

## **Internet Privacy Model - Draft**

**The need to establish effective processes to protect privacy and personal data on the Internet is driven by the need to satisfy regulatory requirements and to follow good business practice.**

The processing of personal data on-line is central to the effectiveness of e-business. Web based organisations can use new technologies to gain access to an individuals' interests and lifestyle, however, such organisations must be careful to avoid invading the individual's right to privacy.

The 1998 Data Protection Act regulates the use of personal data in the UK and its provisions are also applicable to transactions on the Web.

One of the objectives of this project is to explore ways in which we can ensure that different practices in data protection do not create barriers to efficient trade. Businesses and all market players need trustworthy and widely available tools to fulfil their privacy and data protection obligations.

### **Identification of Personal Data**

What is personal data - Personal data is any information capable of identifying a living individual. It can include photographic images, written words and even recorded sounds.

E-mail address information will be personal data where it identifies a particular person

e.g. [JohnSmith@ICL.com](mailto:JohnSmith@ICL.com)

### **Collection of Personal Data (First Principle)**

#### ***Lawful Processing***

Determine that the processing of the personal data is in itself lawful: Schedule 2 of the Act provides that data controllers must not process personal data unless they can base their processing activities on one of six criteria.

Criteria most likely to be relevant to on-line processing are:

- The data subject has given consent to the processing
- Processing is necessary for the performance of a contract

Schedule 3 sets out the conditions for the processing of so-called "sensitive personal data"

The most relevant condition here is likely to be where the individual has given specific consent.

## ***Fair Processing***

The 1998 Act imposes an obligation to ensure that the reasons for the processing are transparent.

Data subjects who are clearly informed of the purposes, in advance of any processing, can click away from the Controller's web site and decide not to provide any personal details.

All non-obvious uses and disclosures of personal data, which are associated with the processing – and any other feature which would be necessary to guarantee fair processing have to be declared in a simple, straightforward and unambiguous fashion.

Any secret collection of personal data e.g. by use of a “cookie” can thus be considered to be unfair processing because data subjects are unaware that their details are being processed

## **Quality of Data & Proportionality (Principles 3, 4 & 5)**

Data should be accurate, kept up to date, adequate, relevant and not excessive in relation to the purposes:

Check for accuracy – organisations must take care – problem area – when you have opinions about people held on line. It makes good business sense to put in mechanisms to ensure that the personal data held properly reflects the current situation

Relevancy is a function of time – you need certain types of information at certain times for certain purposes – but it may not be relevant in the future. How will you establish relevancy?

Is it excessive to make a demand/request for information you don't need.

## **Individual's Rights (Principle 6)**

Individuals have the same rights on-line as they do offline. The growth of Internet and on-line servers has also brought concern for consumers about what information is collected about them.

The right to prevent the use of personal data for direct marketing purposes is unqualified and “direct marketing” is defined as the communication by whatever means of any advertising or marketing material directed to particular individuals.

Generally although Internet held information usually relates to marketing, promotional or public relation purposes, whatever the purpose – you must always:

- Make clear whether you share, disclose or sell any personally identifiable information collected on-line

- Ensure that if in future you may wish to share customer personal data with third parties that the data subjects will always be involved in any prior authorisation
- Make sure that individuals are aware of the implications of their personal details being held on an Internet.

### **Security of Data (Principle 7)**

Giving anybody in the world access to your computers does not strike one immediately as a measure conducive to security, nor does the sending of e-mail, not knowing where that message might be stored or copied. However, the problems associated with securing the Internet often do not differ from those of any other computer network.

Recommendation is to assume that the Internet is fundamentally insecure.

The Data Controller can either classify the network as being suitable only for the transmission of certain kinds of ‘innocuous’ personal data, or add security features such as encryption or the installation of firewalls before breaching this restriction.

Even when appropriate security measures are in place, it must be recognised that there is a likelihood that somebody out there is attempting to undermine their security foundations.

Implement the use of passwords for access to personal data on-line; adopt the use of some other type of personally identifiable information; always take steps to verify the identity of the individual before granting access to alter/amend personal data in any way.

In summary, it is the responsibility of the Data Controllers to put in place appropriate security measures and to consider all the security risks on a periodic basis. The only defence a Data Controller has under the Act if there is a major security breach is that of demonstrating that all reasonable steps have been taken to secure the personal data.

### **Worldwide Transfers**

Restrictions on international transfers of personal data imposed by the eighth principle are synonymous with the global nature of networks

However, the Act provides for a number of exemptions reflected in the eighth principle and in Schedule 4 to the 1998 Act, for example, that the data subject has consented to the transfer in question or that the transfer is necessary for a contract.

This could be addressed by the implementation of appropriate privacy statements/policies which at a minimum would cover issues such as:

- Common worldwide approach
- Security policy explained
- Data gathered: cookies

- Purposes explained
- Potential recipients explained
- Opting out or changing instructions