interest test, access to information contained in files less than 30 years old and provides a route of access to files retained after that point. More information on the relation between the Public Records Act, Data Protection and Freedom of Information can be found in the "Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998", published by The National Archive in agreement with the Information Commissioners Office.

5.1 Initial review activity is undertaken locally, where staff and records managers are required to take into account both the business and potential historical value of the records they have created. Departmental Records Officer (Head of Corporate Information) carry out the final review of records. It is estimated that around 3-4% of records created by MOD are selected for permanent preservation at TNA.

6. The **EC Regulation 1049/2001** introduced the right to see information from the European Commission, Council and Parliament subject to certain exemptions for any citizen or registered resident of the EU. Article 5 covers requests received by a Member State (i.e. a government department) for a document in its possession, which originated from the Parliament, Council or Commission. It provides that, unless it is clear that the document should be, or should not be disclosed, the Member State should consult with the institution concerned in order to take a decision that does not jeopardise the attainment of the objectives of the Regulation. It can, if it

chooses, simply refer the request to the institution. Applications must be answered within 15 working days.

7. The **Human Rights Act 1998** (the HRA) came into force on 2 October 2000 and it gives effect to the principle of rights guaranteed by the European Convention on Human Rights (the Convention). The Convention was adopted by the Council of Europe in 1950 and ratified by the United Kingdom in 1951. It contains a number of fundamental rights and freedoms including the right to life, the right to a fair trial, freedom of thought, religion and speech and the right to respect for private and family life. Before the HRA, rights contained in the Convention could only be enforced in the European Commission and the Court of Human Rights established in Strasbourg. Since the HRA, the Convention rights have become part of domestic law and can be enforced directly in our courts by any person who claims to be a 'victim' of an infringement. There remains a right to bring cases in the Strasbourg court after pursuing domestic remedies.

7.1 Article 8 of the Convention is of particular importance in the context of the release of personal data and data sharing as it provides for a right to a private life, as follows:

> "8.1 Everyone has the right to respect for his private life, his home and his correspondence.
>
> 8.2 There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is 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 or morals, or for the protection of the rights and freedoms of others."

Identifying the Correct Access Regime

See Guidance Notes A3 FOI summary; B2 on the DPA; and B3 and B4 on the EIRs

8. When a request for information is received, it may be necessary to decide which regime applies or if it is a mixed request with parts falling under different regimes. Mixed requests may become apparent during the identification and review of the requested information; in these cases, for each part of the request, you must follow the process through to ensure that you are answering each part under the correct regime. Requests for information do not have to quote the relevant legislation. In most cases, it should be clear from the information sought in the request which access regime should be used to process it; but you must **be aware** that even if the request mentions the wrong legislation, you must still consider the request under the correct regime(s).

8.1 In dealing with straightforward requests (where it is intended to meet the request in full and within 20 working days) the regimes for FOI and EIRs are very similar. If there is to be any delay in answering, or the possibility of withholding or redacting information, then it is vital that the correct regime is followed. The FOI Act and the EIRs have different criteria in these respects. **There is provision in the EIRs to extend the response time to 40 working days, but only for complex and voluminous requests. The only valid reason for extension of the 20 working days in FOI is for consideration of the public interest test when considering the application of qualified exemptions.**