GAP 37: GUIDANCE ON THE DATA PROTECTION ACT 1998 DECEMBER 2004

Summary

This GAP explains the requirements of the Data Protection Act 1998 (The Act), which aims to protect the rights and privacy of individuals.

HSE holds a considerable amount of personal data: for certain duty holders, members of the public, and staff. In order to use this personal information fairly and legitimately, HSE must also adhere to certain principles & conditions and to the specified rights of the individual.

This GAP replaces all previous instructions on Data Protection. It presents up to date Whitehall-wide advice and emphasises our practical experience of the Act.

CONTENTS

SECTION 1

INTRODUCTION

PURPOSE OF THIS GAP

1. In 1998, the HSE Board decided to delegate day to day responsibility for compliance with the 1998 Act to Directorates and Divisions, as they are best placed to understand their locally held personal data and how the Act will affect them.

2. Some staff are designated as Directorate or Divisional data protection contacts and you should find out who that is in your own Directorate or Division. This GAP is designed primarily for them to help advise you on data protection compliance but you are free to read it or refer to it at any time. A less detailed introduction to the Data Protection Act is available on the intranet. You should go to your local contact whenever you have a question about data protection in the first instance.

3. The Board does not expect either your local contact or you to be 'experts' on data protection but as all of us, potentially, have responsibilities under the 1998 Act it is important for each of us to know when the 1998 Act is likely to apply and what we will need to do when it does.

4. This GAP provides enough information for contacts to advise you in most data protection cases.

5. The purpose of this GAP is to:

- explain some of the terms used in the 1998 Act;
- explain the requirements on HSE staff; and
- to indicate central and Directorate/Divisional roles in achieving continuous compliance.

6. This GAP applies to:

- HSC/E's dealings with the public regarding data protection; and
- HSC/E staff: where the detail in the GAP is relevant to HSC/E staff and their data protection rights as individual citizens in relation to the personal data that HSC/E holds on them (e.g. access to certain personnel and payroll records), appropriate guidance appears in the relevant section. Supplementary guidance can be found in Chapter 12 of the HSE Staff Handbook.

Note: the Information Commissioner has published the Employment Practices Data Protection Code in several parts. The Code is intended to explain to both employers and employees how the Data Protection Act 1998 might affect them. The Code is available from the Information Commissioner's website. You are free to read the Code. However, please refer to Chapter 12 of the HSE Staff Handbook and, if necessary, to Personnel Division, if you have any data protection questions relating to you as a member of staff.

7. The Cabinet Office has issued guidance calling for departments to ensure that their personnel records keeping practices are compliant with the Act. HSE applies the guidance to its personnel practices affected by the Act. Personnel Division holds a copy of this guidance which is also available on the Cabinet Office website.

8. This GAP provides advice on how the provisions apply to the personal information that HSE holds. Directorates and Divisions should follow the advice and instructions set out below unless advised to do otherwise by either the Information Management Unit (IMU) or the Solicitor's Office.

What is not covered by this GAP

9. This GAP does not provide prescriptive advice on specific data protection issues. While the advice that appears here can be used to guide Directorates and Divisions in complying with the 1998 Act for most situations likely to arise in HSE, it is neither possible nor desirable to provide prescriptive advice.

10. Neither does this GAP provide detail legal advice on compliance with the Act. If your case or circumstances are not covered in this guidance you should approach your Directorate or Divisional data protection contact in the first instance. In such cases, remember to think through all the issues involved before you reply in full.

11. The IMU and the Solicitor's Office should only be contacted in cases of genuine complexity.

EXECUTIVE SUMMARY

12. Staff should be aware that they should ask their Directorate or Divisional Data Protection/Open Government Contact for clarification and advice as necessary.

13. This GAP explains the requirements of the Act on HSE staff. This Act replaces the Data Protection Act 1984 and seeks to protect people's privacy with respect to information that organisations hold about them. The Act calls this *personal data*. In HSE we hold many types of *personal data*. These include:

- F2508 accident report forms;
- some mailing lists containing names and addresses;
- parts of FOCUS entries;

- qualifications databases (e.g. certificates of diving competence);
- safety policies of sole traders;
- some registers of correspondence.

14. The 1998 Act covers information held manually, on computer and in a "*relevant filing system*". The Act covers all *personal data* that we have already collected and all that we will collect in the future. The Act requires that we in HSE recognise and understand its key elements. These elements include:

- its wide scope, including sets of manual personal data, information held in a highly structured (and for public authorities, *unstructured*) form as well as computerised data;
- the required adherence to the 8 data protection principles and the conditions of processing [1] (see paragraphs 78-103);
- a restriction on the transfer of *personal data* to countries that do not have adequate security[2] (see paragraph 97);
- appropriate security measures to safeguard *personal data*[3] (see paragraph 103);
- the rights for the data subject[4] (see paragraph 92);
- provision for enforcement where the Act's provisions are not carried out[5] (see paragraphs 22-23);
- certain exemptions from the provisions[6] (see paragraphs 60-74); and
- a restriction on the disclosure of *personal data* to others[7] (see paragraphs 207-210).

15. In preparation for the Act's implementation, Directorates and Divisions compiled local plans to implement the Act for the personal data that they have responsibility for. These, together with the guidance in this GAP, should continue to identify the most cost-effective ways of complying with the provisions of the 1998 Act.

Important note

16. It is particularly important to realize that, apart from certain exemptions to certain duties, **all existing statutory restrictions on access to *personal data* - such as section 28 of the Health and Safety at Work etc Act 1974 (HSWA) - are disapplied in respect of the *data subject***, but not in respect of third parties[8]. Please see GAP 1 *(Ed Note: Link to Annex 2, para 32, GAP 1)* if you are not familiar with section 28 of HSWA in this GAP.

---

[1] Section 4(1), (2), (3), (4) of, and Schedule 1, parts I & II of the 1998 Act
[2] Section 4 (1) and (2) of, and Schedule 1, part I, para 8, and Schedule 1, part II, paras 13-15
[3] See part III of the 1998 Act
[4] See part II of the 1998 Act
[5] See part V of the 1998 Act
[6] See part IV of the 1998 Act
[7] Sections 4(1), (2), 7 (3), (4), (6) and 27 (3) of the 1998 Act

SECTION 2

THE BASICS

WHAT IS IN THIS SECTION?

DATA PROTECTION 'RIGHTS'

17. The purpose of both the 1998 Act and the EC Directive[1] to which the Act gives effect, is to protect the fundamental rights and freedoms of **living individuals**, and in particular their right to privacy with respect to the processing of their *personal data* whilst facilitating the free movement of data between member states by the legitimate processing of personal data by data controllers. It is a reserved issue and applies equally throughout the United Kingdom (UK).

18. The Act accords individuals certain rights regarding the personal data or sensitive personal data held on them. These are:

A right of access to personal information held on them (*subject access*)[2].

19. Data subjects have the following subject access rights (subject to the exemptions in paragraphs 147-189 below) upon providing a written request and supplying the information - detailed at paragraphs 129-146 - that HSE is entitled to request to enable us to search for the data:

- the right to seek confirmation that we hold personal data on them or that such data are held by a third party on our behalf (e.g. National Radiological Protection Board as our nominated data processor for certain radiation data);
- if we hold personal data relating to them, data subjects have the right:

  to be given a description of the data;

  to be informed of the purposes for which we are processing the data;

  to be informed of the categories of recipient to whom we may disclose the data;

to be informed whether any automated processing we do will form the sole means of taking decisions significantly affecting them.

- And if the data subjects so wish, they have the right:

  to be given a copy of the data in an *intelligible* form (i.e. with an explanation of codes, abbreviations etc. used, and with sufficient extra information to allow the individual to make sense of their personal data; e.g. in an accident investigation report it is insufficient to provide only the sentences on Mr Smith - you should also include the sentences dealing with circumstances around the accident without mentioning any other person involved); and

  to be given any information we hold on the source of the data (see paragraphs 106-111 on HSE's Notification).

A right to prevent processing likely to cause the data subject, or another, damage or distress[3].

A right to prevent processing for the purposes of direct marketing[4].

A right not to have certain decisions made about them, which are based solely on automated processing[5].

A right to claim compensation where the Act's requirements have been contravened[6].

A right to correct, block, erase or destroy inaccurate personal data[7].

20. Directorates and Divisions will carry out most day-to-day compliance activity.

21. This includes:

- ensuring that your manual and computerised databases conform to the *data protection principles* (see paragraphs 78-100) and the *Conditions of Processing (*see paragraphs 101-103);
- granting individuals access to the *personal data* that HSE holds on them;
- respecting the data protection rights of individuals; and
- disclosing *personal data* to third parties where allowed.

22. All staff must make every effort to comply with the requirements which the1998 Act places upon HSE:

- in some cases, failure to comply is a criminal offence[8];
- in others, it may result in an enforcement or information notice being served on HSE by the Information Commissioner[9].
- *Data subjects* also have the right to seek redress through the civil courts for damage and/or distress caused by any breach of the Act by HSE, and to seek rectification, blocking, erasure and destruction of inaccurate data (see paragraphs 276-282).

23. All cases where:

- there is an indication or allegation that HSE has committed an offence;
- an enforcement or information notice has been served or is expected to be served; or
- a claim for compensation has been made or is expected to be made;

the case must be referred immediately to IMU and the Solicitor's Office.

24. The Act contains a number of exemptions to reactive duties, but HSE policy is to use these only where absolutely necessary see paragraphs 154-155. The rights that exist under the Act are not absolute; they are what are termed "qualified" rights. However, despite this status, data protection rights are fundamental human rights, having their roots in Article 8 of the European Convention on Human Rights (ECHR)[10]. Article 8 therefore allows a public authority to interfere with the right to privacy where that interference is in accordance with the law and in pursuit of a legitimate aim and is necessary in a democratic society[11].

25. All this means is that data protection rights can be refused or withheld where it is legally justified to do so - hence the exemptions.

TERMS AND DEFINITIONS

26. There are a few core terms and definitions that you will need to be familiar with:

Data

27. Information that:

- is being processed by a computer
- has been intentionally recorded for use by a computer

- is not processed by a computer but is part of a relevant filing system or will be

- is a health or education record or a local authority housing or social services record or

- is recorded information held by a public authority that does not fall into one of the categories above.

Data subject

28. An **identifiable living individual**[12] whose personal data is held.

- For HSC/E, data subjects include workers, members of the public, unincorporated businesses (sole traders, self-employed or partners) and HSE staff.

Note: the definition of data subject does not include post holders, e.g. The secretary of a body, when it is the body HSE deals with rather than the post holder in his/her personal capacity.

Data controller

29. A data controller is a person who decides (either alone or jointly) the purposes for which the personal data are used and determines how they are used[13].

- In respect of personal data held by HSC, **HSC is the data controller**.

- In respect of *personal data* held by HSE (including the Health and Safety Laboratory (HSL), **HSE is the *data controller***. The Head of the Information Management Unit is designated as HSE's contact at the Office of the Information Commissioner.

30. HSE has also adopted the concept of 'local data controllers' (which is not recognised by the 1998 Act) - i.e. individuals within an organisation to whom operational responsibility for particular sets of data has been delegated (Directorates and Divisions). However, HSC/E as the data controller retains formal responsibility for compliance, with local data controllers being answerable to the data controller for compliance with the organisation's policies and procedures.

Personal data

31. The definition of personal data is very broad; but,the decision in the case of Durant[14] has attempted to narrow this definition. Personal data is:

- Data which relates to a **living individual** who can be identified from those data; or

- Data and any other information in the possession of, or is likely to come into the possession of, the *data controller* includes:

    - Any **expression of opinion** about the data subject and any indication of the intentions of the data controller or any other person **in respect of the data subject**

    - When dealing with expressions of opinion, you will need to take care to avoid making, where possible, defamatory statements (see Annex E);

    - Data that must be kept (or intended to be kept) on a computerised system or in a relevant filing system. For public authorities (such as HSE), the definition is further extended to unstructured manual data[15] (see paragraphs 44-47 below on 'manual data' for further details).

    - Health records. The following text is an extract from the Information Commissioner's compliance advice "Subject Access and Health Records" 13 November 2001:

32. "A "health record" is defined in the Act as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. The definition of a "health record" could also apply to material held on an X-ray or an MRI scan, for example.

33. The Access to Health Records Act 1990, formerly gave individuals a right of access to manual health records. However, this Act has now been repealed because of the provisions of the Data Protection Act except for the sections dealing with requests for access to records relating to the deceased. Requests for these records will continue to be made under the Access to Health Records Act 1990. However, requests for access to health records relating to living individuals, **whether the records are manual or automated**, will now fall within the scope of subject information provisions of the 1998 Act (see paragraph 136) and must be dealt with in the manner stipulated by the Act."[16]

34. Understanding what data are personal data covered by the 1998 Act is very important. Below are a few guidelines to help you decide if the data you hold are covered by the Act.

35. ***"Personal data"*** under the Act must first fulfill the definition of *data* given above. If they do not, then they are **not** *personal data*.

36. In general, *personal data* are *data* about **particular living individuals** or *data* provided to HSC/E by individuals where those data are either about them or their activities. In many cases HSC/E will get data directly from the *data subject*, but in others they get them from employers, doctors or even members of the public.

37. *Personal data* can also include the broader circumstances, which aid the understanding of a particular incident. For example, it could comprise the safety policy of a sole trader, or the circumstances surrounding an accident in which the *data subject* was the injured person. **This must be looked at on a case-by-case basis.**

38. It is considered that a reference to an individual's name alone is unlikely to be *personal data*. However, it is unlikely that a person's name will be held independently of any supporting information - that would come from the context in which the name is held.

39. Frequently HSC/E does not file personal data under the data subject's name. Sometimes personal data is included in records filed under the name of the employer (e.g. F2508 forms). So long as the data subject or others can give enough information to locate the record (e.g. for a RIDDOR report, name of employer and date of accident) it is personal data. If we are unable to identify the individual until the data subject gives us such pertinent extra information, the information becomes personal data only at this moment.

40. You do not have to be able to put a **name** to an individual in order to be able to identify them: if individuals' records are tagged by a unique identifier (e.g. NI or NHS number) on a database, these constitute personal data.

41. **Anonymising *personal data*** (i.e. so that the *data subject* can no longer be identified from them or through any other way available to HSE or others) places them outside the scope of the Act. Anonymising data ensures the privacy of the data subject; the data cannot form the basis of any decision substantially affecting the individual, and, if disclosed, they do not identify the individual.)

- Anonymise data if you do not need to keep them in a personalised form.

- This may be useful for dealing with *personal data* that are superfluous to requirements (but only where the overall information is still required) or data used for research or statistical purposes.

- Anonymisation must include removing not only the name of *data subjects* but also other information (e.g. NI or NHS number) that could allow them to be traced.

Do not anonymise data **solely** to avoid the obligations imposed under the Act.

Sensitive personal data

42. Sensitive personal data[17] comprise personal data consisting of information about data subjects':

- racial or ethnic origin;
- political opinions (may be of relevance, e.g., when a short CV is prepared for a nomination to a HSC Advisory Committee);
- religious or similar beliefs;
- membership of a trade union (may be of relevance, e.g., when a short CV is prepared for a nomination to a HSC Advisory Committee);
- physical or mental health or condition;
- sexual life;
- actual or alleged offences or related court proceedings.

43. Expression of opinion or intention relating to any of the above will also fall into the category of Sensitive Personal Data.

Manual Data

44. Under the 1998 Act, manual data that did not form part of a relevant filing system was not considered 'Data'. Since January 1st 2005, such manual data *has* come under the scope of DPA as a result of amendments made by the Freedom of Information Act.[10] NB: This applies to 'public authorities' only[19]. For the moment, the duty to extend the remit of DPA to such manual files does not apply to private organisations.

45. Even if a manual filing system is structured in a way that information about a specific individual cannot be made readily accessible, the amendments made by section 69 of the Freedom of Information Act 2000, allow a data subject access to his/her personal data in certain circumstances.

It is no longer a condition that data will only be accessible if it is structured. Miscellaneous documents held in an un-indexed shoe-box, for example, will be covered by the Act.

46. While the effect of the Freedom of Information Act 2000 is to extend subject access rights to unstructured files held by a public authority, it also places some additional hurdles for a data subject to clear in respect of these unstructured files[20]:

- the subject access request must contain a description of the data (an open-ended 'fishing expedition' will not require the data controller to trawl through unstructured manual files).

- Even with a description of the data, the data controller need not comply with the request if it estimates that the cost of compliance would exceed the appropriate limit.[21]

47. Personnel files held by public authorities however are exempted from this extension to unstructured manual files.[22]

Data processor

48. A data processor[23] is a person or organisation (other than employees of the data controller) that processes the information on behalf of the data controller (see paragraph 29).

49. HSC does not normally process personal data itself; this data is normally processed by HSE as a data processor.

- HSC/E sometimes uses other organisations or persons to carry out some or all processing operations in certain circumstances.

50. There are two types of data processor. In some cases the use of a *data processor* is continuous. For example:

- Refit for IT-related issues, where these include the processing of personal data; or

- The National Radiological Protection Board, which processes personal data relating to the Central Index of Dose Information (CIDI).

51. In other cases, for example on research projects, the use of a data processor is confined to a one off task and ends when the task (i.e. contract) is completed. However, in all these cases HSC/E remain the data controllers and are responsible for ensuring compliance with their obligations under the 1998 Act.

Processing

Processing[24] covers anything you might do with personal data from the moment you obtain it until the moment you have destroyed it. It includes the obtaining, recording or holding of data, or carrying out any operation on the data, including the organisation, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking, erasure or destruction; in fact, it is difficult to conceive of any action that would not be classed as processing.

Health Records

52. A health record is any data relating to the physical or mental well-being of an individual (i.e: an x-ray) and has been made by a health professional.

Health Professional

53. Registered: doctors, nurses, dentists, opticians, pharmacist, osteopath, chiropractor, clinical psychologists, a music therapist or a scientist employed by a health service body as a head of department

Investigation Reports

54. Investigation reports dealing with an accident may hold *personal data* relating to one or more specific individuals. As a general guide, if you can refer to an investigation report as the one on Mr or Ms X's accident, then it is probably within scope, although most investigation reports would not meet the characteristics described above. Of course, not all of the information in such reports will necessarily be *personal data*, as parts may consider, for example, the health and safety record and policy of the firm concerned. Casual mentions of individuals in reports (e.g. the name of a person present at the scene of the incident) will not be in scope, as the *data* is not structured in relation to this individual (this is consistent with the decision in Durant v FSA).

E-mail

55. Incoming and outgoing e-mails are covered by the 1998 Act if one or other of the following criteria is met:

- the sender or recipient is identifiable, either through their e-mail address or the text of the e-mail; or

- the text of the e-mail contains personal data, i.e. facts, opinions or intentions about identifiable living individuals

56. Under the Act, e-mails in personal mailboxes and deleted items boxes, e-mails saved into an electronic records management systems and e-mails printed and held in a “relevant filing system” or, in the case of public authorities, in an unstructured manual file, are liable for disclosure, either in part or as a whole, in response to a subject access request, if they contain relevant personal data. This is subject to any third party consideration and exemptions that might apply. Copies on back-up systems may also be liable for disclosure, for example in exceptional circumstances relating to serous criminal allegations where the cost and disruption is merited.

57. E-mails are potentially part of the corporate record of a department and should be subject to the department’s records management policies and procedures. **Nothing should be put in an e-mail that cannot be defended.**

58. All staff should review incoming and outgoing e-mails to decide whether they contain information about the department's business that should be kept as part of the corporate record or for other reasons, e.g. the six-year limitation period for claims for breach of contract to be litigated. If the decision is to retain an e-mail it should be filed [by saving it into the departmental electronic records management system/by printing it off and putting it on the relevant paper file]. The e-mail should then be deleted from the personal mailbox and any "deleted items" box.

59. If an e-mail is not required for the corporate record or other reasons it should be deleted, either immediately or when it has ceased to be of use. This includes e-mails that may have been moved from a mailbox to a personal or shared storage area.

INTRODUCTION TO EXEMPTIONS FROM DATA PROTECTION DUTIES

60. HSC/E is obliged to comply fully with the 1998 Act and to be as open as possible with individuals about the data that we hold on them. The Act contains, however, exemptions[25] to performing certain duties, and it is HSE policy to use these only where absolutely necessary.

61. There are two types of exemption:

- Non-Disclosure Exemptions[26] (that allow you to disclose personal data) and
- Subject Information Exemptions[27] (that allow you to withhold data).

Non-disclosure exemptions

62. Exemption from the non-disclosure provisions is available in circumstances where the Act recognises that public interest requires the disclosure of personal data.

63. There is a two-stage test when considering applying a non-disclosure exemption:

- Does this fall within the relevant sections – 29(3) (crime & taxation), 34 (information made available to the public by or under any enactment) or 35 (disclosures required by law or in connection with legal proceedings).
- If so, each of the non-disclosure provisions[28] should be considered and the exemption applied only to those, where the non-application of the exemption would give rise to an inconsistency, and only to the extent of rectifying that inconsistency.

64. Thus even if an exemption applies, it will not automatically apply to all of the non-disclosure provisions.

65. **Important Note:** Do not confuse the two types of exemption. For example, the exemption available in Section 31 (regulatory activity) applies to the subject information provisions only.

66. Thus, personal data collected for the purposes of securing the health & safety of people at work can be exempted from subject access and/or fair processing (paragraphs 2&3 of Part II, Schedule I) to the extent that the application of these provisions would otherwise prejudice HSE's proper discharge of their functions.

67. It does not however mean that we can disclose such personal data to a third party since this exemption does not apply to the non-disclosure provisions.

68. The exemption available in Section 29(3) (crime & taxation) DOES however apply to the non-disclosure provisions and HSE may use this exemption for disclosure to a third party (i.e. the Police).

69. Please be aware which type of exemption you are using.

Using an exemption

70. Take care when using exemptions. Any intention to use an exemption should first be discussed with the relevant Directorate and/or Divisional Data Protection Contact. The decision should then be passed to the Information Management Unit. The Unit will not approve the use of the exemption - that is a matter for Directorates and Divisions - but it will advise on whether or not the exemption is being used correctly and consistently with the rest of HSE. The Unit will advise the Directorate or Division to reconsider if the exemption is in any way inappropriate and will help to find the right course of action. Exemptions should be considered on a case-by-case basis.

71. Guidance on relevant exemptions is covered below. Most exemptions are self-explanatory. Guidance is given where relevant.

Section 28 of the Health and Safety at Work etc Act 1974

72. Because the Act confers certain rights on individuals, it has the effect of disapplying certain other restrictive statutory provisions. One such provision was section 28 of the Health and Safety at Work etc Act 1974. GAP 1 provides detail on section 28 (see GAP 1 Annex 2 para 32).

73. Before January 1st 2005, restrictions on the release of section 28 data were disapplied in the case of subject access requests. Where a third party sought access to another person's data, the provisions of section 28 were reapplied.

74. However since January 1st 2005, section 28 no longer, in itself, represents a statutory bar. Whether it is subject access or third party access, section 28 restrictions do not apply (although other statutory provisions *may* apply e.g. FOIA as may certain of the exemptions to the 1998 Act).

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. The preamble to the act makes specific reference to the need to protect fundamental rights and freedoms, notably the right to privacy as recognised both in Article 8 of the European Convention of Human Rights and the general principles of Community law. The 1998 Act should therefore be interpreted in the light of, and to give effect to, the Directive's provisions: See Campbell V MGN ltd [2002] EWCA Civ 1373.
[2] Section 7(1) of the 1998 Act
[3] Section 10
[4] Section 11
[5] Section 12
[6] Section 13
[7] Section 14
[8] Sections 55(1), (4), (5), 56 and 60
[9] Part V
[10] Article 8 states:
"8.1. Everyone has the right to respect for his private & family 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 crime and disorder, for the protection of health or morals or for the protection of the rights and freedoms of others."
[11] R(Robertson) v City of Wakefield Metropolitan Council [2002] 2 WLR 889 (see end note lxxvi for explanation);
[12] Section 1(1) Access to the health data of the deceased is governed by the Access to Health Records 1990.
[13] Section 1(1)
[14] The Court of Appeal in Durant vs Financial Services Authority [2003] EWCA Civ 1746 has given guidance on the meaning of "personal data". The result is a possible narrowing of its definition. The preferred view however would be the broader interpretation of personal data laid down by the amendments in the FOIA2000. It is suggested that in order to avoid the risk of improper disclosure, this view should be adopted. Please contact IMU for further details.
[15] Section 1(1)e
[16] In fact, the Access to Health Records Act has only been repealed in part but this does not affect the advice given by the Information Commissioner.
[17] Section 2 and also Schedule 3 (for the conditions for which such data will be considered to have been processed fairly and lawfully in accordance with the first data protection principle.
[18] FOIA 2000, Sections 68,69 & 70
[19] 'Public authority' has the same meaning as that defined in FOIA 2000, section 3(2)
[20] FOIA2000, Section 69(2)
[21] Charges as prescribed by 12(5) of FOIA2000 – HSE currently do not apply these charges
[22] FOIA2000, Section 70 (1), DPA 1998 Section 33A(2)
[23] Section 1(1)
[24] Section 1(1)
[25] Part IV of and Schedule 7 to the 1998 Act
[26] This category of exemption applies to the First Data Protection Principle (except where it requires compliance with the conditions in Schedules 2&3 of the Act, conditions for processing personal and sensitive personal data), the Second, Third, Fourth & Fifth Principles, Section 10 (processing likely to cause damage or distress) and Section 14(1)-(3)(rectification, blocking, erasing & destruction) TO THE EXTENT TO WHICH THEY ARE INCONSISTENT WITH THE DISCLOSURE IN QUESTION.
[27] This category of exemption applies to paragraphs 2&3 of Part II of Schedule I which refer to the fair processing information AND Section 7 (subject access)

[28] the First Data Protection Principle (except where it requires compliance with the conditions in Schedules 2&3 of the Act, conditions for processing personal and sensitive personal data), the Second, Third, Fourth & Fifth Principles, Section 10 (processing likely to cause damage or distress) and Section 14(1)-(3)(rectification, blocking, erasing & destruction)

SECTION 3

PROACTIVE DUTIES

WHAT IS IN THIS SECTION?

INTRODUCTION

75. The duties placed on HSE by the Data Protection Act 1998 fall into two main categories: proactive and reactive. This section covers proactive duties.

76. The proactive duties comprise:

- To comply with the Data Protection Principles and Conditions for Processing set out in the Act in respect of the personal and/or sensitive personal data that HSE holds.
- Advising data subjects that HSE processes their data
- HSC and HSE are required to notify the Information Commissioner of all the purposes for which they process personal and/or sensitive personal data (see paragraph 82).

77. There is currently no duty to monitor HSE's data protection activities. However, as with all policies, this decision will remain under review.

DATA PROTECTION PRINCIPLES

78. All of the following principles must be met for HSE to process personal and/or sensitive personal data fairly and lawfully.

First principle: fair and lawful processing[1]

79. Personal data can only be processed if one or more relevant Conditions for Processing for personal data are met, and - in the case of sensitive personal data - if

one or more relevant Conditions for Processing for sensitive personal data are also met. You may obtain personal data only from the data subject or from a third party that is either authorised or legally required to supply them to us.

80. In the latter case, ensure that the person who supplies the data is aware of the purposes of your processing (see subparagraph (b) below). Ways of dealing with this have included changing forms used for collating certain data (e.g. the witness statement form; forms for applications for approvals/licenses; certain HSE personnel forms) to include mention of the purposes of processing.

Second principle: purposes of processing[2]

81. Personal data may be obtained and processed only for one or more specified and lawful purpose(s), and may be further processed (e.g. by a data controller or a data processor) only for the same or compatible purpose(s).

82. HSE's Notification to the Information Commissioner details the purposes for which we process personal and/or sensitive personal data. The Notification appears on the Information Commissioner's website and details not only the purposes but also the classes of data that we hold and the category of recipients - those to whom we may disclose the data. For convenience, the purposes are reproduced here. HSE process personal data for the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Licensing and registration
- Crime prevention and the prosecution of offenders
- Research
- Consultancy and advisory services
- Information and databank administration
- Legal services
- Administration of justice
- Administration of HSAWA

Third principle: appropriateness of processing[3]

83. You should process only personal data that is adequate, relevant and not excessive in relation to the purpose(s) for which they were collected. Do not request data not needed for our purposes. However, a data subject may give us, voluntarily, personal data superfluous to our purposes, as may be the case with manual forms.

Similarly, a third party may have supplied such extra and unnecessary data. In both cases, (if feasible) consider destroying the unnecessary.

84. There is a practical difficulty in destroying manual data in particular (as it may be on the same form as relevant personal data that we need to keep). You may find it easier to destroy (or, ideally, not enter) superfluous data in a computerised form.

Fourth principle: data accuracy[4]

85. The data you have must be accurate and kept up to date. Keeping records up to date does not mean you have to write to data subjects every so often. However, you should take opportunities to update records (e.g. personal details on mailing lists) where these present themselves. You should also take care not to take decisions that substantively affect data subjects without ensuring that the data you have is accurate and up to date.

86. Where we know a record is out of date, we should either amend it (and bring it up to date) or anonymise/delete it. This includes manually amending frozen databases such as SHIELD.

87. See Right to have inaccurate data rectified, blocked, erased or destroyed paragraphs 276-282.

Fifth principle: holding personal data for only as long as it is necessary[5]

88. Keep personal data in a personalised form (i.e. that allows a data subject to be identified) only for as long as it is required for the purposes for which it was collected; obviously this will vary between purposes.

89. You may, however, keep personal data in a personalised form indefinitely where the personal data is processed only for “research and statistical purposes”. “Research and statistical purposes” are where the information is not to be used in relation to taking decisions affecting a data subject or causing that data subject damage or distress (e.g. some of the data collected by HSE’s statistical units).

90. Personal data should be destroyed or anonymised when they are no longer necessary for the purposes for which they were collected - as long as there are no other barriers to destruction see paragraph 91.

91. Do not destroy or anonymise data while there is still a business purpose for keeping them, solely to avoid the duties of the Act. (Do not, for example, destroy personal data simply because you do not want the data subject to see it). Anonymisation must include removing not only the name of data subjects but also other information (e.g. NI or NHS number) that could allow them to be traced. Anonymisation must result in the inability to identify a specific individual either directly or indirectly from the remaining information.

Sixth principle: respect for data subject rights[6]

92. You may process data only in accordance with the rights of the data subject. These rights are covered in the sections on subject access and other rights of the data subject.

Seventh principle: security of records[7]

93. Measures, appropriate to the risk, must be taken against unlawful or unauthorised processing of personal data and against accidental loss, destruction or damage to personal data.

94. HSC/E policy on appropriate security measures for computerised personal data is set out in GAP 65 "HSE's IT Security policy" (if you have a query, contact HSE's IT Security Officer in BEU). If you follow these procedures, you will have satisfied the requirements of the seventh Data Protection Principle.

95. HSC/E policy on appropriate security measures for manual personal data is set out on the Intranet Security Policies and Procedures – Handling Protectively Marked material. You must treat all manual personal data as 'Restricted' material and follow the minimum-security procedures for handling restricted material outlined in that instruction.

- Store the data in a locked desk or filing cabinet, and keep it locked outside office hours or if the office is left unattended for a period of time.
- Should particular personal data have a protective marking higher than 'Restricted' (i.e. Confidential, Secret or Top Secret), follow procedures required for the marking.
- If you follow these procedures, you will have satisfied the requirements of the seventh data protection principle.
- If you allow processing by a data processor on your behalf, ensure that: the data processor can implement suitable security measures; and
- processing is subject to a written contract under which the data processor is to act only on your instructions, and which holds the data processor to the same obligations as you (examples of contracts include that between HSE and Refit on IT issues, and between HSE and National Radiological Protection Board in respect of exposure data on ionising radiation).

Eighth principle: transfer of personal data outside the EEA[8]

96. The development of technology - mainly e-mail and the Internet - has provided means to transfer information very easily, not only throughout an organisation, but also across countries and international borders. While this can and often does ease the movement of data, it places an additional responsibility on data controllers when they decide to move personal data in this way. The Act recognises this and the final Principle deals with the transfer for data outside the European Economic Area (EEA).

97. In short, you must not transfer personal data outside the EEA unless you are satisfied that the recipient country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing personal data. The EEA comprises the 15 EU member states plus Norway, Iceland and Liechtenstein.

98. In July 2000, the European Union adopted a 'Decision'[9] approving the United States 'safe harbour' arrangement. Commitment to 'safe harbours' will provide an adequate level of protection for transfers of personal data to the US from the EU Member States. This, in turn, will provide a basis for compliance with the 8th Principle of the Act in the UK in relation to transfers to the US.

99. Please advise IMU if you intend to transfer personal data to one or more of the following countries:

> Australia; Canada; Guernsey; Hong Kong; Hungary; Isle of Man; Israel; Japan; Jersey; New Zealand; Poland; Slovak Republic; Slovenia; Switzerland; and Taiwan

100. Guidance on compliance is given in "Transferring personal data outside the EEA" Annex I.

CONDITIONS FOR PROCESSING PERSONAL DATA[10]

101. In order to comply with the first data protection principle, you may process personal data only where your processing satisfies one or more of the following conditions:

- you have the data subject's consent to processing. The 1998 Act does not define "consent" in this case. However, consent would need to be, at the very least, fully informed and, ideally, explicit;

- processing is necessary to carry out a contract to which the data subject is - or is likely to be - a party;

- processing is necessary to comply with a legal obligation (e.g. the GMO (Contained Use) Regulations require the recording of certain personal data);

- processing is necessary to protect the vital interests of the data subject (according to the Information Commissioner, this literally means cases of life or death, which are likely to be very rare for HSE - personal data concerning industrial diseases might in some cases be an example);

- processing is necessary for the administration of justice;

- processing is necessary to carry out HSC/E's statutory functions. **This condition is likely to apply to many of HSC/E's processing of personal data but that in itself may not be sufficient.** HSC/E are established under statute and, therefore, many of our functions are set out in either HSWA or the many relevant statutory provisions. Where we process personal data for the "purpose of our functions", it will be necessary to identify & stipulate which specific function (usually statutory) that we are referring to (e.g. which regulations allow you to have obtained the data and so on). We also process the personal data of HSE staff for the purpose of their employment. (This condition would also include functions we carry out as an agency on behalf of a government department - e.g. ELCI, FEPA and other agency agreements);

- processing is necessary for the purposes of the legitimate interests of the third party to whom the data is disclosed, provided this does not prejudice the rights, freedoms or legitimate interests of the data subject.

CONDITIONS FOR PROCESSING SENSITIVE PERSONAL DATA[11]

102. In order to comply with the first data protection principle, you may process sensitive personal data only where your processing satisfies one or more of the conditions mentioned above and - additionally - one or more of the following conditions:

- the data subject has given his explicit consent (i.e. unequivocal, written and informed - particular to the intended processing operation);

- the law requires the processing in connection with employment (Solicitor's Office and the Home Office have stated that health and safety at work legislation is part of employment law) - e.g. some employers are statutorily required to conduct health or medical surveillance on employees and keep records of this (e.g. the Control of Asbestos at Work Regulations 1987);

- the data subject has taken steps to reveal publicly the data (either directly or indirectly);

- processing is necessary for the purpose of any legal proceedings (including potential proceedings), for seeking legal advice or for defending legal rights;

- processing is necessary for medical purposes (including 'medical research'), and is carried out - or overseen by - a health professional (or equivalent);

- processing is necessary to protect the vital interests of the data subject or of another person where the data controller considers that consent has been unreasonably withheld (see comment in equivalent bullet under paragraph 207;

- processing is necessary to carry out HSC/E's statutory functions. **This condition is likely to apply to many and covers all HSC/E's processing of sensitive personal data but that in itself may not be sufficient.** HSC/E are established under statute and, therefore, many of our functions are set out in either HSWA or the many relevant statutory provisions. Where we process personal data for the "purpose of our functions", it is often necessary to identify & stipulate which specific function (usually statutory) we are referring to (e.g. which regulations allow you to have obtained the data and so on). We also process the personal data of HSE staff for the purpose of their employment. (This condition would also include functions we carry out as an agency on behalf of a Government Department - e.g. ELCI, FEPA and other agency agreements). (See comment in equivalent bullet under paragraph286).

103. When processing sensitive personal data (such as health records) please make sure it is 'carried out with appropriate safeguards for the rights and freedoms of the individual'[12]. For instance, make sure that the data is securely stored and that only those who need access to the data are able to access it. Where possible, anonymise the data.

PROACTIVE DUTY TO INFORM DATA SUBJECTS[13]

104. To allow data subjects to know that there are personal data held on them by a data controller, the Act places a duty on data controllers, so far as is practicable, to provide data subjects, at the time of the collection of the data or as soon afterwards as possible, with the following information:

- the identity of the data controller (in our case, HSC or HSE);

- the identity of any data processor if HSC/E is using one in respect of the database the personal data belong to (e.g. research contractors; Atos Origin Occupational Health Advisors etc);

- the purposes for which we intend to process the data (in our case, for the purposes set out in our Notification to the Information Commissioner);

- any further information needed to enable the fair processing of the personal data, including:

- the categories of Recipient to whom data may be disclosed - these also appear in our Notification under the relevant purpose;

- whether the data has been provided to us because of statutory requirements or voluntarily;

- their right as data subjects to have a copy of the personal data we hold on them and to correct any inaccuracies.

105. For HSE it is probably easiest to provide this information at the time we first collect it. Ways of achieving this have included:

- adapting forms to provide the detail (e.g. application forms used for recruitment);

- providing a purpose-made leaflet for duty holders who are also data subjects.

- Other methods may include:

    - adding a standard paragraph to routine correspondence or an e-mail if that is the method of contact.

NOTIFICATION TO THE INFORMATION COMMISSIONER[14]

106. There is a statutory requirement for all data controllers to notify the Information Commissioner of all the purposes for which they process personal and sensitive personal data, unless one of the exemptions under the Data Protection (Notification and Notification Fees) Regulations 2000 (SI No. 188) applies.

107. HSE must comply with this requirement.

108. HSE's Notification appears on the Information Commissioner's website and is available on the Internet to anyone who wishes to see it. It must be kept fully up to date as HSE can only lawfully process data for the purposes that appear there. Your Directorate or Divisional data protection contact should also have a copy. If anyone requests inspection of or copies of the HSE Notification, they should be advised to look at the Information Commissioner's website or to contact the Commissioner's Office directly. We are not obliged to provide a copy, as the information is already publicly available.

109. The Information Management Unit has responsibility for ensuring that the Notification is kept up to date. The Branch will contact Directorates and Divisions when necessary to review and update the purposes as required. The responsibility for ensuring that the purposes are accurate and appropriate rests with Directorates and Divisions who understand their processing best.

110. Notification requires HSE to inform the Commissioner of the following 'registerable particulars'[15]. These are:

- our name and address as data controller;

- the name and address of any representative we nominate;

- a description of the data we process, and the categories of data subject to which they relate;
- a description of the purposes for which the data are processed;
- a description of any Recipient(s) to whom we may disclose the data;
- details of any countries outside the EEA to which we intend to transfer data;
- a general description of security measures taken to protect the data.

111. It is an offence to process data without Notification where Notification, or a change of Notification, is required.[16]

Assessable processing

112. Where specified types of processing are likely to:

- cause substantial damage or distress to data subjects; or
- prejudice significantly the rights and freedoms of data subjects; the 1998 Act provides that any such types must be notified to the Information Commissioner.

113. The Information Commissioner will then give the data controller an opinion on whether the processing is likely to comply with the provisions of the Act. However, no Order has yet been made under this section nor any designation as to the type of processing expected to be covered. This means that no action needs to be taken at the time of writing.

Data Sharing

114. The 1998 Act does not automatically give you the power to share data with another Department (data sharing being a form pf 'processing'). While the Act specifies that data should be processed fairly & lawfully, it does not specify what 'lawfully' means. You must therefore be sure that you have a lawful basis for sharing the data.

115. A lawful basis for Data sharing is sometimes grounded in statute through legal 'gateways' (e.g. Crime & Disorder Act, s115 & section 17 of the Anti-terrorist, Crime Security Act). More often than not though, there is no relevant statutory power and it will be necessary to determine whether a power to share can reasonably be implied[17]. In determining whether data sharing is possible, it is necessary to look at Administrative law, the Human Rights Act, the common law duty of Confidence and European Law as well as the DPA.

116. The interrelationship between the above in complex but the following approach is a starting point to determine whether the power exists to share data.

117. Establish whether you have the power to carry out the function to which the data sharing relates:

- Decide whether the sharing would infringe Article 8 of the ECHR in a way that is disproportionate to the achievement of the aim;
- Decide whether the sharing would breach any obligations of confidence
- Make sure that processing is in accordance with the DPA principles
- Are there any other issues? (check compatibility with community law).

118. Data sharing protocols are formal agreements between organisations that are sharing data and identify the legal basis for this sharing and set out the principles & commitments that organisations will adopt when processing data. Without such formal agreements, organisations may fall short of applying common standards and there may be confusion over responsibilities.

119. If you plan to exchange personal data on a regular basis, you may wish to consider establishing a protocol with the relevant Department/Agency. However, protocols in themselves *cannot* make processing lawful where no power to data share already exists.

120. Remember, that while the second data protection principle requires data not to be further processed in any manner incompatible with the original purpose for which it was obtained; this is not an outright bar on data sharing. This obligation of compatibility does not have to mean that the processing is identical; merely that it is not contradictory to the original purpose.

121. The Act provides specific limited exemptions to the rule of non-disclosure and S. 29(3) provides a gateway for sharing data where to do otherwise would likely prejudice:

- The prevention/detection of crime
- The apprehension/prosecution of offenders
- The collection of any tax

122. So for example, we would be able to share data collected for health & safety purposes with the Inland Revenue for the purposes of collecting tax as long as this did not infringe the data subject's human rights (i.e. that this was necessary in a democratic society, proportionate and there was no other way to do it).

123. Section 35 of the 1998 Act (the 'Gateways' exemptions), disclosures of personal data required by law or made in connection with legal proceedings are also exempted from the non-disclosure provisions.

124. See Annex H for a data Sharing Case study.

[1] Schedule 1, part I, para 1 and Schedule 1, part II, paragraphs 1-4
[2] Schedule 1, part I, para 2 and Schedule 1, part II, paragraph 5
[3] Schedule 1, part I, para 3
[4] Schedule 1, part I, para 4 and Schedule 1, part II, paragraph 7
[5] Schedule 1, part I, para 5
[6] Schedule 1, part I, para 6 and Schedule 1, part II, paragraph 8
[7] Schedule 1, part I, para 7 and Schedule 1, part II, paragraphs 9-12
[8] Schedule 1, part I, para 8 and Schedule 1, part II, paragraphs 13-18 & schedule 4 for cases where the 8th principle does not apply
[9] Commission decision 520/2000/EC of July 26th 2000 pursuant to Directive 95/46
[10] Section 4(3) and Schedule 2, para 1-6
[11] Section 4(3) and Schedule 3, paras 1-8
[12] Schedule 3(4b)
[13] Schedule 1, Part II, paras 2&3
[14] Part III, sections 16-18 & 20
[15] Section 16(1)
[16] Section 21(1)&(2)
[17] R v Chief Constable of North Wales Police, ex parts AB [1998], 3 All ER 310, Woolgar v Chief Constable of Sussex Police [2000] 1 WLR 25

SECTION 4

REACTIVE DUTIES PART 1 – SUBJECT ACCESS

WHAT IS IN THIS SECTION?

INTRODUCTION

125. Most of HSE's data protection activities will occur day to day and be reactive in nature. These reactive duties are likely to be in areas where HSE must be prepared to respond to requests from the *data subject* (and third parties), usually within a statutory timescale.

126. The reactive duties comprise:

- Granting individuals access to their personal and/or sensitive data that HSE holds on them.

- Respecting and responding to the other data protection rights of individuals where appropriate.

127. These occur only when a request is made to us. These reactive duties apply to both existing and new, computerised and manual records.

128. This section and the following section deal with the first of these reactive duties, subject access. Section 6 deals with the remaining duties.

SUBJECT ACCESS – WHAT THE LAW SAYS

129. Subject access is the term for the data subjects' right to request details of the information that HSE holds about them. It is this right that is most commonly exercised and the one to which HSE will most frequently have to respond particularly to those involved in civil proceedings (see GAP 14). Therefore, you should become familiar with the guidance set out in the following paragraphs.

130. Most subject access requests are likely to come from litigants or potential litigants who will use the right to acquire information from HSE for the purposes of civil proceedings, and perhaps from HSE staff seeking their personal data from line management, Personnel Division or other parts of Resources and Planning Directorate see paragraph 139. However, it is possible that anyone in HSE could receive such a request.

131. For a step-by-step guide to what to do when you receive a request under subject access, see Annex A; see Annex B for model text to aid responses.

132. The 1998 Act requires that requests for subject access **be made in writing**[14]. Should you receive a verbal request, do not ignore it but explain that the law requires the person to make a written request. Regard faxes and E-mails as written requests. If the person is uncomfortable with providing one (or unable to do so), encourage them to seek help from a friend or colleague, but to add their own signature.

133. It is the responsibility of the Directorate or Division holding the relevant data to respond to requests for subject access. You should take the following steps:

- first satisfy yourself as to the identity of the data subject (e.g. written request giving the same address that we hold, or, in very occasional cases of greater doubt, perhaps a phone call confirming personal details such as date of birth if we hold it);

- then check that the data subject has given you sufficient information for you to locate the relevant data (e.g. date of accident, name of employer) - if necessary go back and ask for more specific information;

- comply with any written request - or indicate your reasons for not doing so - within 40 calendar days of receiving the request and sufficient information to locate the relevant data;

- offer to correct any inaccurate data (see paragraphs 276-282).

134. Having received a subject access request, you **must not** make any amendment or deletion to the data, simply to make the data more palatable to HSE.

135. There is no need to mention the Act in the subject access request. If a data protection request is incorrectly made under the Freedom of Information Act, you should treat it as a data protection request[2]. If a Freedom of Information request is incorrectly made under the Act, treat the request under the FOI regime.

Health records

136. Requests for access to personal data relating to living individuals fall under the Subject Access Provisions of the Act. Such data will be considered as sensitive personal data. Access to the health records of the deceased falls under the Access to Health Records Act 1990. If using the exemption to subject access provided in the Health Order[3], you must consult the health professional responsible for the care of the data subject, and if there is more than one, the most suitable.

Charging arrangements

137. The Act allows data controllers to charge a fee for responding to a subject access request. This fee cannot exceed **£10**, however much personal data is requested. It has been agreed that HSE will not charge for subject access requests at the present time, although this decision will be reviewed at appropriate intervals

Failure to comply

138. Failure to comply with a request for subject access contravenes the sixth Data Protection Principle. A data subject may ask for a court to order compliance with a subject access request where HSE has refused it without legitimate reason and the application of an exemption.[4]

139. Should a data subject complain to HSE, follow the instructions given in paragraphs 195-204, which set out the data protection complaints procedure. A separate complaints procedure for HSE staff can be found in Chapter 12 of the Staff Handbook.

Documenting decisions

140. Any decision to apply an exemption (either to withhold data to a data subject or to release data to a third party) should be documented. This record of the decision may be used in the case of a complaint.

REQUESTS MADE IN A LANGUAGE OTHER THAN ENGLISH

141. You may receive a subject access request from an individual for whom English is not a first language, or who may use a preferred or chosen language (e.g. Welsh).

Welsh

142. The Welsh and English languages should be treated equally in the service we provide to the public in Wales. HSE is committed to its responsibilities in complying with the requirements of the Welsh Language Act. A copy of HSE's Welsh Language Scheme is available from the Welsh Language Unit (Contact: Dave Williams, FOD Wales and South West, Government Buildings, Cardiff).

143. Under the Scheme, letters received in Welsh should receive a signed reply in Welsh. It has been agreed with HSE's Welsh Language Adviser that covering letters dealing with responses to subject access requests should be treated in the same way.

144. Annex B provides a translation of the model letters that should be used in response to a subject access request. However, most letters will be unique in that they will refer to the purposes of use and the personal data specific to the individual making the request.

145. If you receive a subject access request in Welsh, you should submit your final covering letter to the Welsh Language Unit (Government Buildings, Cardiff, tel: VPN 511 3105) indicating the timescale in which you need a reply. Make sure that you allow sufficient time to still respond within the maximum 40 days, although the Unit is confident of a speedy turn around of translation requests. You can fax your letter to the Unit if a reply is needed urgently.

Other languages

146. If you receive a subject access request in another language, e.g. Urdu, you will need to consider the most courteous and common sense way to reply; there is no legal requirement to reply in the language that the request was made in[5].

Exemptions to subject access requests

Introduction

147. Any mention of a data subject is, potentially, disclosable and a much wider range of material is disclosable under the Act than has previously been the case. Unlike the Freedom of Information Act 2000, the Act has no exemptions for policy advice or internal discussions so this kind of material may also be disclosable where it relates to a data subject.

Protective markings

148. You should also be aware that protective markings that may appear on a document do not, in themselves, have any relevance when dealing with disclosure under the Act. Unless a relevant, appropriate and necessary exemption needs to be applied, personal data from such documents may have to be disclosed.

149. The Act recognises that there will be occasions when it would not be appropriate to respond to a subject access request so it offers a number of exemptions that allow you to refuse a request.

Using an exemption

150. Using an exemption interferes with an individual's rights of access so you need to consider very carefully if an exemption should be used. Do not hesitate from using an exemption if you believe it is the appropriate and necessary course of action. But you must be absolutely sure before you do so. Each subject access request should be handled on its merits.

151. **Important note:** at a glance, these may look daunting and complicated. As with all law, legal provisions can be a bit of a mystery until you are able to understand what they are saying. Remember that the1998 Act is there to protect people's personal information and to ensure that it is only processed by those who are authorised to do so. The exemptions help to define how personal data should be processed in certain circumstances where other needs are considered to outweigh the immediate subject access rights of an individual.

152. When you look at them, the exemptions reflect common sense situations. Some of them will always be applied, such as where the data is processed for research purposes, others only for as long as the data needs to remain exempt, i.e. where there is prejudice to enforcement activities.

153. This section explains the exemptions where necessary and puts them into an HSE context. Your Directorate/Divisional Contact, IMU or, where needed, the Solicitor's Office, are all sources of advice and guidance that are there to help you in more complicated cases.

HSE's policy on exemptions

154. There will be occasions when it will be necessary for HSE to refuse a data subject access to or a copy of their personal data. As explained in paragraph 150 above, it is HSE policy to only apply an exemption when it is considered absolutely necessary to do so. However, where the use of an exemption is both necessary and appropriate, HSE will apply them in accordance with the 1998 Act.

155. Legitimately applying an appropriate exemption is the only way to lawfully withhold personal data.

The exemptions in detail

156. The exemptions below are listed in the same order as they appear in the Act. You are not required to comply with a subject access request if one or more of the following conditions apply. Please read the exemptions carefully:

157. Where providing a copy of the data (in an understandable form) would involve **disproportionate effort**[6].

158. This is not as straightforward as it appears. This exemption is not a replica of the one that is available under the Code of Practice on Access to Government Information, or the one that appears in the Freedom of Information Act 2000.

159. This exemption applies **only** to **providing a hard copy** of the personal data requested. It does **not** apply to the searching, gathering, or collating. If you are aware that the request is likely to involve a considerable amount of data and this exemption may need to be applied, then it is advisable to ask the data subject at the outset to be as specific as possible about what data is being sought. It is acceptable under the Act to go back to the data subject to pursue this. If the data subject continues to request a full set of their data and there is just too much data to

reasonably copy, then you should consider allowing access in another way - i.e. sight access. This means considering whether it is reasonable to invite the data subject into the local office or Headquarters to see the data we have on them.

160. This exemption applies to the "effort" involved in providing hard copy, not the cost. The use of this exemption should be considered on a case-by-case basis. What may be appropriate in one case may not be appropriate for another.

161. This exemption should not be confused with the exemption that, since January 2005, has applied to unstructured manual data[7].

162. Where there are **repeated and identical or similar requests**[8] from the same data subject, unless a "reasonable interval" has elapsed between requests.

163. When deciding what comprises a "reasonable interval", consider the nature of the data, the purposes of processing, and how frequently the data is amended. This will need to be decided on a case-by-case basis. A short "reasonable interval" would include where a record is being added to regularly, and the data subject wishes to know whether any new data has been added. You should grant a request in such circumstances.

164. Where **information to be disclosed would include personal data relating to another individual**[9] (unless the other individual has given his consent or it is not reasonable in the circumstances to obtain this consent - see paragraphs 207-210).

165. Where possible, disclose the information in such a way as to ensure that other individuals cannot be identified from it. It may be easier to extract the data being requested rather than to redact (edit) the record.

166. Where there is prejudice to **national security**[10], e.g. certain personal data concerning nuclear issues.

167. Where there is prejudice to the **prevention and detection of crime, apprehension and prosecution of offenders**[11], i.e. high-level enforcement action.

168. This exemption is only applicable when prejudice actually exists. There is unlikely to be any prejudice once proceedings are complete, including any appeals proceedings, or a decision not to prosecute was taken. You will need to decide on a case-by-case basis whether releasing information on past reports could prejudice any current enforcement action. If you have any doubts or are unsure of how to proceed, you should consult the Solicitor's Office.

169. Where there is prejudice to **health, safety and environmental regulatory activity**[12],

- i.e. low level enforcement, e.g. notices, licensing and permissioning regimes, approvals and certificates of exemption.

170. Where data are processed only for **research, historical or statistical purposes**[13].

171. This exemption can only be applied where the processing complies with the rest of the Act, that is to say the Data Protection Principles; and providing the results do not allow any data subject to be identified, directly or indirectly.

172. Where data are processed for the purposes of **management forecasting or planning**[14], and disclosure would prejudice the data controller's business or other activity.

173. Where data are processed for the special purposes of **journalism**[15].

174. Please note that HSE does not process personal data for journalistic purposes. However, we do have considerable dealings with journalists and the media which may involve the personal data of both those individuals injured or made ill by their work or a work activity, or individuals (self-employed, sole traders, business partners) who have breached health & safety law.

175. Each case will need to be looked at. However, we can disclose the personal data of individuals who have breached health and safety law, where there is a clear health, safety or environmental reason for doing so - i.e. where HSE believes that it is in the public interest to disclose the information. In these circumstances we can do so as such action may be considered to be for the purpose of our functions. Our notified purposes allow us to do this.

176. **This advice is based on disclosure after the appeal period for a prohibition/improvement notice has expired. If you are considering the disclosure of this personal data before the appeal period has expired, you must seek the advice of the Solicitors Office. No disclosure should be made where there are existing or potential criminal proceedings, and where the appeals period for such proceedings has not expired. Nor must we disclose personal data relating to an acquitted person or to a person whose appeal has been successful. It is important that we do not potentially prejudice such proceedings. Again, if you are considering disclosing personal data in such circumstances, you must seek the advice of the Solicitors Office.**

177. Disclosure of the personal data of an individual injured or made ill by their work or a work activity to the media is more difficult to justify. It is unlikely that there will be health, safety or environmental purpose for releasing such information. Remember that we can only process personal data for the Notified purposes; we can only disclose personal data for those same purposes. **You should seek the advice of the IMU Branch or the Solicitor's Office if you think you may need to disclose personal data in these circumstances.**

178. It is permitted to mention:

- HSE staff by name in any official HSC/E press release; and
- Research contractors, e.g. in connection with any work they have undertaken on our behalf.

179. Where a health practitioner considers that disclosure of the data would be **harmful to the physical and mental health of the data subject**[16].

180. Only a health practitioner (such as a doctor) can make this decision. If you think that this exemption may be relevant to any data that you have been asked to disclose, then you must seek the views of a health practitioner before doing so. This is not to say that only health professionals can handle health records or make decisions regarding disclosure. In reality, where you have reason to believe that it may be harmful to release the data (usually in cases where the individual is unaware of a medical diagnosis), contact IMU for further advice.

181. Where the data consist of records of the intentions of the data controller in relation to any **negotiations with the data subject**[17]

- i.e. in personnel work, where disclosure would prejudice those negotiations.

182. Where **HSE is under a legal requirement to make the data available to the public**[18]

183. Either through publication or making it available for inspection (e.g. some enforcement notices are required to be on public registers under the Environment and Safety Information Act 1988). HSE has set up the Prosecutions Database as a result of a policy decision. We are under no legal requirement to make the data available.

184. Where the data comprise **confidential references**[19] given by HSE for the purposes of actual or prospective education, training, employment or appointment.

185. However, please note that references **received** by HSE from others are **not** exempted by the Act. An employment reference may be marked 'in confidence' and, while this should be carefully considered if the reference forms part of a subject access request, such a marking does not guarantee the confidentiality of the data.

186. Where the data comprise an assessment of the **suitability of any person for office, Honours or Crown employment**:[20]

- Including: judicial office, appointment as Queen's Counsel, or for any state honour.

187. Where the data concern a claim to **legal professional privilege**[21]

188. If you consider this to be the case, then you must contact IMU or Solicitor's Office for advice.

189. Where the data disclosed would be **evidence of a criminal offence by HSC/E or by any individual HSC/E staff member**[22]

- (i.e. the act of disclosure itself not being an offence).

Reasonably foreseeable

190. Although not a statutory exemption, the Information Commissioner has offered the following useful advice. Where the data subject has provided HSE with their data (e.g. the subject access letter itself), it is reasonably foreseeable that the data subject is already aware of the data, how HSE received it and the purpose for which HSE will process it.

191. So, where a subject access request is made, such data need not necessarily be supplied to the data subject but you should still alert the data subject to its existence. If the data subject still requires a copy, then they should receive it.

CONSULTING OTHER DATA CONTROLLERS

192. Some subject access requests may involve personal data that has been disclosed to you by another (separate) data controller. If you hold such data, you will need to decide whether or not you have 'control' over it and if you can process it independently or without reference to the other data controller.

193. If you cannot do so, then you should consult the other data controller before disclosing the data. *You* may consider that there is no harm to HSE in disclosing it, but there may be harm to the processing of that data by the other data controller if you do so.

194. It is unlikely that this will apply very often, as HSE should only have data that is relevant to the notified purposes. If you do have data that is excessive to our notified purposes, then you should make arrangements to destroy the data as soon as possible.

COMPLAINTS

195. When HSE refuses data subject access, third party access or any other data protection rights, it is HSE policy, wherever appropriate, to let the data subject or other individual know why they have been refused, and the avenues of complaint that are available to them.

196. This will not always be the case, of course. There may be occasions when we cannot disclose the exemption as, to do so, would indicate why we have had to apply the exemption in the first instance. In most cases it is likely to apply to the exemption where disclosure may prejudice our ability to prosecute or take enforcement action against an individual duty holder who is also a data subject under the Act (e.g. self-employed or a business partner). If we are considering enforcement action against an individual duty holder, responding to a subject access request from them may prevent our ability to effectively carry out that action.

197. If you consider that this may be the case, you may wish to consult the Solicitor's Office via IMU before taking a final decision.

198. We may also need to avoid citing the exemption that covers the situation where disclosure may affect the physical or mental health of the data subject or another person**. If we alert the data subject or others to the use of the**

exemption, there is the possibility of causing the very result we are trying to avoid. Remember, only a health practitioner can advise when this exemption should be applied.

Statutory routes of complaint[23]

199. The1998 Act sets out two possible statutory avenues of complaint: application to a court or application to the Information Commissioner for an assessment of whether the data controller's processing is being carried out in accordance with the requirements of the Act:

200. Data subjects may bring a civil action pursuant to section13 of the 1998 Act. Compensation may be awarded if damage and/or distress *and* damage have been suffered. Criminal offences under the Act may be tried in the magistrates' court (£5000 maximum fine) or the Crown Court (unlimited fine). Government departments are not liable to prosecution under the Act but individual civil servants may be prosecuted if they are personally guilty of an offence under section 55 (unlawful obtaining/disclosure) or of obstructing the execution of a warrant issued in accordance with the Act (Schedule 9, paragraph 12).

201. Any person who believes that they are directly affected by any processing of personal data may make a request for assessment by the Information Commissioner.

202. The Information Commissioner may serve an information notice requiring the data controller to provide such information relating to data protection compliance in respect of a particular complaint. The Information Commissioner may also serve an enforcement notice if he believes that Data Protection principles are being or have been contravened. In deciding whether to do so, the Information Commissioner must consider whether damage or distress has been or is likely to be caused. Compliance with the notice should ensure compliance with the 1998 Act.

HSE's complaints policy

203. In addition to the statutory routes of redress, HSE can offer people refused under the Act the opportunity to request an internal review of our decision. All DPA appeals must be made through the IMU and submitted in writing (fax and email are acceptable). The IMU will act as secretariat and appellant contact points for all appeals. The IMU will detail all stages of the appeal on the tracking system. The review will be carried out in accordance with the FOIA appeals procedure except for the fees regime(see GAP 1, paragraphs 98 - 108 . This procedure would be available to external complainants only. **A separate, internal complaints procedure for HSE staff can be found in Chapter 12 of the Staff Handbook**.

204. Whenever a refusal is made, those refused must therefore be told that:

- they can apply to HSE for an internal review of our decision (via the IMU Data Controller to an independent SCS Appeals officer,); and

- alternatively, they can apply to a court or ask the Information Commissioner to carry out an assessment of whether our refusal was in line with the requirements of the Act.

Please note: we must <u>not</u> give the impression that an internal review, for either external enquirers or HSC/E staff, is a step that must be followed before other avenues of complaint are available. It is only an alternative and data subjects are under no obligation to use it.

[1] Section 7(2)& (3)
[2] FOIA2000, Section 40(1-7)
[3] Health (The data Protection (Subject Access Modification)(Health) Order 2000 (SI 2000, 413)
[4] Section 7(8)&(9)
[5] According to a letter received by HSE from the OIC (31st October 2002), the Section 7(1)© requirement for communication of personal data in response to a SAR "…does not refer specifically to providing a translation of the personal data into another language…the Commissioner's view is that the question of intelligibility applies to such things as codes and technical and medical terminology rather than to other languages…Some data controllers [may] wish to go beyond this minimum requirement"
[6] Section 8(2)(a)
[7] Section 69(2) FOIA inserts a section 9A to the DPA whereby manual data held by public authorities comes under the 1998 Act. 9A(3) says that a public authority is not obliged to comply with 7(1) of the Act (Subject Access) 'in relation to the unstructured personal data if the authority estimates that the cost of complying with the request so far as relating to those data would exceed the appropriate limit).
[8] Section 8(3)&(4)
[9] Section 7(3),(4),(5)&(6)
[10] Section 28
[11] Section 29(1)&(2)
[12] Section 31(1)&(2)(e)(f)
[13] Section 33
[14] Section 37 and Schedule 7
[15] Section 32
[16] Health (The Data Protection Subject Access Modification)(health)Order 2000 – SI2000 No 413: The Health Order
[17] Section 37 & Schedule 7, para 7
[18] Section 34 (1)
[19] Section 37 & Schedule 7, para
[20] Section 37 & Schedule 7, paras 3&4
[21] Section 37 & Schedule 7, para 10
[22] Section 29
[23] Part V

SECTION 5

DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

WHAT IS IN THIS SECTION

INTRODUCTION

205. If you receive a request from an individual who is seeking access to personal data that is not their own (and they are not acting on behalf of the data subject/s), that individual is considered a "third party" under the terms of the 1998 Act. A "third party" is someone other than the data subject, the data controller (or sections of it) or a data processor carrying out work on behalf of the data controller. Ministers, government departments and other regulatory bodies are all examples of third parties for the purposes of disclosure of personal.

206. Personal data can, however, be freely transferred **within** HSE and to a data processor that HSE is using to do processing operations on its behalf.

207. You must **not** release information to the data subject from which another individual can be identified (including being the source of the information), unless one or more of the following conditions applies[1]:

- the other individual has given his explicit, unambiguous and informed consent to disclosure. Send a letter by recorded delivery, and with advice of delivery, to the other individual, if you have their address, stating that they have 15 calendar days to reply. Unlike FOI requests, however, **you should not accept a non-response from the individual as their implied consent to disclose personal data.** If you do not receive a reply within 15 calendar days, you should view your request for consent as being denied. You should also consider what other steps you could/should take to seek explicit consent.

For example, have you attempted to telephone them (if you have their telephone number)?

- Or it is reasonable to comply with the request without the consent of the other individual (consider the duty of confidentiality to the other individual, how much effort you have put into obtaining consent, whether the individual is capable of giving consent, or any refusal of consent, or the absence of a reply from the individual).

208. The Information Commissioner has indicated that overriding a refusal to give consent is expected only to occur in *exceptional* circumstances. Therefore, you should consult the IMU in all cases where you are considering using this provision before you do so.

209. Where neither of the two conditions in the paragraph above applies, provide as much of the information as possible without permitting the other individual to be identified either directly or indirectly or, where possible, disclose the information in such a way that the other individual cannot be identified from it.

210. You may find it easier to *extract* the personal data rather than *redact* (edit) the records containing the data. An individual is entitled only to *their* data under the Act, not to the data of anyone else

Important note: the guardian of a child under 14 (or under 12 in Scotland) or of an incapacitated person counts as a data subject, not a third party, for the purposes of disclosure of personal data; treat their requests as under subject access.

You will however need to establish that the person in question is executing a legal duty and therefore has the right to act as a guardian or attorney. The level of safeguards that you put in place to satisfy yourself of the status of the representative will depend on the nature of the data in question; the more sensitive the data, the greater the level of documentation you will need to see. If in doubt, contact IMU.

ENVIRONMENTAL INFORMATION REGULATIONS 1992[2]

211. The absolute prohibition on the disclosure of personal data without the data subject's consent in the Environmental Information Regulations 1992 remains in force. This prohibition is not affected by the exemptions to the non-disclosure provisions mentioned below. Therefore whenever personal data is also environmental information as defined in the Regulations it cannot be disclosed under any circumstances without the data subject's consent save where a court ordered us to disclose it.

DISCLOSURE OF NAMES OF OFFICIALS[3]

212. Where a data subject is entitled to receive personal data that includes information relating to a minister or an official acting in an official capacity, you should carry out a balancing exercise to decide whether the information relating to the minister or official should be disclosed. This includes taking account of the circumstances of the particular case and, where necessary, consulting the individual concerned.

213. A blanket policy of non-disclosure of the names of ministers and officials in every case is unlikely to be justified. Equally, the names of officials should not be routinely disclosed, except where those names have been previously disclosed, or where they are required to appear in official press releases etc.

214. This balancing exercise should be based on three questions:

- Was the minister or official involved in any decisions relating to the data subject (remember, expressions of opinion about the data subject, or about the data controller's intention towards them - a line manager's role would be included here - are to be considered personal data and should be disclosed)? If so, you should consider:
    - What will be the impact on the data subject if the minister's or official's personal data is disclosed; and
    - What will be the impact be on the data subject if the minister's or official's personal data is withheld;

215. Because ministers are in the public eye, there is likely to be an expectation that their names will be disclosed from time to time without consent. Therefore, in making a judgment whether to disclose or not, it may be reasonable to be more open in disclosing the names of ministers than those of junior officials.

216. Names may be blanked out where it is reasonable and the intelligibility of the data is not affected.

DISCLOSURE OF 'POSTHOLDER' INFORMATION

217. Where someone is referred to because they hold a particular post - e.g. secretary to a committee, or through a post they hold in a company, you do not have to seek consent nor, in usual circumstances, delete their data. Where the reference to that third party is clearly related to their acting in an official capacity they can be said to be a postholder. Postholder details are widely considered to be outside the intended scope of *personal data* and can be disclosed. This would be the case particularly where the third party has played a part in making an official decision in respect of the data subject - e.g. the data subject's line manager.

218. Remember, expressions of opinion about the data subject, or about the data controller's intention towards them (a line manager's role would be included here) are to be considered personal data and should be disclosed.

REQUESTS FROM A DATA SUBJECT'S REPRESENTATIVE

Data subjects who may be mentally incapacitated or a minor

219. It is unlikely that a mentally incapacitated person or a minor under 14 years old will make a request under subject access. However, it is possible that their representative (e.g. a parent acting on behalf of their child injured on a building site; or a legally responsible guardian) may make a request on their behalf. If you receive such a request, you should consider it in the normal way, replying to the data subject c/o their representative.

220. Unless incapacitated, children of 14 years or older (12 years or older in Scotland) can make their own request.

Disclosure to solicitors, Members of Parliament, trade union representatives etc[4]

221. Sometimes a data subject's representative (for example, by a solicitor or a trade union official) will make a request for subject access. This is often the case for the Field Operations Directorate (FOD). You must be fully satisfied that the representative is legitimately acting on behalf of the data subject before subject access can be granted. To help you, the following would be acceptable proofs of legitimacy:

- a letter from a solicitor on the firm's headed paper and stating that the data subject is the firm's client (FOD offices will probably be familiar with the local solicitors firms it deals with); or

- a letter on headed paper from a trade's union headquarters or local branch stating that the union is acting on behalf of the data subject.

222. If you are in any doubt as to the legitimacy of the representative, you should seek written confirmation from the data subject before granting subject access. The 1998 Act allows you to do this and to seek whatever information you require to satisfy yourself that the request is legitimately being made on behalf of the data subject. The Information Commissioner offers no particular guidance on the lengths to go to for data controllers. The Commissioner's Office has indicated that this is very much a matter for data controllers provided these lengths does not become oppressive or unjustifiably restrictive.

Disclosure Of Sensitive Personal Data To MPs And Other Elected Representatives

223. In order to overcome the need to obtain explicit consent to disclose sensitive personal data to an MP or other elected representative (which may cause difficulties if urgent action is required), the Elected Representatives Order[5] was enacted.

224. It provides a condition for data controllers to disclose sensitive personal data to elected officials and allows elected representatives to process sensitive personal data without explicit consent. **Note: There is no requirement to disclose, merely an allowance.**

225. Where an MP or other elected representative (or their secretary or other assistant) approaches HSE on behalf of a constituent, it should usually be assumed that he/she is acting with the consent of the data subject. A representative may be required to verify his identity if you are not certain of his/her legitimacy (if the letter is from a known address but is asking for a reply to be sent to a different and unknown address, it may be necessary in order to ensure that, for instance a fraudulent request has not been made on forged or stolen headed paper).

NON-DISCLOSURE TO THIRD PARTIES

226. In addition to the statutory bar on disclosure outlined above, the non-disclosure provisions in the 1998 Act place restrictions on the circumstances where HSE can disclose personal data to third parties. As a general rule, **do not disclose personal data to third parties where the disclosure would be inconsistent with the non-disclosure provisions**.

227. The non-disclosure provisions are those provisions in the 1998 Act, which prohibit the disclosure of personal data to third parties. You are not allowed to disclose to a third party where:

- that disclosure would make you contravene one or more of the first five data protection principles (except the requirement that you satisfy one or more of the conditions necessary for processing); or

- you have granted data subjects their right to stop processing (or one or more processing operations) because processing has caused (or is likely to cause) damage of distress; or

- a court has ordered the rectification, blocking, erasure and/or destruction of the data.

228. The last two are likely to be rare occurrences whereas disclosure of personal data, which might be inconsistent with the first five data protection principles, will be a common problem for HSE. The following paragraphs look at how the first five principles restrain disclosure.

DISCLOSURE TO THIRD PARTIES & THE DATA PROTECTION PRINCIPLES

First principle

229. This requires data to be processed fairly and lawfully (see paragraph 79). In particular personal data must have been lawfully obtained and the data subject is usually aware that we hold data on them etc (see paragraph 80). Where you have not carried out these duties, if the personal data has not been obtained fairly and lawfully you must not disclose it to third parties.

Second principle

230. This requires personal data to be obtained and processed only for the specified purposes - in HSE's case, for those purposes that we have notified to the Information Commissioner (see paragraph 82). Disclosure of personal data is just one operation of processing. The second data protection principle requires that the processing of personal data must not be incompatible with the purposes for which you collected it. In deciding whether disclosure of personal data would be compatible with this Principle, the 1998 Act requires that HSE have regard to the purposes for which the person to whom HSE would disclose the data, would use the data.

Third principle

231. This requires data to be adequate, relevant and not excessive in relation to the purpose for which they were collected (see paragraph 83). Do not disclose data that are not relevant or are excessive. Furthermore, either delete the data or take action to either make them relevant or not excessive.

Fourth principle

232. This requires data to be accurate and current (see paragraph 85). You should not disclose data which you believe to be inaccurate or which you consider are out of date. If you know the data to be either inaccurate or out of date, you should take immediate action to ensure its accuracy and currency.

Fifth principle.

233. Personal data should be kept in a personalised form only for as long as is necessary for the purposes for which they were collected (see paragraph 88). If you continue to hold personal data beyond the period necessary, you should not disclose them to third parties (and should take steps to depersonalise or destroy them as soon as possible).

EXEMPTIONS TO THE NON-DISCLOSURE PROVISIONS COVERING THIRD PARTY REQUESTS

234. There are, however, a number of exemptions to the non-disclosure provisions. These are a little different from the other exemptions available in the 1998 Act. Those can be applied to *restrict* or *prevent disclosure,* while these exemptions, when applied, have the effect of *disclosing* data.

235. In general, the exemptions are *allowances* to disclose, not *requirements* to do so. This means that you would have to decide whether you wished to disclose in circumstances where you are allowed to do so. The following gives guidance on where you would normally disclose where allowed to do so:

236. For the purposes of **safeguarding national security**[6]

237. In this case a Minister must sign a certificate certifying that the information is needed for the purposes of safeguarding national security.

238. HSE would disclose personal data in response to such a certificate.

239. Where non-disclosure would **prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders**[7]

240. This is an allowance to disclose, not a requirement. In most circumstances we would disclose requested personal data to the police.

241. Where other prosecuting authorities (for example, the Inland Revenue, the Customs and Excise or the Department of Social Security) are involved and are 'trawling' for information we may decide not to disclose.

242. In all cases under this exemption you should advise the Information Management Unit before taking action as you would for any other refusal.

243. Where the personal data are processed only for **journalistic purposes**[8]

244. HSE does **not** process personal data for journalistic purposes; only for those purposes notified to the Information Commissioner. However, we do have considerable dealings with journalists and the media which may involve the personal data of both those individuals injured or made ill by their work or a work activity, or individuals (self-employed; sole traders, business partners) who have transgressed health and safety law.

245. Each case will need to be looked at individually and no 'rule of thumb' can be established. However, we can disclose the personal data of individuals who have breached health and safety law, where there is a clear health, safety or environmental reason for doing so - i.e. where HSE believes that it is in the public interest to disclose the information we can do so as such action may be considered to be for the purpose of our functions. **This advice is subject to disclosure being made after the appeal period for a prohibition/improvement notice has expired.**

246. Disclosure of the personal data of an individual injured or made ill by their work or a work activity to the media is more difficult to justify. It is unlikely that there will be a health, safety or environmental purpose for releasing such information. **You should seek the advice of the IMU if you think you may need to disclose personal data in these circumstances.**

247. It is permitted to mention:

- HSE staff by name in any official HSC/E press release; and
- Research contractors, e.g. in connection with any work they have undertaken on our behalf.

248. Where HSE holds data only for **research purposes**[9] (including the compilation of statistics) the data may be disclosed, but only for those purposes.

249. HSE would need to assess on a case-by-case basis whether we would disclose in these circumstances.

250. Where **an enactment requires the information to be made public**[10]

251. In this case we must obey the law. An example in HSE would be information on the self-employed, business partners or sole traders in the registers of enforcement notices having public safety or environmental implications, which the Environment and Safety Information Act 1988 requires us to keep and make public.

252. Where the **law requires disclosure**[11] - under an enactment, a rule of law or by order of a court.

253. In these cases we must disclose. The most likely circumstance is disclosure required by a court order - for example, of a witness statement.

254. Where disclosure is allowed for:

- the purpose of, or in connection with, **legal proceedings**[12], including prospective proceedings;
- the purpose of obtaining legal advice;
- the purpose of establishing, exercising or defending legal rights.

SUMMARY

255. The two most important considerations in deciding to disclose personal data to third parties is whether the disclosure would be in line with the second data protection principle (i.e. is the disclosure being made for the purposes for which HSE has collected it) and does one of the exemptions apply?). If the answer is yes, the disclosure is lawful. If not, do not disclose unless one of the exemptions applies.

256. All potential refusals to disclose personal data to third parties **must** be made known to the IMU **before** the refusal is given to the third party. The Unit may also give advice on aspects of such disclosure but the final decision must remain yours.

257. Should a third party complain to HSE about our refusal to disclose personal data, you should follow the guidance in GAP 1, 98-108 ".

[1] Section 7(4),(5)&(6)
[2] SI 1992 No. 3240 as amended by SI 1998 No. 1447
[3] Cabinet Office DP Handbook for Government Departments, part 17 (http://www.cabinet-office.gov.uk/publicationscheme/dphandbook/)
[4] SI 2002/2905: Data Protection(processing of sensitive personal data)(Elected Representatives)Order 2002
[5] the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) order 2002 (SI 2002 No. 2905)
[6] Section 28
[7] Section 29(3)
[8] Section 32
[9] Section 33
[10] Section 34
[11] Section 35(1)
[12] Section 35(2)

SECTION 6

REACTIVE DUTIES PART 2 - OTHER RIGHTS

WHAT IS IN THIS SECTION

INTRODUCTION

258. The right of subject access is by far the most exercised right. More data subjects request access to the data HSE holds on them than in relation to any other right. But data subjects have additional data protection rights, which they can exercise with equal weight. These additional rights are not 'add-ons' to subject access. They are full rights and should be offered the same weight and consideration as subject access. The additional rights are explained below.

RIGHT TO PREVENT PROCESSING THAT WOULD CAUSE DAMAGE OR DISTRESS[1]

259. Data subjects can request **in writing** that we stop all or any part of our processing (e.g. disclosure) concerning their personal data if they perceive that this is causing (or is likely to cause) substantial damage or distress to them or to a third party, and that this damage or distress would be **unwarranted**. The data subject must give reasons for their request.

260. If you receive such a request, you should remember that the damage or distress is in the eye of the data subject so you should consider carefully any representations that are made. We would probably not grant any request where we consider the damage or distress to be trivial (*de minimis*); otherwise we must give it serious consideration.

261. You must respond to the data subject within 21 days of receiving the request, telling them whether you have complied or intend to comply, or - if you do not comply - the reasons for refusing the request. You **must always** advise the IMU if you wish/intend to refuse a request.

262. As with a refusal to grant subject access, where a request to exercise this right is refused, a data subject may take HSE to court. If the court upholds the data subject's case, you must comply with any resulting court order. **If you receive a court order, you should advise the IMU and Solicitor's Office immediately.**

Exemptions to this right

263. There are situations when HSC/E may be able to process data despite causing damage or distress to the data subject[2]:

- you have the data subject's consent to the processing and the consent has not been withdrawn; or
- processing is necessary to carry out a contract to which the data subject is, or is likely to be, a party; or
- processing is necessary to comply with a legal obligation; or
- processing is necessary to protect the vital interests of the data subject (which has been interpreted by the Information Commissioner to mean a "life or death" situation).

The decision to apply one of these exemptions should be taken carefully.

RIGHT TO PREVENT PROCESSING FOR DIRECT MARKETING PURPOSES[3]

264. The data subject can request in writing that we stop processing for the purposes of direct marketing[4].

265. Direct marketing in HSE terms includes sending advertising or marketing material to duty holders who are data subjects, Directorates or Divisions sending out free leaflets (or newsletters) about complying with health, safety and environmental legislation which include information on how to obtain priced publications, or Directorates or Divisions sending out information (whether electronically or by hard copy) on seminars/training events for which a charge will be levied.

266. You must comply with requests from the data subject to remove their name from databases used (whether wholly or in part) for direct marketing - or have a means for preventing personal data included in databases HSE maintains for other purposes (e.g. FOCUS) being used for direct marketing.

267. Ensure that you also delete the data subject's details from other databases used for the purposes of direct marketing.

268. Where a request is refused, a data subject may take HSE to court; you must comply with any resulting court order. **If you receive a court order, you should advise the IMU and Solicitor's Office immediately.**

Exemptions to this right

269. There are **no** exemptions to this right.

RIGHTS IN RELATION TO AUTOMATED DECISION-TAKING[5]

270. Data subjects have the right to request in writing that HSE ensures that no decisions that would significantly affect them are made that are based solely on the basis of the results of automatic processing.

271. Automatic processing employs computer-based marking systems, whereby a certain score results in a certain decision (e.g. inspection rating systems for the self-employed, sole traders and partners; psychometric testing for employment purposes).

272. Directorates and Divisional Data Protection Implementation Plans outlined whether any decisions they take are wholly automated. No plans have indicated this to be the case. Moreover, it is likely that (at least the possibility of) human intervention exists in all decisions taken by HSE. As such it is likely that HSE does not make decisions that would significantly affect data subjects solely on the basis of the results of automatic processing.

273. However, if you do base any such decision on automatic processing, then you must inform the data subject of this. The data subject then has 21 days to request in writing that you reconsider the decision, or base it on non-automatic processing. You then have 21 days to respond.

Exemptions to this right

274. You are exempt from this duty if:

- the decision is taken in relation to considering whether to enter into, or performing, a contract with a data subject (which is unlikely for HSE) or the decision is legally required; **and**

- the decision grants a request made by the data subject or the data subject has been allowed to contest the decision.

275. The data subject may take HSE to court if they consider your decision is not exempt; you must comply with any resulting court order. **If you receive a court order, advise the IMU and Solicitor's Office immediately.**

RIGHT TO HAVE INACCURATE DATA RECTIFIED, BLOCKED, ERASED OR DESTROYED[6]

276. The data subject has the right to request that inaccurate data are rectified, blocked, erased or destroyed. The Act does not lay down the procedure by which a data subject should do this, other than applying to a court to force a remedy on HSE.

277. Remember that the definition of personal data includes opinions. A court has the right to order the rectification (etc.) of any inaccurate data or any expression of opinion based on inaccurate data, and may order compensation if it decides that the data subject has suffered damage.

278. When collecting data (e.g. inspectors making inquiries at the scene of an accident or line managers keeping records on staff), take reasonable steps to ensure the accuracy of the data.

279. If a data subject alerts you to their intention to exercise this right, try to persuade a data subject not to apply to a court without giving HSE the opportunity to deal with the data subject's concerns in the first instance. For example, when you update forms etc to alert people to the provisions of the Act, it is good practice to tell the data subject that you will amend any data HSE agrees are inaccurate. When the data subject requests subject access (see paragraphs –85-87), do likewise. .

280. Where you are satisfied that the data you hold are inaccurate, you should rectify the data as soon as possible and inform anyone to whom you have disclosed the data. Where you are unsure that the data are inaccurate, and you are unable to identify corroborative evidence to support the data subject's request to alter the data, you have the option of adding a supplementary statement to the data saying that, in the view of the data subject, the data should be rectified. Again, you must notify anyone to whom you have disclosed the data of the supplementary statement.

281. Where you are satisfied that the data you hold are inaccurate, you should correct the data as soon as possible and inform anyone to whom you have disclosed the data *(as far as is reasonably practicable*). Where you are unsure that the data is inaccurate, and you are unable to identify corroborative evidence to support the data subject's request to alter the data (as in the case of a disputed F2508 form), you should add a supplementary statement to the data saying that, in the view of the data subject, the data should be rectified. Adding such a note should always be the course of action where the data has been collected as part of an investigation, prosecution or enforcement action – **you may not alter data that could be used in court**. Again, you must notify anyone to whom you have disclosed the data of the supplementary statement. **If you intend to refuse to alter personal data you should advise the IMU before contacting the data subject with HSE's decision. If you receive a court order relating to this right, you should advise IMU and Solicitor's Office immediately.**

282. Remember: Where you have taken advantage of the exemptions to subject access, the data subject will not have received a copy of his personal data and thus will be unable to request any amendments to inaccurate data.

[1] Section 10
[2] Schedule 2, paras 1-4 and 6(2)
[3] Section 11
[4] R(Robertson) v City of Wakefield Metropolitan Council [2002] 2 WLR 889. The decision held that the council could not supply names and addresses from the electoral roll to third parties for the purposes of direct marketing without consent as this would infringe both the 1998 Act and Article 8 of the ECHR
[5] Section 12
[6] Section 14

SECTION 7

DISCLOSURE FOR THE PURPOSES OF LEGAL PROCEEDINGS

WHAT IS IN THIS SECTION

INTRODUCTION

283. HSE is often asked to disclose information for the purposes of legal proceedings (including cases at employment tribunals). Data subjects (or their representatives), or third parties sometimes ask us for subject access.

284. Litigants in legal proceedings have at least the same data protection rights as any other data subject and are entitled to subject access in the same way. This is true whether HSE is a party to a case (for example, when we prosecute someone for breaches of health and safety legislation or when a person appeals against an improvement or prohibition notice) or where we are not a party (for example when an employer is being sued for compensation by someone injured at work).

SUBJECT ACCESS AND LEGAL PROCEEDINGS

285. If we hold personal data on a particular data subject who requests subject access we must grant it unless one of the exemptions to subject access applies. Please remember that section 28 of the HSW Act and other statutory restrictions on disclosure are disapplied in respect of subject access and so those restrictions cannot be applied in such circumstances.

286. If a litigant requests third party access, i.e. for the personal data we hold on someone else, we must reply in line with the non-disclosure provisions in the 1998 Act. These provisions contain an exemption to the general principle of non-disclosure of personal data to third parties where the personal data is wanted for:

- the purposes of, or in connection with, legal proceedings, including prospective proceedings;
- the purposes of obtaining legal advice; or
- the purposes of establishing, exercising or defending legal rights.

287. In general, therefore, third party access should be granted where personal data are requested for the purposes of legal proceedings. However, statutory restrictions on the disclosure of information in other legislation, such as section 28 of the HSW Act, are **not** disapplied in respect of third party access to personal data. Where disclosure is restricted in other legislation, disclosure can take place only under the conditions set in that legislation.

288. Further and fuller instructions on the disclosure of information where HSE is a non-party are contained in GAP 14.

REFUSALS AND COURT ORDERS IN RESPECT OF LEGAL PROCEEDINGS

289. You should advise IMU of your intention to refuse a request before you do so.

290. Where HSE for whatever reason has to refuse a litigant access to personal data, either through subject access or third party access, the litigant can apply to a court for an order for disclosure and if the courts grants an order HSE would have to disclose the data (subject to being granted a ‘stay’ while awaiting appeal).

ANNEX A

WHAT TO DO IF YOU RECEIVE A SUBJECT ACCESS REQUEST

Here we detail the steps you should take when you receive a request for subject access.

THE REQUEST

- Is the request in writing? If so proceed. If the request is verbal, ask for a written request.

- Are you satisfied that the individual requesting the information or their representative are who they say they are? If not, you can ask for as much further information as you think you will need to satisfy yourself as to the legitimacy of the request (e.g. date of birth, middle name etc. (see paragraphs 219 - 225 on representatives).

- Do you have enough information to locate the personal information belonging to the individual? (e.g. that he/she had an accident on a certain date, while working for a certain company). If not, again you can go back and ask the data subject (or their representative) for any necessary further information.

- No fees are payable (see paragraphs 137).

Determine whether we hold the personal data requested. Use the interpretation of what constitutes *personal data* to identify whether we hold such data on the individual.

THE RESPONSE

First check whether any of the exemptions apply. If they do not, you should reply to the data subject using the model letter set out at Annex B. The letter has been agreed to comply with central Government's data controllers' legal obligations so you should only adapt it slightly to reflect your Directorate's or Division's processing activities. Your letter will:

- confirm whether or not we hold the personal data requested;

- give a description of the data (e.g. accident report, name and address details, details of training/qualifications, details of post held and responsibilities, radiation dose data, date of birth, national insurance number etc. This, of course, will depend on why you process the data and what has been requested);

- state the purposes for which we use the data (the purposes for which HSE processes personal data appear in our Notification to the Information Commissioner. See paragraphs 106-111);

- state the categories of Recipient (e.g. central government) to whom we may disclose the data (again, these appear in our Notification);

- confirm whether any automated processing we do will form the sole means of important decisions about them (this is highly unlikely in HSE);

- tell the individual of their right to ask for any inaccurate data to be corrected, and ask that they do this via HSE. This right does not automatically mean that the data will be corrected. The right extends to allowing the individual to ask, but they will need to demonstrate why our records are inaccurate. Where sufficient proof is provided, you should make arrangements to amend your records to reflect the accurate information. However, some records, such as RIDDOR, are statutorily required and we cannot merely amend them even if the individual has provided evidence that the information held is wrong. While we cannot amend the record itself, we must still show the necessary amendments and record why we cannot amend the data. This is best achieved by adding a supplementary statement to the record. Any future decision in respect of the individual should, of course, be based on the up to date, accurate information. For HSE staff, a request to amend inaccurate data should be sent to the relevant part of HSE).

- tell the individual which data they are entitled to under the Act and which can be disclosed to them as a matter of policy in keeping with the Board's broader openness policy (see GAP 1 Annex 1).

If the individual requests a copy of the data. First check whether there is any reason why you cannot let the individual have access to their personal data i.e. do any of the exemptions listed for subject access apply? (see paragraphs 156-189) and paragraph 157 on disproportionate effort). If they do: see paragraphs on *Refusing a request for subject access* below. If no exemptions apply, follow the bullets below:

- Provide a copy of the personal data in an intelligible form.

- This means that you will have to explain all codes (e.g. headings in investigation reports) and abbreviations (e.g. 'IP', 'HSWA' etc.) and give sufficient information to provide context for the sentences that directly mention the individual.

- Provide the data in a form that does not identify any other individual, unless you have the other individual's consent or you have decided that it is reasonable to proceed without that person's consent (see paragraph 101).

- Provide any information we hold on the source of the data (i.e. who supplied it to us).

HOW TO HANDLE AN OPEN ENDED REQUEST

Some subject access requests might say, “give me everything you have on me”! Despite the emphasis on responding to a request, the Act recognises that data controllers need to be able to approach such requests sensibly. You cannot ignore the request, but you can quite legitimately ask the data subject to be more specific about what they actually want. In fact, the statutory 40 day response time does not begin until the data controller is satisfied that it has sufficient information from the data subject to begin a search for their data.

If you receive an open-ended subject access request**,** you should go back to the data subject as quickly as possible and ask for further information that will help you to refine your search and compilation. A model follow-up letter appears at Annex C to help you to do this. You should adapt the letter where needed if the data subject has some knowledge of HSE and its activities.

Points to note in determining what further information the Department “Reasonably requires”:

- It is unreasonable to expect someone to be able to provide information they do not possess – for example, people outside the department are unlikely to have knowledge of the structure of records within divisions.
- It is reasonable to ask for general pointers such as dates and locations
- If a request comes from someone with knowledge of how the Department works (i.e.: employees), it may be reasonable to ask for further information about the likely location of the personal data.
- It *may* be possible to ask <u>why</u> a person believes that their data are being processed if it is reasonably required to help locate the data.

REFUSING A REQUEST FOR SUBJECT ACCESS (EITHER IN WHOLE OR IN PART) BY APPLYING AN EXEMPTION

You need to be absolutely sure that applying an exemption is the appropriate and necessary course of action. The decision to apply an exemption is yours. You are best placed to understand the context of the processing that you do and what the impact would be, if any, if the data subject were to have access to their data at this particular time. If the data subject challenges HSE’s use of an exemption, the refusing Directorate or Division will need to justify the decision that was made.

Once you have decided that you will need to apply an exemption, you should advise IMU of what you intend to do <u>before</u> refusing any part of the request. Remember, the Branch’s role is not to authorise the use of an exemption - that is for you. But the Branch can offer advice on the consistent use of exemptions in HSE. If the Branch believes that you are considering the exemption inappropriately, you will be asked to reconsider your decision.

If you are using the correct exemption and you consider it appropriate and necessary to do so, you should:

- fully document the reasons for the refusal;

- tell the individual that you are unable to release the data, and the reason(s) why this is the case; i.e. the exemption that is being applied. You do not need to go into too much detail. The exemption should only relate to the part of the request that you are refusing. If you can release other personal data, then you must do so;

- advise the data subject that they have the right to challenge this decision through HSE's internal complaints procedure (see paragraph 203), through the Information Commissioner or the courts.

ANNEX B

MODEL REPLY TO A SUBJECT ACCESS REQUEST

Dear

Thank you for your letter of [...date.....] to the [...D/D.....], received on [... date.....], making a subject access request under the Data Protection Act 1998.

[Delete as appropriate]

[D/D] has checked its records and holds no personal data to which you are entitled under the Data Protection Act 1998.

Or:

I can confirm that personal data in relation to you are being processed. Listed below are extracts from the records that are held showing the data to which you are entitled to under the Data Protection Act.

If appropriate:

[It is HSE policy to be as open as possible with people when they ask for their personal data. Although not covered by the Act, listed below are further data relating to you that we are disclosing in line with HSE policy.]

The data are in no particular order and the period covered by our search was from [ ] up to the date your request was received.

[Some of the personal data we hold on you identifies one or more other individuals. We have not disclosed such information unless we have had the explicit or implicit consent of the individual concerned or we considered that it was reasonable in all the circumstances to disclose it without their consent.]

[The data are held for use in connection with [... You will need to set out which of the notified purposes you process the data for...]. Recipients of the data we hold may include [... You will need to detail the relevant Recipients from HSE's Notification as are relevant to the purposes above...].

[It is not currently the practice of HSE to charge for subject access requests made under the Act [, and I am returning your [cheque for £10].]

If you are dissatisfied with the response, you may do one or more of the following:

a. reply to me at the address below setting out your concerns or appeal and how you think HSE may be of further help to you;

. Write to the Information Management Unit (IMU), Magdalen House, Stanley Precinct, Bootle Merseyside, L20 3QZThe IMU oversees HSE,s appeals procedure; or

b Complain to a court or the Information Commissioner if you are not satisfied with the response you receive from HSE. The address for the Commissioner is:

Information Commissioner
Wycliffe House
Water Lane
Cheshire
SK9 5AF

Fax number: 01625 524 510

Tel number: 01625 545 745 Switchboard: 01625 545 700

E-mail: data@dataprotection.gov.uk

DX: 20819 Wilmslow

Yours sincerely

ANNEX C

MODEL LETTER SEEKING FURTHER INFORMATION/PROOF OF IDENTITY FOR OPEN-ENDED REQUESTS

Dear

Data Protection Act 1998 - your recent subject access request

Thank you for your letter of _____

You will be aware that most government departments hold large sets of data which are covered by the Data Protection Act 1998. It would assist us in locating any personal data held on you in HSE if you could give us some indication of the type of information that you believe we may be holding on you. It would be helpful if you could indicate whether you believe a particular part of HSE is holding data on you, or whether your request is in relation to a specific incident, or correspondence on a particular matter.

I would also be grateful if you could provide us with proof of your identity. A photocopy of the relevant page of your passport and a copy of a recent utility bill would be acceptable. Please let me know if this causes any difficulties.

We require the above information under section 7(3) of the Data Protection Act 1998 which states that "where a data controller (a) reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks, and (b) has informed him of that requirement, the data controller is not obliged to comply with the request unless he is supplied with that further information".

HSE is a data controller. We need to be sure about the identity of an individual who asks for their personal data to ensure that we disclose the correct data to the correct individual.

Thank you for your understanding in this matter. I look forward to hearing from you.

Yours sincerely

ANNEX D

SUBJECT ACCESS - REDACTING (EDITING) OR EXTRACTING TEXT

Under section 7(1)(c)(i) of the DPA an individual is entitled as part of his subject access request to:

> "have communicated to him in intelligible form … the information constituting any personal data of which that individual is the data subject …".

The right of access is therefore to the personal data, not to the document in which the data is contained. Since usually only part of a document will contain personal data, you have probably been either providing documents that show the relevant personal data with the remainder redacted or blocked out, or
extracting the relevant personal data and constructing a digest of extracts.

You will need to decide whether to provide extracts or redacted material in each individual instance, depending on the nature of the case. Either approach will be acceptable.

While both methods of providing a data subject with personal data (i.e. documents that have been redacted or extracts from documents that have been typed out) are acceptable, the provision of personal data in the form of extracts is often preferable in presentational terms. This is, however, resource intensive and you will need to determine which method (or a mixture of the two) is appropriate on as case-by-case basis.

To help you make your decision, you may find the following useful:

- the resource and cost implications;
- the amount of information from a document to be released, i.e. where one method offers the only sensible option;
- the option that offers the best chance of avoiding accidental disclosure of irrelevant, third party or exempt information; and
- the presentational aspects of the proposed method.

For example:

The relevant part of a letter between officials dated 1/1/04 reads:

> "Please provide advice for [name withheld] on (name of data subject) and a draft reply to his letter."

Our correspondence records show that we received 50 letters from you between 1/1/03 and 31/12/04. We no longer retain copies of your letters or our replies".

The relevant part of a letter from an official to a Minister dated 1/1/04 reads:

> "I recommend that you write to [name withheld] setting out your views on (name of data subject)."

The relevant parts of an e-mail between officials dated 1/1/04 reads:

> "We have been informed that (name of data subject) has written to the Minister ……. and that he intends to make a formal complaint."

ANNEX E

DEFAMATION: LIBEL & SLANDER

DEFINITIONS OF DEFAMATION

You should be on guard against making statements, which could be defamatory. A defamatory statement is one that injures the reputation of another person: “it tends to lower him in the estimation of right-thinking members of society generally”[1]

Such a statement constitutes a ‘libel’ if it is:

- published (publication for these purposes is simply the communication of the defamatory matter to a third person); AND
- it is in writing, printing or some other permanent form.

A statement will amount to ‘slander’ if it is:

- published; AND
- made orally or in some other transient form

An action for defamation can be brought by:

- an individual;
- a company, in respect of statements that damage its business and reputation

An action for defamation many not be brought by a Local Authority.

DEFENCES TO DEFAMATION

There are a number of defenses to an action for defamation including:

- the words complained of are true in substance and fact;
- the statement is protected by absolute or qualified privilege
- the statement constituted fair comment on a matter of public interest; that is, opinion which any person could honestly hold based on the facts known to them
- The words were published innocently by a person not the author, editor or publisher, who took reasonable care in relation to its publication and did not know or have reason to believe that this was defamatory and an ‘offer of amends’ has been made. It will constitute a defense if the offer was made as soon as reasonably practicable

Absolute privilege attaches to:

- Words spoken in the ordinary course of legal proceedings;
- A fair and accurate report of public legal proceedings published contemporaneously[2]

Qualified Privilege attaches where:

- The person who makes the communication has a duty to its recipients and they have an interest in receiving it (e.g. where you have sought to publicise a letter containing implications for public safety);
- Where it fairly and accurately reports public legal proceedings that are not contemporaneous.

Statements must not be published maliciously. Reports are published malicious if the publisher knew the report was untrue, was reckless with the truth or intended to injure the complainant.

ANNEX F

BREACH OF CONFIDENCE

INTRODUCTION

English law provides remedies for breach of confidence. A duty of confidence arises when confidential information comes to the knowledge of a person (including public authorities such as HSE) in circumstances where it would be unfair were that information to be disclosed to others (e.g. because the recipient was on notice, or had agreed, that the information was to be so treated).

Breach of confidence is the breach of a duty of care that can give rise to a civil claim. The law governing breach of confidence is complex and if in doubt, you should seek help from Solicitors' Office. A breach will normally arise in connection with the disclosure of information that has a commercial **value but can also include personal information about individuals.**

DEFINITIONS OF A BREACH OF CONFIDENCE

For an action to be successful, it must be established that:

- The information has the 'necessary degree of confidence about it';
- The information was provided in circumstances importing an obligation of confidence; AND
- (for an injunction or declaration to be granted), there was an unauthorised use or disclosure of that information and at least the risk of damage.[1]

The courts have held that the duty of confidence only applies to information not already in the public domain. It does not apply to information that is trivial.

The duty that confidence be maintained may be outweighed by some other public interest factor that favour disclosure, either to the world at large or the appropriate authorities. This may require a court to balance the public interest in disclosure against the public interest in maintaining confidentiality.

Certain public bodies, including HSE, have both statutory (e.g. section 28 HSAWA) and common-law[2] obligations to keep certain information confidential.

Disclosure of confidential information will not be restrained where there is a 'just cause for disclosing it'.[3]

[1] Coco v AN Clark (Engineers) LTD [1969]
[2] For example, photographs taken by police of a suspect under caution or a statement taken under caution
[1] Malone v Metropolitan Police Commissioner [1972]

ANNEX G

THE HUMAN RIGHTS ACT

INTRODUCTION

The Human Rights Act (HRA) 1998 incorporates the European Convention on Human Rights (ECHR) 1950 into British domestic law.

The ECHR sets out a number of rights in its articles. These include:

- The right to life (Article 2)
- The right not to suffer inhuman treatment (3)
- The right to a fair trial (6)
- The right to privacy and family life (8)
- The right to marriage and the family (12)

Not all rights are equal. There are three categories of rights:

- Absolute rights (the right to life). These cannot be infringed no matter how necessary it may seem.

- Limited rights (the right to personal freedom). Specific limitations to these apply such as, in the case of the right to freedom, lawful detention following a conviction.

- Qualified rights (the right to privacy). Infringements need to promote a specific legitimate aim. The law and necessary in a democratic society must properly regulate the infringement. This concept means that the interference with the right must be a proportionate response to a legitimate aim. If the aim can be achieved by another method that would not be so intrusive, the alternative option should be taken.

HOW DOES THE HRA WORK?

Firstly, all legislation must be interpreted and given effect, as far as possible, compatible with the ECHR rights.

Secondly, it makes it unlawful for a public authority to act incompatibly with the Convention rights unless, as the result of a provision of primary legislation, it could not have acted differently.

Thirdly, UK courts and tribunals must take the Convention rights into account in all cases. This means that common law must be developed compatible with the ECHR and Strasbourg case – law must be taken into account.

QUALIFIED RIGHTS

Qualified rights are the most difficult to deal with as they involve the search for fair balance – the interests of an individual as against those of society.

When assessing whether a qualified right is being interfered with, it is important to ask the right questions in the right order. Asking the wrong questions or the right questions in the wrong order will leave your decision open to challenge.

Asking the right questions in the right order may mean starting from a different point than one you may be familiar with.

What are the right questions in the right order?

- Is a protected right involved?
- If so, is there an interference with that right?
- If so, is the interference prescribed by law?
- If so, is it pursuing a legitimate aim?
- If so, is it necessary in a democratic society?

Ahmed v UK (1998)
This is an example of working through the 5 questions.
The political activities of 50,000 local government officers in the UK holding "politically restricted posts" are limited by the Local Government Officers Regulations 1990. The limitations are intended to secure political impartiality. These regulations were challenged in Strasbourg.

Is a protected right involved?

- Yes. The rights to freedom of expression (10) and assembly (11).

Is there an interference with these rights?

- Yes. Political activities are limited by the regulations.

Is this interference prescribed by law?

- Yes.

Is the interference pursuing a legitimate aim?

- Yes. Protecting the right of others – ensuring democracy through impartiality.

Is this interference necessary in a democratic society?

- Yes. The regulations meet a pressing social need, are no more than is necessary to achieve a legitimate aim (i.e. they are proportionate) and are supported by relevant and sufficient reasons.

ARTICLE 8

When dealing with Data Protection issues, it is mostly to be the rights outlined in Article 8 (privacy) that are possibly being interfered with.

Article 8 says that you have the right to respect for your private and family life, your home and your correspondence. You have the right to live your own life with such personal privacy as is reasonable in a democratic society. Any interference must be legitimate and proportionate.

Specifically, Article 8 can include the right to have information about you, such as official records, photographs, letters, diaries and medical information, kept private and confidential. Unless there is a good reason, public bodies should not collect this information.

Any interference with this right:
needs to have a clear legal basis;
must be for reasons of either national security, public safety, the protection of the economy, prevention of crime, the protection of the health and morals or the protection of the rights and freedoms of others;
must be necessary (not just reasonable);
must be proportionate;
and only go so far as what is required to meet the aim.

DPA & ARTICLE 8

The fundamental premise upon which the DPA is founded is that of the Right To Privacy. The Convention right may thus be considered to be rather wider in scope than the more specific rights provided for by the Data Protection Act. It may be contended that the main objective of Data Protection law is to ensure that the fundamental right to privacy is not infringed through the abuse of today's technology.

Because DPA is built around Article 8, proper implementation of the Act should mean that the article is not infringed. However, looking at the ECRH and using the 5 questions above may help in determining whether you are properly implementing the Act.

ANNEX H

DATA SHARING CASE STUDY

To illustrate how the data protection principles should be considered before information is disclosed or transferred:

Take for example, a partnership arrangement that may be aimed at addressing the problem of illegal immigrants on a particular farm. It needs to be decided whose data needs to be shared, and how data sharing might help to tackle the problem.

There must be a lawful basis for processing data. It must be determined whether the type of processing to be carried out can satisfy at least one of the criteria in Schedule 2 of the first data protection principle, which requires that all processing has a legitimate basis. It must also be determined whether the processing will involve sensitive personal data, and therefore which ground in Schedule 3 will be satisfied.

HSE will also need to consider other legal obligations they might owe in relation to the personal data they hold, such as whether they hold it under a duty of confidence. In this case, it needs to be considered whether consent can or should be sought from an individual, and if consent cannot be obtained the authority concerned will need to consider whether there are any grounds on which the need for consent can be overridden.

To satisfy the third principle partners (HSE, the Home office, the relevant police authority) will need to ascertain what categories of information need to be disclosed. Information must be adequate, relevant and not excessive for purpose. Information cannot be accessed or obtained by any person who is not an appropriate member of the initiative.

Appropriate security measures need to be taken to prevent unauthorised disclosure of or access to personal data. The means of making the referral to the initiative should ensure that the information cannot be accessed or obtained by any person who is not taking part in the initiative.

The data protection implications attached to the retention of data will need to be considered, including how the data collection will be notified, how data is to recorded and how long kept, and how individuals will exercise their rights, for example by making a subject access request about their information. The partnership will need to have a mechanism by which subject access requests are considered to determine whether the source authority wishes to rely on a subject access exemption under the Data Protection Act.

Where non-or depersonalised data is used, for example for the mapping of incidences of particular types of offences, the provisions of the Data Protection Act should not apply providing the data does not include identifiable personal information.

ANNEX I

TRANSFERRING PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (SCHEDULES 1 AND 4 OF THE ACT)

You cannot transfer personal data outside the European Economic Area (the 15 EU member states plus Norway, Iceland and Liechtenstein) unless you are certain that the recipient country can offer an adequate level of protection. When determining what constitutes an “adequate level of protection”, consider:

- the nature of the personal data (e.g. sensitive or not);
- the purposes for which and the period during which the data are to be processed;
- the legal protection offered by the relevant country;
- the security measures protecting data in the relevant country.

If you are considering transferring data to countries not in the EEA, please contact the IMU as early as possible. The Data Protection Commissioner has been unable to publish a list of countries that it considers to have adequate data protection legislation, so IMU will help you to make decisions on a case-by-case basis (seeking advice from the Commissioner where necessary).

Essentially, to transfer personal data outside the EEA, the national or international obligations of the country should be similar to those of the EEA in the level of protection they offer to personal data. Consider also the sensitivity of the data, the security measures which will safeguard it, and whether the purposes for which the data will be processed are compatible with the purposes for which you obtained it. If you are transferring data to a nominated data processor, ensure that you have a written contract relating to data protection duties.

Alternatively, consider anonymising the data that you transfer. These data will no longer be personal, and thus no longer covered under the scope of the Act.

Exemptions. Personal data can be transferred abroad without the above requirements being fulfilled if one of the following applies:

- the data subject has given his consent to the transfer;
- the transfer is necessary to carry out a contract to which the data subject is - or is likely to be - a party, or has requested, or which is in the interests of the data subject;
- the transfer is in the public interest (as ordered by the Secretary of State);
- the transfer is necessary for legal proceedings, for seeking legal advice or for defending legal rights;

- the transfer is necessary to protect the vital interests of the data subject;
- the transfer is part of a public register which is being transferred;
- the transfer has been specifically made on terms approved or specifically authorised by the Data Protection Commissioner.