**Data Protection Laws**

Eduardo Johnson

Martineau Ustaran

*research@marjohn.com*

**Abstract**

This Autumn, the UK Government is expected to introduce a Bill which will give legal effect to the European Union Directive on data protection. In October 1995, the European Parliament and the Council adopted a Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. As stated by the Directive, the United Kingdom and the rest of the member states have until October 1998 to incorporate its terms into national legislation. The implementation of this Directive involves a challenging legislative process which is to be addressed at a crucial time for the regulation of world-wide communications.

The exponential growth of global computer networks such as the Internet is creating an unprecedented scenario where large amounts of personal data can be transmitted across national borders and become publicly available. Therefore, the new regulatory regime dealing with data protection needs to be properly adjusted to cope with this scenario. This article looks at the Government's Proposals for new data protection legislation in the UK and identifies those aspects which are likely to present a greater challenge in the context of today's electronic communications.

**Keywords**

data protection; electronic communications; personal data; European Directive; Data Protection Registrar; controller; security; notification; data transfers; Internet; regulatory regime.

**1. Introduction**

The use of computers to process personal information in the UK is governed by the Data Protection Act 1984 <http://www.hmso.gov.uk/acts/acts1984/1984035.htm>. This act is derived from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It has a twofold aim: (i) to place registration and practice obligations on those who hold personal data on computer, and (ii) to give rights to individuals about whom information is stored on computer. The day-to-day administration of the regime created by the Act is undertaken by the Office of the Data Protection Registrar <http://www.open.gov.uk/dpr/dprhome.htm>.

In October 1995, the European Parliament and the Council adopted a Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data[[1]](#endnote-1) <http://ltc.law.warwick.ac.uk/jilt/dp/material/directiv.htm>. The United Kingdom and the rest of the member states have until October 1998 to incorporate its terms into national legislation[[2]](#endnote-2). In the UK, the implementation process began in March 1996 with the publication by the previous Government of a Consultation Paper <http://www.open.gov.uk/home\_off/ccpd/dataprot.htm> which sought views on the way in which the Directive should be implemented.

A Home Office's press release <http://www.coi.gov.uk/coi/depts/GHO/coi6825b.ok> of 22 March announced that the Government was determined to introducing any required provisions in a way which minimised the burden on businesses. The Home Office added that the Government intended to go no further in implementing the Directive, than was absolutely necessary to satisfy its obligations under European Law. The Consultation Paper confirmed this attitude by stating that the Government intended to implement the Directive in the least burdensome way for data users, while protecting individuals.

The Data Protection Registrar however, saw this proposal as a minimalist approach to such a crucial task[[3]](#endnote-3). Accordingly, in a document called 'Questions to Answer' <http://www.open.gov.uk/dpr/dprpaper.htm> published one month after the Consultation Paper, the Registrar took the view that the most secure way of implementing the Directive was to introduce a new Bill in Parliament. 'Questions to Answer' was only meant to set out the background to the issues raised by the Directive in order to stimulate debate. The full Response of the Data Protection Registrar <http://www.open.gov.uk/dpr/answer/content.htm> to the Consultation Paper went even further by saying that contrary to the view expressed by the Government, this was an opportunity to take a fundamental look at the way data protection law operated in the UK.

The new Government decided in favour of the view maintained by the Registrar and announced its decision to introduce new legislation to strengthen data protection controls in the Queen's Speech on the opening of the Parliament <http://www.coi.gov.uk/coi/qs\_97/speech.html> last May. Detailed Government's Proposals <http://www.homeoffice.gov.uk/datap2.htm> for new data protection legislation which will implement the Directive in the UK were published on 28 July 1997. These Proposals build on the previous Consultation Paper and the responses received, and serve as an introduction to the forthcoming Bill. Some of the issues contemplated by the Proposals have a direct impact on electronic communications. This article addresses these issues in light of the challenges presented by today's information and communications technology.

**2. Regulatory challenges**

The background to the Government's Proposals is concisely set out in the foreword by the Home Secretary, Jack Straw. The information society offers endless opportunities to communicate. When the content of the message communicated consists of personal information, data protection ensures that those who handle the information do it in a proper and responsible manner. The objective pursued by the Proposals is to ensure proper protection for information about individuals while avoiding unnecessary interference with legitimate processing. This intricate balance could be jeopardised by several issues which are now considered in detail.

***2.1 Geographical extent***

According to recital 20 of the Directive, the fact that the processing of data is carried out by someone located in a third country must not affect the level of protection awarded to individuals. This principle is translated into operational terms by article 4.1(c), which provides that member states must apply their laws to the processing operations of a controller not established in the European Union that uses equipment situated in their territories. The only exception applicable to this provision concerns the case where the equipment is used only for purposes of transit through the territory of the EU. This is an entirely justifiable exception given the nature of Internet communications for example, where messages can take many and varying paths to recipients[[4]](#endnote-4).

The Directive also states that when controllers are situated outside the EU, they must designate a representative in the territories of the member states where the equipment is located. Consequently, the proposed implementation of article 4.1(c) in the UK requires that a UK representative is designated by the foreign organisation. However, if the application of the future data protection law to foreign controllers is restricted in this way, unscrupulous users of data may be able to escape regulatory controls by retreating to 'data havens'.

As drafted, the Proposals seem to suggest that the law would only apply when the organisation controlling the data has designated a representative in the UK. Given the development in the use of global networks, it is possible for a controller located outside the UK to use electronic facilities with remote access to equipment located in the UK. If this were the case, the level of protection applicable would be at the mercy of controllers who could access and process personal information in the UK from the place of their choice. If the aim of recital 20 of the Directive is to be observed, the Government will need to contemplate all possible scenarios and provide for an adequate and fair solution.

***2.2 Security***

As the Registrar indicated in the Response to the Consultation Paper, the eight Principles which constitute the substantive provisions of the Data Protection Act, are broadly similar to the principles which form the core of the Directive[[5]](#endnote-5). This statement is also acknowledged by the UK Government, which intends to follow the approach of the 1984 Act by retaining all eight principles. The first six principles of the Act are mirrored by article 6 of the Directive[[6]](#endnote-6) and according to the Government, they will only require minor adjustments. As the Comments of the Data Protection Registrar on the Government's Proposals <http://www.open.gov.uk/dpr/whiteres.htm> put it, the retention of the principles, amended to reflect the requirements of the Directive, will helpfully emphasise the continuity between the present and new laws. However, the principles concerning subject access and security are addressed in more detail by the Directive and will need a thorough revision.

With regard to security, the Directive's basic obligation to take appropriate technical and organisational protective measures closely follows the wording of the Data Protection Act. However, as recognised by the Registrar in her Response to the Consultation Paper, the article dealing with security of processing in the Directive is further reaching than the Act's eighth Principle. In fact, this provision presents one of the most obvious challenges to the application of data protection law to network communications[[7]](#endnote-7). The Directive acknowledges this by adding that measures to protect personal data need to be provided particularly where the processing involves the transmission of data over a network.

The arguments concerning the alleged inherent insecurity of the Internet are difficult to reconcile[[8]](#endnote-8). Aware of this fact, the Directive states that in order to ensure the appropriate level of security, controllers need to consider the state of the art and the cost of implementing security measures, bearing in mind the risks involved in the processing. No further guidance is given to member states which will have to decide for themselves what, if any, specific levels of security are required. The Government's Proposals suggest that this matter will receive further attention.

Although it is likely that the Government will favour a case-by-case approach, some concrete measures should ideally be required for certain cases. For example, given the uncertainty about the suitability of e-mail to transmit confidential information, the adoption of sensible rules on the use of encryption would be of great assistance to both Internet users and network operators. Whether there is room or time for specific regulation on this matter in the forthcoming Bill is an arguable matter, but the Government should take this opportunity to assess the security implications currently affecting electronic communications.

***2.3 Exemptions from notification***

In a brave interpretation of the Directive's provision which allows member states to simplify or exempt certain categories of processing operations from notification, the Government intends to include some key categories on its list of exemptions. As announced in the Proposals, the Government has been relying on the work of the Data Protection Registrar to set up the detailed regime dealing with notification[[9]](#endnote-9). The Registrar had previously supported the general principle that certain predefined processing operations which are unlikely to affect the rights and freedoms of data subjects should be exempted from notification. As a result, the Government is now prepared to follow the Registrar's proposition to exempt from notification processing operations carried out for particular purposes.

The purposes selected by the Registrar for an outright exemption include two categories which are at the core of the trading activities conducted via electronic communications: (i) purchase and sales administration, and (ii) advertising, marketing and public relations. It is certainly in the benefit of the development of electronic commerce that the Government is willing to allow controllers to carry out these processing operations without compulsory notification. However, in order to protect the rights of individuals who, for example, are the target of personalised e-mailshots[[10]](#endnote-10) or make credit card payments electronically, the Government also needs to emphasise the requirement to comply with the principles, even if notification is not compulsory.

***2.4 Transfers to third countries***

The practical application of the articles of the Directive concerning transfers of personal data to third countries is very difficult to foresee in the context of global communications. Articles 25 and 26 of the Directive gravitate around one principle: transfers of data to a non-EU country may only take place if that country ensures an adequate level of protection. This is to say that, subject to limited concessions, the Directive prevents the use of the Internet to convey personal information, since in many cases it is not possible to predict where the recipient will be located. This legal 'cul-de-sac' has already been denounced (Millard C; 1997, p20) but an alternative set of rules aimed at resolving this problem remains to be seen.

The original Consultation Paper of the Home Office conceded that the exceptions to the principle were wide-ranging and that the number of cases in which transfers were to be prohibited due to the inadequacy of data protection controls in a third country, was likely to be small. The Consultation Paper went on to say that controllers wishing to transfer personal data outside the EU, would have to consider first whether their proposed transfers were covered by any of the exceptions, and if this was not the case, they would need to assess the adequacy of the protection. Similarly, the Registrar recommended that the duty to comply with article 25 be imposed directly on controllers, who would be assisted by 'adequate' and 'not adequate' lists prepared by the European Commission.

The latter view seems to be in line with the current European Commision's document on Possible Ways Forward in Assessing Adequacy <http://www.bna.com/e-law/docs/eudata1.html>. This document recognises that given the vast number of transfers of personal data taking place between EU and non-EU countries, mechanisms will have to be developed to help member states, supervisory authorities and controllers decide on the adequacy of transfers. The main mechanism envisaged by the Commission consists of a 'white list' of third countries which can be assumed to ensure an adequate level of protection. In the event that a third country does not feature on the white list, the Commission has suggested that member states will need to establish a set of criteria which should be met before carrying out transfers which would pose particular threats to privacy. According to the Commission, Internet transfers ⎯such as on-line credit card payments and the use of 'cookies'[[11]](#endnote-11)⎯ are among the categories which are likely to pose particular risks.

The Government's Proposals do not contain any specific initiatives and favour a regulatory regime where the controller decides on the adequacy of protection of third countries in accordance with previously established safeguards. However, this does not seem to offer a satisfactory solution to cases such as the publication of personal information on a web site. The majority of the WWW can be accessed without restriction from virtually anywhere in the world, which means that limiting such access on a geographical basis will not generally be in the hands of the controller. As a result, a realistic and workable approach to data protection regulation on this area is needed if the benefits of the Internet as a means of communication are to be preserved.

**3. Conclusion**

The implementation of the data protection Directive in the UK must be guided by the twofold objective of the Directive: (i) to protect individuals, and (ii) to ensure a free flow of personal data between member states. Electronic communications (with Register) can have a direct effect on the way personal information is controlled, accessed, used and disseminated. Therefore, any regulatory mechanism which seeks to achieve the balance demanded by the Directive needs to be considered in this context. The UK Government is currently in the process of carrying out this complicated task. However, this challenge is also an opportunity to re-focus the UK regulatory regime on data protection. Having an understanding of the issues involved is important, but looking into these issues from a practical angle is essential in order to guarantee both effective communications and the individual's privacy.

**References**

Bainbridge D and Pearce G (1995) 'Controls and constraints on processing personal data', *New Law Journal* 1579.

Flint D (1997) 'E-mail Security: A Personal View', *Internet Newsletter for Lawyers*, September/October Issue.

Gringras C (1997) *The Laws of the Internet* (London: Butterworths).

Kanani Y (1996) 'Surfing Not Sinking', *Internet Business*, Issue 2.

Kosten F and Pounder C (1996) 'The EC Data Protection Directive 1995: An analysis', *Web Journal of Current Legal Issues*, Issue 2

<http://www.ncl.ac.uk/~nlawwww/1996/issue 2/kosten2>.

Martineau Johnson (1996) 'Data Protection: A Changing Scenario', *Education Brief*, Issue 10.

Millard C (1997) 'Transborder data: go with the flow', *Legalease Special Report: Intellectual Property 1997*.

Special Feature on the European Data Protection Directive (1996) *JILT*, Issue 1 <http://ltc.law.warwick.ac.uk/jilt/issue1/1DP.htm>.

**Links**

ACLU v. Reno, 929 F Supp 824 (1996) <http://zeus.bna.com/e-law/cases/aclureno.html>

Comments of the Data Protection Registrar on the Government's Proposals <http://www.open.gov.uk/dpr/whiteres.htm>

Consultation Paper <http://www.open.gov.uk/home\_off/ccpd/dataprot.htm>

Cookie Central <http://www.cookiecentral.com>

Data Protection Act 1984 <http://www.hmso.gov.uk/acts/acts1984/1984035.htm>

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

<http://ltc.law.warwick.ac.uk/jilt/dp/material/directiv.htm>

Government's Proposals <http://www.homeoffice.gov.uk/datap2.htm>

Home Office's press release of 22 March 1996 <http://www.coi.gov.uk/coi/depts/GHO/coi6825b.ok>

Kosten F and Pounder C (1996) 'The EC Data Protection Directive 1995: An analysis', *Web Journal of Current Legal Issues*, Issue 2 <http://www.ncl.ac.uk/~nlawwww/1996/issue 2/kosten2>

Office of the Data Protection Registrar <http://www.open.gov.uk/dpr/dprhome.htm>

Queen's Speech on the opening of the Parliament <http://www.coi.gov.uk/coi/qs\_97/speech.html>

'Questions to Answers' <http://www.open.gov.uk/dpr/dprpaper.htm>

Possible Ways Forward in Assessing Adequacy <http://www.bna.com/e-law/docs/eudata1.html>

Response of the Data Protection Registrar to the Consultation Paper <http://www.open.gov.uk/dpr/answer/content.htm>

Special Feature on the European Data Protection Directive (1996) *JILT*, Issue 1 <http://ltc.law.warwick.ac.uk/jilt/issue1/1DP.htm>

1. **Endnotes**

   Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

   <http://ltc.law.warwick.ac.uk/jilt/dp/material/directiv.htm>. [↑](#endnote-ref-1)
2. For an early discussion on the implementation process see Special Feature on the European Data Protection Directive (1996) *JILT*, Issue 1 <http://ltc.law.warwick.ac.uk/jilt/issue1/1DP.htm>. [↑](#endnote-ref-2)
3. 'Data registrar calls for privacy review', *The Lawyer*, 30 July 1996, p. 8. [↑](#endnote-ref-3)
4. As pointed out in the decision *ACLU v. Reno*, 929 F Supp 824 (1996)

   <http://zeus.bna.com/e-law/cases/aclureno.html> [↑](#endnote-ref-4)
5. This is a generally accepted view. See Bainbridge D and Pearce G (1995) 'Controls and constraints on processing personal data', *New Law Journal* 1579. [↑](#endnote-ref-5)
6. For a slightly different opinion on this topic see Kosten F and Pounder C (1996) 'The EC Data Protection Directive 1995: An analysis', *Web Journal of Current Legal Issues*, Issue 2 <http://www.ncl.ac.uk/~nlawwww/1996/issue 2/kosten2>. [↑](#endnote-ref-6)
7. A similar opinion can be found in Gringras C (1997) *The Laws of the Internet* (London: Butterworths), p. 287. [↑](#endnote-ref-7)
8. For opposite arguments see Kanani Y (1996) 'Surfing Not Sinking', *Internet Business*, Issue 2, p. 28; and Flint D (1997) 'E-mail Security: A Personal View', *Internet Newsletter for Lawyers*, September/October Issue, p. 10. [↑](#endnote-ref-8)
9. For a brief outlook into the likely changes affecting the notification obligations of education institutions see Martineau Johnson (1996) 'Data Protection: A Changing Scenario', *Education Brief*, Issue 10. [↑](#endnote-ref-9)
10. An initiative to deal with unsolicited promotional e-mail called 'Suppression Markers in Internet Addresses' was suggested by the Office of the Data Protection Registrar in October 1996. [↑](#endnote-ref-10)
11. Further information on the use of Internet 'cookies' can be found at Cookie Central <http://www.cookiecentral.com>. [↑](#endnote-ref-11)