Best Practice Guidance on Data Protection for Systems Designers

Version: May 2002

Draft for Public Consultation

Contents

Best-Practice Guidance on
Data Protection For Systems Designers

About this guidance

1. The purpose of the guidance provided in this document is to communicate guidance on Data Protection to system designers, based on current best practice.

2. The Data Protection Act requires “technical measures” to be taken any person or organization keeping personal data. These guidelines themselves are technical measures, since they are intended to help assure the technical development and operation of a system that will manage personal data. The application of this guidance will not necessarily result in a legally compliant system, although evidence that you have followed the advice in this document would count substantially in your favour, should any Data Protection issue crop up.

3. The legal duty for compliance with the Data Protection Act falls on the Data Controller (the person or organization responsible for the data themselves, normally your client). However, as a designer or developer, you have a professional responsibility towards your client to help them achieve and maintain compliance. This document will help you by prompting your client for the relevant information at the relevant phase of your design and development process.

4. The guidance in this document will allow you to be specific about such issues, ensuring any further advice you seek will receive a concise and relevant answer. If you are in doubt about any particular aspect of your system design, you can contact the Office of the Information Commissioner, the successor to the Data Protection Registrar, by:

email
mail@dataprotection.gov.uk

telephone
01625 545 745

or visit the website
http://www.dataprotection.gov.uk/

5. Where terms have a special significance in the context of this report, they are clarified in the glossary. These clarifications are not authoritative legal definitions and should not be treated as such. Should you wish to see it, the full text of the Data Protection Act 1998 had been made available online at:

http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.html

Data protection and systems development

Confused about Data Protection? Concerned about liability? Confounded by legal advice? This document is for you. These guidelines have been prepared by experts on Data Protection (DP) and on systems development. It should help you know where you stand when you build a system for a client, or for yourself for that matter, and how to build a better product. Data Protection is about looking after people's privacy by making them aware of how information about them is obtained, how it is used and so that it is processed in way that is fair to them. This might be to do with getting a loan to buy a car, admitting them to a club or targeting them for an advertising campaign. The guidelines you'll find here should clear up some of the confusion about how best to build systems that take care of these matters whilst still offering your client an effective ICT solution to their needs.

When faced with design alternatives, we would typically base our choices on a number of factors. One of the central factors in all system design is of course cost containment. We may contrast alternatives by their initial cost; their cost of maintenance following release, and in-house versus external spend. Time to develop is a distinct factor, although intimately related to cost both by virtue of person effort and market value at date of release. Other factors include compatibility with legacy systems, integration with industry-standard applications, extranet interfacing and standards for data exchange, and so on. All phases of implementation must depend on a process of "design rationale" in just this way: linking decisions on design alternatives to the factors that matter for that particular development.

Data Protection Law adds a number of concerns to this decision process. These might in general be described as 'clarity of data partitioning' and 'traceability'. If we have clearly laid-out systems development principles for deciding between alternatives, so much easier will be the process for managing the choices we actually make. Integration of DP Law means that DP concerns become part of design rationale. Looking at DP obligations in this way, it becomes clear that a normal process of quality assurance auditing on a particular development would also support a DP audit. In other words, a documented design rationale stands to be of benefit to the efficiency of the development process, for justification to a customer of the design decisions you have taken and to encourage trust in the client's user base. These guidelines are intended to give you clear principles for guiding your development process.

There are two sections to these guidelines. The first is called **FARSTARS** – it's a mnemonic for **eight systems development principles** (a byte!) that should guide the design decisions you take. The second lists the guidelines themselves in terms of FARSTARS.

FARSTARS

This section describes the principles of data protection that have driven the production of the Data Protection Act[1]. It is intended to help you understand what Data Protection Law is about and why it is relevant to your system design and development process. The Data Protection Act is aimed mainly at people on whom information may be held and at people who may hold information about others. From your perspective, as a systems developer, it may seem as though you are not included. That would be a dangerously misleading assumption on your part.

In effect, you will be acting as the agent of the system commissioner, your client, and so have been delegated some degree of responsibility for compliance with the Act. By understanding what kinds of responsibility there are, you can be clear about how much responsibility you are taking on and how much stays with your client. In general, the more clearly you and your client can set out the kinds of processing to be done, the less responsibility for DP compliance will fall upon your shoulders. This is because, from a systems development perspective, Data Protection Law is about coupling clarity of the purpose of process with a clear delimitation of actual processing.

The principles refer to four essential ideas:

- Personal data: any data that, if possessed by a person or organisation, may be traced to another living person
- Data subject: the living person who is the subject of personal data
- Processing: any operation performed on any data, including but not limited to storage and retrieval, transmission, collation and combination with other data
- Data controller: person or organization that processes personal data.

Ownership of personal data can be a complex issue. The important thing for you to know is that individuals always retain rights over information about them. We are not concerned with ownership of information here. The Data Subject may pass on permission to process their personal data but they do not pass on ownership. Any person or organization who obtains permission to process personal data then has a duty to the Data Subject to take good care of that Data Subject's personal data.

These four ideas recur in each of the eight systems development principles[2]. An acronym, FARSTARS, should help you to remember the eight principles. It stands for Fair Adequate Rights Specific Transfer Accuracy Retention Security. Each of principle is explained below:

[1] *The full text of the Data Protection Act 1998 is available online at:* http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.html

[2] *The eight systems development principles* ***are not the same*** *as the data protection principles, although they are related to them. The systems development principles are based around an idealized development cycle.*

FAIR collection –

Personal data must be obtained by giving Data Subjects an honest account of why you want that information. Besides the Data Subjects themselves, personal data may also be obtained from intermediary agencies as long as they have in turn permission to pass on such information. Collection of personal data must be lawful: you can't mislead potential providers of personal data about your reason for wanting these data and you can't ask them for data that break any laws.

There are several conditions for being allowed to collect personal data. These are set out in a part of the Act called 'Schedule 2'. Ordinarily, the Data Controller must be able to meet at least one of these conditions. It also means that personal data cannot just be reused for anything at all after it has been obtained, if that means processing beyond the original reasons for its collection. Some kinds of personal data require additional care, termed 'sensitive personal data' by the Act (See Appendix 4). You should make sure that the data controller has thought about this and ask them to explain how they have met the conditions for its lawful collection. These conditions are to be found in a part of the DP Act called 'Schedule 3' (See Appendix 3). They are separate from the conditions on processing normal personal data. The Data Controller must meet at least one of these, on top of the conditions for processing normal personal data.

ADEQUATE collection –

You need to obtain *enough but no more* personal data so that your work can be done properly. There is such a thing as collecting too little information about people, as well as collecting too much!

RIGHTS to know –

People have a right to see any information you have about them. If they write to you requesting to see such information, you must satisfy their request for ALL the information you hold about them. Even if it isn't easy to find everything! Furthermore, should a Data Subject decide to refuse to give or later to recind permission for you to keep or to use in their personal data in a particular way, you may be obliged to honour their wishes. You must be able to immediately set in train a process to remove and destroy all relevant personal data from your systems.

SPECIFIC purpose –

You are collecting data for one or more purpose, connected with the aims of your organization or business. So you have identified a need for the personal data in terms of your organization. Personal data can never be separated from these purposes, even if they might be useful for the aims of your business in other ways later on. You are always limited in your use of personal data, unless you have "exceptional lawful authority", for the purpose you stated and compatible purposes when those personal data were obtained. You may never use personal data for unlawful purposes, of course, but should be careful always to do the minimum processing necessary in order to meet the organization's stated purposes. You can of course go back to the Data Subjects at any time to explain why you want to use their personal data in different ways.

TRANSFER of personal data –

Although personal data is not regulated in the same way all over the world, within the European Economic Area (EEA) the rules are essentially the same. That means you can move personal data around the EEA by whatever means, as long as you stay within the provisions of the law or else satisfy one of the conditions of for this kind of processing (See Appendices 2 & 3). The rules in other parts of the world, such as the USA and India, are not the same and so you should check an approved list[3] before allowing transfer outside the EEA of any personal data under your control.

ACCURACY of personal data –

You must take reasonable steps to ensure that personal data is accurate at the time it is collected. You must then keep it up to date, if it is to be retained, so that any processing you gives good results. Remember: rubbish in, rubbish out. It is your responsibility to maintain this accuracy, not the responsibility of the Data Subject.

RETENTION of personal data –

When you ask somebody for their personal data, you do so for a reason (see SPECIFIC). For any purpose you might legitimately have, you should also be able to say for how long that purpose is to be valid. Some purposes may need the personal data for only a few weeks, while others may need the personal data for a number of years. Just as you should be prepared to justify collection of personal data for a specific purpose, you must be able to justify the retention period on the basis of need. You cannot just decide to keep all personal data forever, 'just in case'. At the end of the identified retention period, you must either renew your permission to keep those data or else you must destroy them. These considerations should be brought together into a time schedule for managing personal data within the system you are designing.

SECURITY of personal data –

Once you have obtained personal data, in the spirit of all the other principles above, you must then make sure that you take care of it. This duty of care towards the Data Subjects, in trust of their personal data, means having secure systems for processing and also secure procedures for using such systems. Security is not only about stopping outsiders getting in to your systems, or intercepting messages between legitimate users of the personal data under your control. It is just as much about restricting access to data within your organization. It is also about making sure of the integrity of the personal data in your care, so that ACCURACY is not compromised by, for example, accidental corruption. SECURITY follows on from a clear definition and delineation of SPECIFIC purposes and also from good data management practices.

[3] See http://www.dataprotection.gov.uk/

The Guidelines

1 Contract and Requirements

The first stage of your development involves establishing what your client wants you to develop. This involves a contractual responsibility on your part to ensure that you properly understand the intention and the scope of the development. It also places a responsibility on you to establish *necessary* processing. Necessary processing covers anything that is being done for a clearly specified purpose, relevant to the client's business. That means setting out clearly what your client wants to know about the people on whom they are to hold information and why they want to know it.

On the one hand, this means that you should establish how and why the client wants to aggregate general, impersonal data. On the other, there are the ways in which your client may wish to pull together aspects of the information they hold about a particular individual – a "Data Subject". Both kinds of processing can have significant consequences for Data Subjects and so should be include quite explicitly in your considerations at this stage.

Your client may not know very much about the Data Protection Act, so you cannot rely on them only to ask you to do things allowed by law. You must ask them to be as clear as possible about these matters and to put it in writing. That way, it will be clear that the client is not collecting personal data in an ad-hoc way, but that they are doing so for a specified purpose. It will also be clear that they are taking responsibility for decisions about the extent and purpose of personal data to be collected. This is important as there are a number of alternatives in DP Law. These alternatives can mean that permission does not have to be sought from Data Subjects before their personal data are processed. Where your client believes this applies, they should state this to you clearly, identifying the relevant alternatives.

Before you start:

Obtain a copy of and relevant Codes of Practice for the industry sector associated with the proposed system[4]

Obtain the name and contact details of the Data Controller or person responsible on behalf of the Data Controller for the development of this system[5]

Develop procedures that will ensure that all actions regarding data protection are fully documented

What you need from the Data Controller:

A written specification of the period of validity of the data to be collected

A written specification of the purposes for which all personal data (in the scope of the system) are to be collected

A written specification of the review period associated with the purposes of the data collected

[4] *The term 'proposed system' refers to the system you are proposing to develop i.e. the system under consideration at the time of reading this guidance.*

[5] *See Appendix 6 for definition of Data Controller.*

Work with the Data Controller to:

Agree a procedure for assuring the validity of the data. (e.g. if communication is made with the Data Subject at a specified address and no response is obtained after 30 days then assume that the contact details are invalid and delete the record)

Agree on the wording of a Privacy Statement to be made available to potential and actual Data Subjects (see Appendix 5 for further guidance). This might be presented to Data Subjects as a page on a website, a spoken statement by a telesales operative or part of a letter sent out to potential clients.

1.1 Fair

Identify what personal data is to be collected:

- Ensure that the data can be fairly collected i.e. without the Data Subject being misled or deceived about the purpose for which the data is being collected (See Appendix 2).
- Ensure that you know the specific conditions laid down for use of personal data containing a personal identifier (e.g. NI or NHS number)
- Ensure that you have identified whether personal data supplied by children (under 12 and under 16) will be treated differently

Ask the client for copy of their strategy for informing Data Subjects about the reasons for collecting personal data.

Where the client has identified more than one purpose for collecting personal data, ensure that they have clearly identified levels of permission to be given by Data Subjects.

Make sure that the client has identified any sensitive personal data if there are any among the data they wish to collect (see Appendix 4) and, if so, that the special conditions can be met (see Appendix 3).

1.2 Adequate

Insist that the client specifies the collection of *sufficient* information in order that the processing can produce valid results.

Ensure that all the data specified by the client are in fact *necessary* to carry out such processing.

1.3 Rights

Obtain from the client a statement that details how your development will interface with their other systems and processes.

Obtain from the client a statement of their intended strategy for honouring the right of Data Subjects to remove or to prohibit some or all of the processing of their personal data.

1.4 Specific

Obtain from the client a list of their reasons for wanting to collect personal data.

Detail any relationships that exist between the purposes that the client has identified (i.e. common and unique requirements for personal data).

1.5 Transfer

Find out whether the client already deals with other organizations, either as a contractor or else for subcontracting, with which the data is to be shared.

Find out whether the client *anticipates* dealing with third-party organizations in this way.

If the answer to either was no, go on to section ***1.6 Accurate***.
Otherwise, do:

Find out whether the other organizations are to be contracted not to pass on data to further parties.

Ensure that the other organizations are either within the European Economic Area, or else located in approved states[6].

Ensure that the client has assessed the security practices of other organizations.

Ensure that the client has or plans to implement a secure mechanism for transmission and receipt of data.

1.6 Accurate

Ensure that the client has explained to you how they keep data up to date.

Ensure that each item of personal data is associated with a 'check-by' date for each of the purposes they have explained (see **1.4 Specific**).

1.7 Retention

Ensure that the client provides you with a 'use by' date for each of the purposes they have explained, with a view to constructing a feasible retention schedule (see **Specific**).

Ensure that the client explains the steps they currently take to eliminate data from their systems, once 'use-by' dates are exceeded.

Find out how the client manages multiple copies of data (such as backup storage) and how these are brought in to the plan for destruction.

1.8 Security

Identify the latest and most robust technological developments that can be employed when transferring personal data between servers.

Where appropriate, review security standards as set out by BS7799 and ISO 17799.

Ensure that the client explains the processes they use to maintain security of their databases against intrusion from external sources.

Ensure that the client explains how security and integrity is maintained between data sets within their own organization.

Ensure that the client explains how the security of their physical documents is managed, where such documents are produced from their current computer systems.

[6] *For an up-to-date list of approved states, see* http://www.dataprotection.org.uk/

2 Design and build

The design stage includes the conceptual design of the proposed system regardless of representation notation used (text, graphical, formal notation or other) or method of system building employed or of the programming language used.

2.1 Fair

Ensure that the identity of the Data Controller is readily accessible to a potential Data Subject (e.g. the front page of a web site or known to a telesales operative).

Make sure that clear statements are devised to explain the purpose for which the data is being collected to potential Data Subjects

Ensure that clear statements cover EACH item of data collected

Where several purposes have motivated collection of personal data, ensure that there is a clear distinction between data required for the various purposes that the Data Subject is to be asked about.

Design your database to separate personal data by purpose, so that queries made in support of one purpose cannot retrieve data that have been exclusively recorded for another purpose.

2.2 Adequate

Identify all the sources from which data are to be collected that relate the Data Subject and ensure that each data item conforms to the purposes statements agreed with the Data Controller. Examples of such data include IP addresses, caching of on-line forms, cookies, log files, incident reports and operator performance metrics.

Ensure that you put checks in place for the content of free-field data entry (such as forms intended for ASCII input). Especially, be wary of text fields that scroll their content out of view.

2.3 Rights

Make clear statements indicating to the Data Subject how to request access to personal data held

Agree with the Data Controller appropriate procedures for satisfying any request for access to personal data

Organize your database so that all information held on a Data Subject may be produced on request with the minimum of administrative effort on the part of your client or his agents.

When some of the personal data you are storing is sensitive (see Appendix 4), make sure that it is clearly separated within your data structures from non-sensitive personal data.

Ensure that the Data Subject has a clear choice to opt out of direct marketing associated with the site e.g. the ‘tick box’ is empty rather than already ticked.

In the case of website design, avoid designing the site so that it is dependent on the use of cookies or web bugs. Data Subjects must be able to switch off cookies and still use the site. If cookies must be used, make them sessional rather than persistent.

Ensure that any logic processes associated with automated decision making are clearly documented. Data subjects may require access to these.

2.4 Specific

Separate out those purposes requiring specific identification or tracing of data back to the Data Subject. Consider how you might use data obtained from a specific person without actually needing to refer to them personally. In general, processing that does not require a personal identifier is to be preferred. One strategy is to substitute an anonymous or encoded identifier for

the real identifier (person's name, IP address etc.) to allow generic processing whilst always respecting the confidence placed in the organization by the Data Subject. Examples might include sales in the last quarter by postcode area, or age by incidence of obesity.

Where personal identification is not required, implement query methods that do not retrospectively identify a Data Subject from data that has been drawn from their record.

Ensure that you construct databases and access mechanisms that respect the *different* kinds of processing you have agreed with your client.

2.5 Transfer

Ensure that the system can identify the country of origin of personal data and the country of destination.

If transfers are made outside the European Union Area, or the list of approved countries, then first obtain the consent of the Data Subject.

2.6 Accurate

Implement a means for notifying the system administrator when, according to your retention schedule, a data check-by date has been reached.

Implement an auditable mechanism for signing-off data that has been checked for accuracy, following notification of a check-by date.

Ensure that you have implemented a robust method for automatically removing data if the check-by date is exceeded by a defined period without being signed off as accurate.

Ensure that any new data provided by the Data Subject is processed immediately.

Ensure that all data is properly validated on entry e.g. format and range of each field.

Use default values with care, Data Inputters (including the Data Subject) may too rapidly accept default values suggested by the system.

2.7 Retention

Implement a means for notifying the system administrator when, according to your retention schedule, a data use-by date has been reached.

Implement a means for advance notification of use-by date being exceeded, so that any action for renewing the retention period may be taken.

Implement an auditable mechanism for signing-off data that has had an extension to its use-by date.

Ensure that you have implemented a robust method for automatically removing data if the use-by date is exceeded by a defined period.

2.8 Security

Ensure that a secure data collection process is devised for bringing personal data into your system.

Implement a disclosure log, to make it possible to audit the transfer of any personal data from one database or repository to another.

Ensure that data cannot be accidentally accessed by other users of your site

Ensure that the latest virus protection mechanisms are maintained on the system

Ensure adequate back-up of all data

Make clear statements about how personal data is protected during storage and transmission

Provide Data Subjects with essential advice on the creation, use and storage of passwords

3 Testing and evaluation

This stage includes both verification that the system behaves as designed and also validation in the real world that the software meets the requirements.

3.1 Fair

Where appropriate, perform user tests with those members of the client's workforce who will be directly involved in data acquisition processes (e.g. telesales operators). Make sure they are clear about how to explain why personal data is being collected, how long it is to be retained, and how a Data Subject may later remove it.

3.2 Adequate

Ensure that your client is satisfied that the decisions on the basis of processing operations with your system are reasonable, compared to a human decision-maker.

Identify test cases of decisions that cannot be made automatically and so should be automatically deferred pending human intervention.

Identify test cases of incomplete data in order that an authorized administrator might trace a query back to the full record.

3.3 Rights

Ensure that your implementation makes it possible to retrieve all data held on a Data Subject.

Specify the conditions that must be met in order to retrieve all data held on a Data Subject, to ensure that this may only be done when the Data Subject requests it or else for some clearly specified purpose within the client organization.

3.4 Specific

Ensure that test data is not be attributable to real individuals.

Clearly separate live data from test data

3.5 Transfer

Ensure that personal data cannot be transferred inadvertently by third parties e.g. through banner ads placed on a website.

3.6 Accurate

Ensure that documented procedures accompany your system, so that operatives know what to do when 'check-by' dates are notified.

Ensure that there is a clear and easy process by which Data Subjects may have corrections made to their personal data, and that 'use-by' and 'check-by' dates are amended appropriately.

3.7 Retention

Ensure that there is a clear and easy process by which Data Subjects may have their personal data removed from your client's databases, and that 'use-by' date references are amended appropriately.

Ensure that data is not left in temporary processing areas.

3.8 Security

Test the security of your databases from external incursion.
Test the security of your databases from internal incursion/leakage between databases.

4 Release, use and continuous monitoring

This stage is concerned with the process of releasing the system for use and the monitoring of the system while it is in use.

4.1 Fair

If web bugs are used to monitor Data Subjects when reading emails or web pages then you must make it clear to the Data Subject that monitoring is taking place.

Provide Data Subjects with clear statements about how cookies are used.

Provide Data Subjects with details of how to 'switch off' cookies

4.2 Adequate

If any new data item is identified as being valuable to the organisation then discuss the implications for change of purpose with the Data Controller.

4.3 Rights

Respond promptly to requests for access to personal data made by Data Subjects.

4.4 Specific

Where a business case is devised for using personal data in a new way, ensure that Data Subjects are notified and permission obtained before implementing the new purpose. Adequate steps should be taken to deal with those who are not notified and/or do not give permission.

4.5 Transfer

Where third parties outside of the EU are used as data bureux, review the list of approved countries at specified intervals.

If a third party is considered for subcontracting data processing, and they are outside of the EU and not based in a country on the approved list, make sure that it is possible to contact Data Subjects to obtain their permission for this change.

4.6 Accurate

Ensure that all data is fully validated.

Review the procedures for validation in respect of operational incidents that have arisen.

4.7 Retention

Check retention periods of the data and delete out of date items.

Delete all personal data prior to decommissioning of the system.

Review the procedures for destruction of personal data and renewal of permission in respect of operational incidents that have arisen.

4.8 Security

Ensure that access to data is monitored and recorded.

Ensure that access log files are secure.

Ensure the use of up-to-date virus protection and measures to prevent access violations.

Ensure adequate escalation procedures in the event of a breach.

References

BCS 1998, Data Protection – everybody's business: A Practical Guide for Professionals and Business Managers, The British Computer Society, ISBN 1-902505-04-2

BCS 1999, E-Commerce – A World of Opportunity: A Practical Guide for Professionals and Business Managers, 1999, The British Computer Society, ISBN 1-902505-08-5

Borkin 2000, Presentation given by John Borkin of the Dutch Data Protection Commission, www.registratiekamer.nl at IeC2000

Data Protection Act 1998, ISBN-0-10-542998-8, The Stationary Office Limited, http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

Hes,R., and Borking, J. Privacy Enhancing Technologies: The Path to Anonimity, http://www.registratiekamer.nl/bis/top_1_5_35_3.html

Masons, 2000, Specification for procuring IT systems in compliance with the Data Protection Act 1998, version 2, Masons, September 2000

Smith 2000, Presentation given by David Smith, UK Assistant Information Commissioner, www.dataprotection.gov.uk at IeC2000

Technical Report One 2000, Technical Report One: Development of Guidance on Data Protection in System Design, Leon Watts and Linda Macaulay, report for the Office of the Data Protection Commissioner.

Watts, L. A., & Macaulay, L. (2001). Development of Guidance on Data Protection in Systems Design: Technical Report 1 (1). Department of Computation, UMIST.

Appendix 1: The Eight Principles of Data Protection

The follow definitions of the eight data protection principles are taken from Chapter 29 of the Data Protection Act, 1998. Emboldening has been added to show the relationship between these definitions and the FARSTARS principles for systems designers.

THE PRINCIPLES

1. Personal data shall be processed **fairly** and lawfully and, in particular, shall not be processed unless-

   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more **specified** and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be **adequate**, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be **accurate** and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall **not be kept for longer** than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the **rights** of Data Subjects under this Act.

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

8. Personal data shall not be **transferred** to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

Appendix 2: Schedule 2 of the Data Protection Act.

The Data Controller may only process personal data if they have satisfied at least one of the conditions set out below. If the Data Controller intends to process sensitive personal data, they may only do so if they additionally satisfy one of the conditions of Schedule 3 (see Appendix 3).

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.

2. The processing is necessary:

(a) for the performance of a contract to which the data subject is a party, or
(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary:

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix 3: Schedule 3 of the Data Protection Act:

There are ten separate conditions that apply to the collection of "sensitive personal data" (See Appendix 3). The Data Controller must meet *at least one* of these in order to be able to process lawfully sensitive personal data *in addition to* the stipulation for normal personal data (listed in Appendix 2).

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his/her explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary:

(a) in order to protect the vital interests of the data subject or another person, in a case where-
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing:

(a) is carried out in the course of its legitimate activities by any body or association which-
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(b) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(c) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing:

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing:

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(d)is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix 4: Sensitive personal data.

Sensitive personal data on a Data Subject include information on any of the following matters:

(a) the racial or ethnic origin of the Data Subject,

(b) his/her political opinions,

(c) his/her religious beliefs or other beliefs of a similar nature,

(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his/her physical or mental health or condition,

(f) his/her sexual life,

(g) the commission or alleged commission by him/her of any offence

(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Appendix 5: Characteristics of an Effective Privacy Statement

A Privacy Statement should be a no longer than one page in length.

Wherever possible privacy statements should be made at the point at which the data is collected.

A typical 'Privacy Statement' will provide answers to the following questions about 'our site':

- What information does 'our site' receive and how do we use it?
- May I choose what information I disclose?
- May I choose what information I receive?
- What if I need to review or change any personal information previously disclosed?
- What kind of security is used to protect my information
- Who has access to my information?
- What about other companies featured on 'our site'
- What about children's information?
- Who can I contact if I have any questions regarding my privacy?
- What are my rights to access, control and remove my personal data?

Appendix 6: Glossary of Terms

Aggregate information.

Information that may be collected by a Web site but is not "personally identifiable" to Data Subject (see definition below). Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as none of these fields is linked to a user's personal information, the data is considered aggregate.

Browser.

Also called a Web browser. Software that enables Data Subject to search and or navigate through Web sites or "browse" parts of the Internet, especially the World Wide Web. Examples: Netscape Navigator and Microsoft Internet Explorer.

Bulletin board.

A public area online where Data Subject can post a message for everyone else to read. If Data Subject post a message to a bulletin board, in nearly all cases, other member participants will be able to contact Data Subject by e-mail.

Chat.

A function that allows a group of people to communicate simultaneously by typing messages to one another online. Typically, everyone participating in the chat sees the message as soon as Data Subject sends it. Designated chat areas are often referred to as "chat rooms," and any individual or group of individual Data Subjects in the room will be able to contact Data Subject by e-mail.

Client

The client is the person who has commissioned the system. The client could be an individual or an organisation.

Cookie.

A block of text placed in a file on Data Subjects computer's hard drive by a Web site the Data Subject has visited. A cookie is used to identify Data Subject the next time Data Subject accesses the site. Cookies cannot identify an individual user specifically unless the cookie data is attached to personally identifiable information collected some other way, such as via an online registration form.

Data Controller

A person, usually an organization, who determines the purposes for which and the manner in which any personal data are processed.

Data Subject

The person who the personal data are about.

Domain name.

The company, individual, or organization "name" the Data Subject uses to access a Web site

Encryption.

The process of converting data into a private code for secure transmission.

Identity Protector

A Privacy Enhancing Technology (see below) which facilitates decoupling of personal identity from the information content of the data.

Personal data

Personal data means data which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

Personally identifiable information.

Information that can be traced back to an individual user, e.g. Data Subject name, postal address, or e-mail address. Personal user preferences tracked by a web site via a "cookie" (see definition above) is also considered personally identifiable when linked to other personally identifiable information provided by the Data Subject online.

Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) are software based mechanisms that have the potential to encode or facilitate aspects of the Data Protection Act.

Privacy statement.

A page or pages on a web site that lay out its privacy policies, i.e. what personal information is collected by the site, how it will be used, whom it will be shared with, and whether Data Subjects have the option to exercise control over how the Data Subject's information will be used.

Sensitive Personal Data

Sensitive Personal Data are those giving information as to a person's race, ethnic origin, religious and other beliefs, political opinions, health or commission of criminal offences. (See Appendix 2).

Webmaster.

Typically, an individual or an individual within a company or organization assigned with the task of updating and maintaining an individual Web site.

Web Bug

A web bug is a graphic on a web page or in an e-mail message that is designed to monitor who is reading the web page or email message. Web bugs are often invisible because they are typically only 1x1 pixel in size. They are represented as HTML IMG tags. Typically a web bug will cause the following information to be sent to a server: the IP address of the computer that fetched the web bug; the url of the page that the web bug is located on; the url of the web bug image; the time the web bug was used; the type of browser that fetched the web bug; a previously set cookie value.

Authors:

Dr. Leon Watts
Professor Linda A. Macaulay
Department of Computation
University of Manchester Institute of Science and Technology (UMIST)
Sackville Street, Manchester M60 1QD,UK
Tel: +44-161-200-3354
www.co.umist.ac.uk