



## Data Protection Issues for Intranet Managers

Martin White  
Managing Director  
Intranet Focus Ltd

Telephone: +44 (0) 1403 267030  
Online <http://www.intranetfocus.com/>  
Email: [contactus@intranetfocus.com](mailto:contactus@intranetfocus.com)

Revised April 2007

## **The Author: Martin White**

Martin White is Managing Director of Intranet Focus Ltd., which he established in 1999. Martin has written the Behind the Firewall column on intranet management issues for the US magazine EContent (<http://www.econtentmag.com>) since 2001, for which he is a Contributing Editor, a position he also holds for Intranets: Enterprise Strategies and Solutions (<http://www.intranetstoday.com>) and for which he is Reviews Editor. Martin was a workshop leader for Nielsen Norman User Experience events in 2005 and 2006, and is also taking part in the 2007 event.

Martin is the author of The Content Management Handbook, which was published by Facet Publishing Ltd in early 2005. His latest book, Making Search Work, was published by Facet Publishing in March 2007.

Martin was Chairman of the Online Information Conference (<http://www.online-information.co.uk>) from 1999-2006. In 2005 he was the recipient of the Information Industry Award for Lifetime Contribution. He has been Visiting Professor at the Department of Information Studies, University of Sheffield <http://www.shef.ac.uk/is/> since 2002 and is a member of the Governing Board of CAB International. (<http://www.cabi.org>), acting as Chairman of the Finance and Audit Committee. He is also a member of the Publications Board of the Royal Society of Chemistry.

## **The Company: Intranet Focus Ltd**

### **Designing and enhancing intranets and extranets**

For organizations that have not yet set up an intranet we can carry out an information audit to confirm the information requirements needed to achieve the objectives of the organization, and from these develop a content strategy, information architecture and governance structure.

For organizations that have an intranet, or a number of departmental intranets, we can assess their design against current good practice, and undertake user surveys and usability tests. We can develop information architectures and metadata schemes. The business experience of our consultants enables us to support multi-national/multi-lingual intranets. We also provide guidance on the integration of intranets as the result of a merger or an acquisition.

### **Content Management and Search software selection**

We support the selection and deployment of content management software. We can develop a content management strategy, and from this prepare a formal RFP that can be sent out to a short list of vendors. To assist in the selection of a vendor we have developed a checklist based on our experience in major projects in North America and Europe. Once the vendor has been selected we can work with the client and the vendor to develop realistic implementation and content migration strategies. We can carry out similar projects for the selection of enterprise search software and corporate portal software. We maintain complete independence from any vendor.

## Introduction

This briefing paper provides an overview of the European Directive on Data Protection, which all EU Member States have to implement by October 2001. The Directive imposes constraints on the transfer of personal data from the EU Member States (technically countries within the European Economic Area, to include Norway) to any country that does not have adequate data protection legislation. Very few countries in the world have such legislation, including the USA. Intranets, and e-mail, are increasingly used by companies with operations in a number of countries to communicate and process information about their staff and clients. Because of the very strict rules on the communication and processing of this type of information intranet managers need to take steps to ensure that all appropriate actions have been taken to comply with the legislation.

This briefing paper should be used only as a guide to the issues, and not as a definitive statement on procedures or as a legal opinion.

1. Background
2. The EU Directive on the Protection of Personal Data
3. Issues of definition
4. Data transfers from the EU
5. The Lindqvist case
6. The situation in the USA
7. Contractual clauses for the transfer of information to non-EU countries
8. Intranet, internet and e-mail implications
9. Conclusions and recommendations
10. Web Resources

## 1. Background

There are very strict procedures under which transfers of personal data can take place between companies located in a Member State of the European Union and companies in any other country in the world. This is sometimes referred to as trans-border data flow.

The fundamental issues of transborder data flow are not new. In the late 1970s there was considerable concern about this issue, leading to the adoption in 1980 by the OECD of Guidelines Governing the Protection of Privacy and Transborder Flows of Data, and this was followed in 1981 by the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Although the USA is a signatory to the OECD Guidelines it has not implemented them in law, and as a result there are now some substantial problems arising with the potential illegality of the transfer of personal data between the EU and the USA, and indeed with virtually every other country in the world.

One important provision of the Directive is to ensure that personal data can be freely transferred within the EU, subject to very strict provisions, in order to facilitate the development of a single market. However there are equally strict provisions about the export of personal data to other (so-called 'third') countries where there is no equivalent legislation, and currently very few countries do have such legislation. One country that takes an entirely different approach, that of industry self-regulation, is the USA, and the result is that at present the transfer of personal data to the USA from any EU member state is in breach of the provisions of the Directive unless

carried out under the provisions of the Safe Harbour Agreement, which are dealt with later in this paper.

The implications of this situation are very important to businesses in both the EU and the USA. Any personal data on an intranet that links the EU and the USA (and for that matter almost any other country in the world) can only be transferred with the explicit approval of the person concerned on a case-by-case and country-by-country basis. Personal data on lap-top computers falls within the provisions of the Directive if a manager carries their lap-top between countries. Also included are Web sites outside the EU that seek to gain personal information from EU citizens. The legislation affects non-EU citizens in Europe (even if only in transit) but not EU citizens in other countries.

In this paper some of the implications for companies with intranets and extranets are considered. The implications on other activities are considered in outline, but this paper should in no way be considered a legal opinion.

## 2. The EU Directive on the Protection of Personal Data

The provisions of the EU Directive on the Protection of Personal Data (95/46/EC) are fairly close to those of the Council of Europe Convention 108 of 1981, and countries that are signatories of the Convention have at least a regulatory framework in place for data privacy. The Directive is not in itself 'law'. It sets out the minimum requirements that have to be complied with by the national legislation of Member States, and the date (25 October 1998 - three years after adoption in October 1995) that this compliance has to be implemented. Within the EU the Member States are not only implementing the Directive differently, but the Data Registrar in each member State will also implement any legislation according to their own interpretation.

In 2002 major study was carried out on behalf of the Commission by Douwe Korff, of the University of Essex that provided a comparison of the ways in which the core Directive had been implemented in EU member states.

At the beginning of 2007 the European Commission published an appraisal of the work that had been carried out on the implementation of the Directive [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/lawreport/com\\_2007\\_87\\_f\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf) and this provides a useful overview of the issues and the priorities of the Commission.

The basic principles of the EU Data Protection legislation are the following.

**Purpose limitation** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer

**Data quality** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant, and not excessive in relation to the purposes for which they are transferred or further processed.

**Transparency** - individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness.

**Security** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by processing.

**Rights of access** - the data subject should have a right to obtain a copy of all the data relating to them that are processed, and a right to the rectification of the data where they are shown to be inaccurate.

**Restrictions on transfer** - further transfers of the personal data by the recipient of the original data transfer should only be permitted where the second recipient is also subject to the rules affording an adequate level of protection.

It is this last principle that is the main difference between the EU Directive and the Council of Europe Convention. It should also be noted that in the majority of the Member States this will also be the first time that protection becomes available for paper-based as well as electronic data.

Another new element is the introduction of the concept of Sensitive Personal Data, and this covers information about

- Racial or ethnic origin
- Political opinions
- Religious and other beliefs
- Trade Union membership
- Physical or mental health
- Criminal proceedings or convictions
- Sex life

The way in which this data is handled is subject to more stringent provisions than other forms of personal data, requiring explicit consent of the individual, with very clear indications of why it is necessary to collect and transfer this information.

Data subjects also have much wider powers to see what data a company or organisation does have about them, and the purpose for which it is being used.

### 3. Issues of definition

The issues of where processing of the data takes place are complex. The nature of the Internet is that the message is split up into individual packets, and each packet may be sent over a different network path before being recombined in the correct order at the eventual destination. It is therefore quite likely that a message sent from London to Rome may well go through a network switch in New York, and as a result technically that data has been exported to the USA, even if only for a fraction of a second. If an EU citizen is providing personal information to a site or an intranet which, even though it is operated by a EU company the server is located outside the EU, then this personal data is being exported to a third country.

The OECD and Council of Europe documents were of course prepared in the pre-PC age, and more importantly in the pre-internet age, and are therefore focused on a mainframe data processing environment. Even when the European Commission Directive was agreed in 1995 the Internet was still mainly an academic network with no commercial significance.

It is unclear what is meant by the word 'contract'. In the case of the airline industry, for example, is the contract between an airline and a customer just to transport them from country A to country B, or does the contract also include provision of food and other services, such as frequent flyer privileges, or Air Miles? This makes a difference as to what information an airline can request from a passenger and store for future use.

Finally the use of the phrase 'has given' would seem to imply prior agreement by the individual, rather than retrospective agreement, and that the agreement is informed and specific to a particular purpose.

## 4. Data transfers from the EU

This paper is primarily concerned with Articles 25 and 26 of the European Directive as they affect transborder operations, but the other provisions of the Directive also need to be taken into account. In summary Article 25 states that transfer of personal data to a third country may take place only if the third country ensures an adequate level of protection, and goes on to say that this adequacy will be assessed in the light of the professional rules and security measures which are complied with in that country.

Article 26 goes on to say that this transfer can take place if the data subject has given their consent unambiguously to the proposed transfer, and that the transfer is necessary for the performance of a contract. It seems likely that a 'non-response' is likely to be adequate. In other words the consent form cannot be worded in such a way that if the data subject has not replied within a given period of time they can be deemed to have given consent.

The first derogation also seems to imply that there must be full information given to the data subject, such as a list of all the third countries that the data might be transferred to, rather than a generic agreement. In other words it is unlikely that a generic waiver could be introduced into the contract of an employee, both because the requirement is for agreement to a specific purpose, and also because it might be argued that a new employee is not in a position to understand the implications of the waiver at that early stage of employment in a new company.

There are a number of other situations set out under Article 26 under which personal data can be transferred, but they are quite narrow in definition.

Interpreting the implications of these Articles is not easy at present, but it would seem that this means that the data subject has to be informed about the implications of transferring data to *each* country.

Some of the issues that are raised have still to be fully clarified by the regulatory authorities. It is important to appreciate the difference where data is processed in a third country but is under the authority of a Data Controller (the person – or persons - in the company responsible for conformance to data protection legislation), compared with the situation where the data is transferred to another data controller.

The definition of 'personal data' is very broad, and in Article 2 of the Directive it is taken to mean any information relating to an identified or identifiable natural person. Furthermore the Directive applies even when a person's name is not listed but when the person can be identified by reference to an identification number (such as a staff number) or by any other means. This could well include photographs of otherwise anonymous individuals.

There has been a focus recently on the USA because of the volume of trade between Europe and the USA, but virtually all other countries of the world need to be considered. Some countries, such as Hong Kong, have promulgated or are preparing data privacy legislation along the lines of the EU Directive. However these countries are in a very small minority. The remaining countries have either very limited or no such initiative, and as a result these countries will be on the list of non-compliant third countries for some time to come. The reason for the emphasis on the words '*are complied with*' above is because the Commission is clearly seeking to indicate that any self-regulating situation must have very severe sanctions for non-compliance, and that is rarely the case in these countries at the present time.

Currently the only countries that have data privacy legislation that the Commission regards as being totally in line with the EU Directive are

- Argentina
- Canada
- Guernsey
- Isle of Man
- Switzerland

See [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm) for the documents from the European Commission.

## 5. The Lindqvist case

In 2003 the European Court of Justice ruled on a situation where Mrs. Lindqvist, a Swedish citizen, had published information about members of her local community on her web site. The Swedish authorities fined her for transferring data outside the EU, as the web pages were loaded onto an internet service host that although based in the EU provided access to her pages to anyone world wide. the ECJ concluded that it could not presume that the legislation intended the expression "transfer of data to a third country" to cover the loading by an individual of data onto an Internet page, even if those data are accessible by individuals in third countries. The Court concluded that activities such as those carried out by Mrs Lindqvist did not constitute a transfer of data to a third country provided the hosting provider was established in a European state (even if the provider uses a server outside the EC).

However this view was taken with regard only to Mrs. Lindqvist, and does not have a bearing on the internet service provider.

The full text of Case C-101/01 dated 6 November 2003 can be found on the ECJ web site <http://www.curia.eu.int/>. A useful summary has been prepared by the law firm of Bird and Bird <http://www.twobirds.com/english/publications/legalnews/websitesdata.cfm>

## 6. The situation in the USA

There is no explicit guarantee of privacy rights under the Constitution of the United States of America. In a number of judgements over the years the Supreme Court has created a variety of privacy rights out of the Bill of Rights and the Fourth and Fourteenth Amendments. The Fourth Amendment deals with the powers of the police to search for or seize records, and the Fourteenth with the restriction of the Government from compelling individuals to disclose certain personal information. However these constitutional rights only apply to government actions,

and not to the private sector. There was also a landmark article in the Harvard Law Review in 1980 by Samuel Warren and Louis Brandeis in which a series of four torts were set out under which certain violations of privacy could be brought before the courts, but in practice these have had little impact.

As a result in the USA there is no equivalent federal data privacy legislation, and there is unlikely to be for a considerable period of time. There are some related legislation, including the Video Privacy Act and the Telephone Consumer Protection Act, and some states do have some rather broadly-worded statutes, notably Massachusetts, and to a more limited extent Wisconsin.

The fundamental problem is that there is no clear legal remedies for breaches of data privacy. Instead the approach has been to set up industry-specific codes of practice that provide a measure of protection. In virtually every case there are no substantive penalties (such as cancellation of membership of the relevant industry association) for non-compliance, and this approach is not regarded by the EU as offering an adequate level of compliance.

To address this situation in 2000 the US Department of Commerce established a set of Safe Harbor Privacy Principles. <http://www.export.gov/safeharbor/> They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates in meeting the formal legal requirements of the European legislation. There is no legal redress for failing to conform to the Principles but any company in breach of these would certainly be under considerable pressure from the many other companies complying with these Principles. This is because the European Commission could, in theory, withdraw from their acceptance of the Principles and this could lead to considerable commercial problems in data management.

Participation in the Safe Harbor is entirely voluntary. Organizations that decide to participate in the safe harbor must comply with the Safe Harbor's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to self certify annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor protocol It must also state in its published privacy policy statement that it adheres to the Safe Harbor.

There is a good analysis of the European Commission viewpoint on these Principles at [http://ec.europa.eu/justice\\_home/fsi/privacy/thridcountries/adequacy-faq1\\_en.htm](http://ec.europa.eu/justice_home/fsi/privacy/thridcountries/adequacy-faq1_en.htm)

## **7. Contractual clauses for the transfer of information to non-EU countries**

Many companies were very concerned about the implications that the inability of the US to meet the EU criteria for data privacy compliance will have on their international operations, and a number of industry lobby groups were been set up.

Largely as a result of the efforts of these lobby groups in June 2001 the European Commission adopted a Decision setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union. The Decision obliges Member States to recognise that companies or organisations using such standard clauses in

contracts concerning personal data transfers to countries outside the EU are offering "adequate protection" to the data. The EU's Data Protection Directive (95/46/EC) requires all personal data transferred to countries outside the Union to benefit from "adequate protection". Use of these standard contractual clauses will be voluntary but will offer companies and organisations a straightforward means of complying with their obligation to ensure "adequate protection" for personal data transferred to countries outside the EU which have not been recognised by the Commission as providing adequate protection for such data.

The standard contractual clauses contain a legally enforceable declaration ("warrant") whereby both the "Data Exporter" and the "Data Importer" undertake to process the data in accordance with basic data protection rules and agree that individuals may enforce their rights under the contract.

The Commission Decision obliges Member States to recognise the contractual clauses annexed to the Decision as providing adequate safeguards and fulfilling the requirements of the Directive for data transfers to non-EU countries that do not provide for an adequate level of protection for personal data. However, the standard contractual clauses are neither compulsory for businesses, nor are they the only way of lawfully transferring data to third countries. They add a new possibility to those already existing under the Data Protection Directive, which establishes several cases where data may still be transferred to countries where the data protection regime is not adequate. These include cases where individuals have given their unambiguous consent for data to be transferred outside the EU and where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subjects. In addition, Member States' data protection authorities may authorise such transfers on a case by case basis when they are satisfied the data enjoys "adequate protection".

Data Protection Authorities in the Member States retain powers to prohibit or suspend data flows in exceptional circumstances, but the effect of this Decision is that they cannot refuse data transfers made under contracts that incorporate the standard contractual clauses approved by the Commission. The Decision also does not prevent national Data Protection Authorities authorising other 'ad hoc' contractual arrangements for the export of data out of the EU based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy.

In January 2005 the European Commission has approved a new set of standard contractual clauses.

[http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm)

Companies believe that some of the new clauses, such as those on litigation, allocation of responsibilities or auditing requirements, are more business-friendly. Yet they provide for a similar level of data protection as those of 2001 and to prevent abuses, the data protection authorities are given more powers to intervene and impose sanctions where necessary. The implementation of this new set of clauses will be reviewed in 2008.

Contractual clauses are not necessary to transfer data to Switzerland, Canada, Argentina and the UK territories of Guernsey and the Isle of Man, whose own regimes are recognised by the Commission as offering adequate data protection. Neither are they needed for transfers to US companies adhering to the 'Safe Harbor' Privacy Principles issued by the US Department of Commerce.

## 8. Intranet, internet and e-mail implications

The problems of conformance are not just related to intranets. The same issues apply to e-mails and any other form of transferring data, such as a floppy disk, or in a lap-top computer being taken out of the country. For example, sending details of an employee's cv to the USA from the UK without consent would be in breach of the legislation. There is a view by some companies that if they only send information to other sites of their company then the legislation does not apply. This is not the case, and full consent needs to be obtained.

Many web sites contain information about employees, especially in consulting companies, and since these sites can be accessed from virtually any country in then world then the consent of the individual to the information being posted on the site needs to be obtained.

Some intranets have an internal staff newsletter. In the interests of good communication there might be a news story about how a member of staff had been ill, but was now coming back to work for a few days a week. This is almost certainly sensitive personal data, as it related to the health of the person, and this should not then be circulated electronically without the permission of the person concerned.

It would certainly seem that individual employees will need to be issued with some form of amendment to their contract of employment which states what personal information is being sent (either by push or through pull) to other countries, and for what purpose, and their consent sought for this transfer. This will certainly apply to any cvs that contain personal information such as date of birth, sex, home address, or any information on religious beliefs etc.

Indeed one of the problems is working out just what is covered, and advice will need to be taken from lawyers specialising in data privacy, recognising that there is no case law at the present moment, and that in each country the data protection regulator, who is independent of the government, may take a different view on what is acceptable, especially in the early stages of the implementation of the Directive. At this time it seems unlikely that a generic clause which allows the company to send personal information around to any of its sites world wide for 'management purposes' would be permitted under the provisions of the Directive.

Many consulting projects, especially in human resources and change management, will require the consultants to check on personal information about employees. Using a corporate intranet from a single site to gain access to this information is likely to be forbidden, and of course if this information is to be held by a third party such as a consulting company, or an outplacement agency, then the employee's permission needs to be sought in advance. The employee also has the right to ensure that the information being held is correct, and this will require companies to implement intranet systems so that the employee can only see their own record, and not that of others. For employees that have left the company this right will extend as long as their file is maintained, which also gives rise to a range of problems, such as the time that a company should reasonably maintain that file.

The situation with applications for positions, and for information about free-lance staff, also needs careful consideration. It would seem that details about an applicant for a position in France, for example, cannot be transferred over an intranet to an office in the USA without the permission of the applicant. There are also issues with references provided by third parties, remembering that a person has the right to have access to any personal information about themselves, and they also have the right to amend this information if it is incorrect. Since all

intranets are assumed to be for the use of employees only, providing access to a third party needs careful consideration.

Another common situation is where a proposal is being prepared for an international client, and employee details are being accessed over an intranet to prepare the proposal. These details may include, for example, personal information concerning the employee's ability to work overseas for periods of time. If this information is exported from the EU to the USA it would seem that the employee will need to give their permission, and yet at that moment in time the company may not wish to disclose to the employee that they are being considered for the project.

A major issue with search log analysis, especially in the EU, is the data privacy issue. In reviewing intranet search logs there could be searches on voluntary redundancy, sexual harassment or discrimination or for the addresses of senior staff. All these might be taken as an indication that the person carrying out these searches was planning to take redundancy, sue the organisation for sexual harassment or discrimination, or send the addresses of senior managers to an animal rights activist group. The extent to which search logs might be construed to contain personal information has not yet been tested in the courts but the issue has come to the top of the agenda of data protection managers and legislators after AOL published details of the search logs of over 650,000 subscribers in July 2006.

The implications of this legislation and the Safe Harbor protocol is that only US companies working within the protocol can process personal data in the US from their operations in the EU. There is also a very important distinction between personal information and sensitive personal information.

Sensitive personal information covers

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or

One of the key issues is that a person has to give their informed consent for this information to be held in a database. To develop a scenario, assume that the HR database of a US organisation in Europe contains, with permission, information on the racial or ethnic origin of staff. Assume also that someone in the US wanted to check on which members of staff had a particular ethnic origin. The first issue is whether data privacy legislation would allow someone in the US to carry out that search, and it might well require authorization under the Safe Harbor protocols, and such authorization has not been given the search logs, in revealing the search, could potentially put the search team under a requirement to inform the organisation that such a search had been carried out.

It has to be understood that this is a hypothetical scenario, and is included only to highlight the complexities of data privacy legislation and the fact that to date search logs have probably escaped due attention. The AOL release of search logs has certainly changed that.

## 9. Conclusions and recommendations

The overall situation remains somewhat uncertain at present. There is still not a significant amount of guidance yet available from data protection regulators, or from the European Commission, and even the most expert of lawyers are finding it difficult to provide definitive advice.

Our recommendation at present is to plan for the worst case, and take the following actions.

- Become fully conversant with the Directive, and the current and proposed national legislation of all countries where you have current or potential clients and – especially – employees.
- Work with an experienced lawyer in each country to create standard agreements for employees to sign concerning the main uses to which personal information is stored and can be used, remembering that a blanket permission is unlikely to be sufficient.
- These lawyers should also be consulted on the applicability of the 2001 and 2005 set of model contracts to the business that you are in, and also start to assess the implications of the Safe Harbor approach for data transfer to the USA.
- Conduct a risk assessment on your business activities on the basis that a data regulator implemented your worst-case scenario, perhaps responding to a lead from a disaffected employee.
- Conduct a thorough audit of your intranet for personal information that could fall within the scope of the Directive.
- Set up a working party with trans-national representation from personnel, IT, intranet, and legal functions.
- Ensure that records are kept of the data sets on each server if these servers are in different countries, and the access to these servers from outside of that country.
- Consider that transaction logs and email records might be called as evidence by an employee that personal information was accessed in breach of the Directive.
- Consulting companies (in the broadest sense) in particular need to review the extent and purpose for which they hold personal information about employees, clients, prospects, associates and contractors. An important issue here is that consulting companies (and recruitment agencies) often retain such information for use in future assignments, and the data subject has the right to continue to examine their records for as long as the record is maintained.

## Web Resources

This section of the paper provides an evaluated set of resources, including books and newsletters as well as web sites. The links were checked and updated in January 2001. We would welcome suggestions for sites that should be added to this section.

### EU legislation and supporting documents

The primary source of official EU documentation on data privacy, including important Working Papers, is the DGXV web site [http://ec.europa.eu/justice\\_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/)

The Quick Links site <http://www.qlinks.net/quicklinks/dataprot.htm> is also an effective way of monitoring developments in the EU, with a good selection of news stories each day, and a categorised archive of these stories.

### US sites.

Many of the US-based sites do give a good coverage of data protection issues world wide, especially Privacy Exchange (<http://www.privacyexchange.org/>) and the Electronic Privacy Information Center (<http://www.epic.org/>). Both have good lists of links, and the EPIC site also lists newsgroups. Now that the Safe Harbor regulations have been agreed the US Department of Commerce (<http://www.export.gov/safeharbor/>) has set up a new web site specifically to provide information on the regulations

Issues for the corporate sector are well addressed by Privacy & American Business (<http://www.pandab.org/>), which has paid particular attention to human resources issues and which publishes probably the best newsletter covering data protection developments in the USA. Many of the leading US companies also support the Online Privacy Alliance (<http://www.privacyalliance.com/>), though there is little other than OPA material on the site.

To keep track of US Federal and State legislation, and the progress of current law suits there is no better source than Tech Law Journal (<http://www.techlawjournal.com/>)

### International

Although the scope of Privacy International (<http://www.privacy.org/>), a human rights group set up in 1990, is much broader than data privacy, it does offer a balanced global perspective on issues, and has a country-by-country assessment of data privacy issues for over fifty countries. The group is based on London and has an office in Washington.

As a companion to the newsletter from Privacy & American Business referred to above there is an excellent newsletter from the UK company Privacy Laws & Business (<http://www.privacylaws.com/>). A subscription to the newsletter also includes a hotline enquiry service. The company was set up by Stewart Dresner, who has been tracking developments in this sector for the last two decades, and runs a wide range of conferences.