Introduction

Companies that wish to sell products or services to consumers living in the European Union through the Internet face a wide variety of legislation, much of which is not uniform. The EU itself has issued a number of directives applicable to such activities under its general authority to establish standards for commerce among EU member nations and continues to work on additional directives. However, EU directives are not themselves law and require action by each member state to implement them. Implementation typically occurs at different times and is often accomplished through legislation that may differ in some respects from the directive itself, although the legislation may not be less strict than required by the Directive. Therefore, while the directives achieve uniformity in a broad sense, certainty of compliance with the specifics of laws regulating electronic commerce in each of the EU’s member states requires a review of the laws of each nation.

The EU’s Directives are quite technical and are not fully understood by many. The purpose of this article is to provide a summary of EU Directives affecting electronic commerce in order to facilitate a review of legal issues faced by persons wishing to conduct e-commerce activities in the EU and in the European Economic Area (the “EEA”, which includes EU and non-EU nations).

Directive on Data Protection (often referred to as the “EU Privacy Directive”) (Directive 95/46/EC available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett). Under this Directive (which has also been implemented within EEA), member states have adopted legislation to regulate government and business use of personal data. In general, the Directive

- states that personal data may not be processed (except in cases of necessity) without the consent of the person and requires disclosure of information practices by entities that collect information, such as Web site operators; and
prohibits the transmission of personal data out of the EEA to countries whose laws do not provide an adequate level of data privacy protection.

When the Directive became effective, the EU took the position that the privacy laws of the entire rest of the world did not provide adequate protection. Since that time, the EU has declared the privacy laws of Argentina, Canada, Guernsey, Hungary and Switzerland to be compliant.

For companies located in non-compliant countries, there are exceptions and alternatives that are available to avoid violation of the Directive.

The most common exception is adherence to the “Safe Harbor Principles,” negotiated in 2000 between the U.S. Department of Commerce and the European Commission. The Safe Harbor Agreement allows U.S. companies that are subject to regulation by an independent statutory body with jurisdiction to hear complaints against the organization with respect to privacy issues (the FTC and the Department of Transportation are the only two bodies that have been so recognized); to exempt themselves from the Directive by self-certifying that they will be bound by seven privacy principles (notice, choice, onward transfer (i.e., requiring third parties to be bound by the principles), security, data integrity and access to correct or remove information). Companies electing Safe Harbor will be placed on an EU Safe Harbor list thereby permitting the transfer of personal data from the EEA, without violation of the Directive.

Initially following its adoption in 2001, few U.S. companies elected to sign up for the Safe Harbor on the basis that the Safe Harbor requires compliance obligations that are significantly greater than existing U.S. privacy standards. However, as EU enforcement of the laws adopted under this Directive has increased, an increasing number of U.S. companies have been signing on to Safe Harbor (469 as of this writing). Some companies are choosing to certify only those portions of their database that are subject to the Safe Harbor requirements.

Since EU member states are implementing the Directive somewhat differently, U.S. companies which have not opted for Safe Harbor are required to disclose their data collection policies to, and obtain the consent of, the data protection authority of each member country.

Alternatives to Safe Harbor to ensure the uninterrupted flow of data may be available in certain circumstances. One such alternative is to use standard contractual clauses that have been adopted by the European Commission. These clauses are intended to provide adequate protection for transfers of personal data from out of the EEA by creating legally enforceable covenants to process the data in accordance with basic data protection rules and to permit individuals to enforce those contract rights.
Other alternatives include obtaining the unambiguous consent of the subject of the data transfer or negotiating directly with the data protection authorities in each member state from which data will be transferred.

However, each of these alternatives involves a number of significant issues and this entire issue is one that requires careful analysis for each individual company’s circumstances.

The failure to implement a means of compliance with or exemption from the Directive can result in serious consequences for violations, with penalties that can include fines up to € 600,000 and a cut off of data flow.

**Directive on Protection of Consumers in Respect of Distance Contracts 97/7/EC**

The EU Directive on Protection of Consumers in Respect of Distance Contracts is intended to provide protection to consumers by providing a legal framework for e-commerce and other “long distance” sales transactions in which buyer and the seller are not physically present in the same location at the time of the transaction. It is applicable to non-EU businesses that do business with EU consumers. The Directive requires businesses to comply with a broad range of solicitation and sales practices, including the following:

- Consumers must be given written confirmation of electronic contracts entered into online.
- Consumers have the right to revoke such contracts without cause within seven days of receipt of confirmation. If no confirmation is provided, the period within which the transaction may be revoked without cause is extended to within three months of (i) receipt of the goods or (ii) conclusion of the contract for services. Revocation is without charge, except for the cost of returning any goods delivered under the contract.
- Unless otherwise agreed, suppliers must fulfill orders within 30 days. If not, the supplier must inform the customer and provide a refund as soon as possible but in any event within 30 days.
- Prior consent is required for communications through fax and automated calling systems.
- If a contract has a close connection with the territory of one or more EU member states, the Directive’s protection cannot be lost notwithstanding a contract’s choice of a non-EU country’s laws.

The Directive does not apply to certain categories of contracts including those relating to foods and beverages, accommodations, transport, catering or leisure services, newspapers, periodicals, magazines or gaming or lottery services.

**Directive on Community Framework for Electronic Signatures 1999/93/EC**
This Directive defines the requirements for electronic signature certificates and certification services. Its key elements are
- Electronic signatures cannot be discriminated against if they meet certain specific requirements, in which case they will be given the same validity as hand-written signatures.
- Electronic signatures may be used as evidence in legal proceedings

**Directive on Electronic Commerce 2000/31/EC**

In order to encourage e-commerce, this Directive requires member states to remove legal impediments to the enforceability of electronic contracts. Among other things, this Directive

- Makes clear that click-through agreements are enforceable, while still requiring that electronic contracts satisfy the same substantive requirements imposed on traditional written contracts.
- Requires an exemption from liability for intermediaries which act as a mere conduit of information from third parties and limits service providers’ liability for other intermediary activities such as the storage of information.
- Requires that commercial e-mail communications be clearly identifiable.
- The provision of online services by regulated professions (such as lawyers or accountants) is permitted and national rules on online advertising may not prevent professions from operating web sites.

**Directive on Value-Added Tax Arrangements 2002/38/EC**

The Directive, effective July 1, 2003, provides that “electronically-supplied services” which are provided:

1. by persons based in and acting out of non-EU countries ("Non-EU Suppliers");
2. to non-business organizations or private individuals (or other non-VAT registrable persons) within the EU ("EU Non-Business Customers"), will be subject to VAT in the EU member state where the customer is based.

No definition of "electronically-supplied services" is provided, but the Directive provides the following illustrative list:

1. the supply of a website, web-hosting and the distance maintenance of programs and equipment;
2. the supply and updating via download of software;
3. the supply via download of images, text and information (for example, electronic publications), and making databases available;
4. the supply via download of music, films and games (including games of chance and gambling games), and of political, cultural, artistic, sporting, scientific and entertainment broadcasts and events; and

5. the supply of distance learning via the Internet.

Non-EU Suppliers supplying "electronically-supplied services" to an EU recipient who is receiving the services for the purposes of its business will not have to charge EU VAT on the services. Instead, the EU recipient must itself account for the VAT (if any) that may be chargeable on the supply.

Non-EU Suppliers supplying "electronically-supplied services" to EU Non-Business Customers will be supplying services within the EU. If no applicable exemption applies (for example, securities and stock brokers are exempted), the Non-EU Supplier will be required to register and account for VAT in each EU member state in which it has an EU Non-Business Customer.

To address the administrative difficulties of registering in all EU countries, the Directive provides that a non-EU Supplier with no presence in the EU may register for VAT electronically in one EU member state only.

The Directive treats broadcasting services (including cable and satellite broadcasting) similar to "electronically-supplied services" for purposes of accounting for VAT on its provision.

**Directive on Privacy and Electronic Communications 2002/58/EC**

In addition to the EU Privacy Directive 95/46/EC, the EU adopted the Privacy and Electronic Communications Directive which addresses spam and other unsolicited electronic messaging solicitations including telephone, email and instant messaging. Member states were required to implement this directive into law by October 30, 2003.


- **Opt-in for Spam** – A recipient’s prior permission is required before sending unsolicited marketing emails to individuals. Certain exceptions are provided for existing customers.
- **Spyware, web bugs, hidden identifiers and other similar devices** - should be allowed only for legitimate purposes, with the knowledge of the users concerned.
- Cookies – Cookies may only be used for legitimate purposes (such as verifying the identity of a user). Visitors must be provided with “clear and comprehensive information” about any cookies or other similar devices, including the purpose of such processing, and be provided with the option to refuse them. Web site access may be conditioned on the acceptance of cookies.

- Directories – Subscribers must be given a choice as to the inclusion of their personal data in any listing of subscribers to a service.

- Providers of publicly available electronic communications must implement appropriate security measures.

- Traffic data of users and subscribers (data used to establish communications and transmit information) and only be stored to the extent necessary for the provision of the services and must be erased when no longer needed for the purpose of the transmission.

- Location data (such as the geographic position of the terminal equipment of a user) may only be processed when made anonymous or with the consent of the user and then only to the extent of and for the duration necessary for the provision of a value added service.

- The use of automated calling systems are only permitted with respect to natural persons who have given their consent.

Directive 2002/58/EC is applicable to the processing of data through networks in the EEA and therefore making use of equipment for the processing of consumers’ personal data through the use of equipment, automated or otherwise, situated in an EEA state, is subject to the Directive. The mere transit of personal data such as through the telecommunications networks of the Internet is not covered by the Directive. Significantly, the consumer need not be an EEA resident or citizen. The Directive applies if the processing equipment (examples are computers, terminals and servers) is located within the EEA. For example, sending cookies to an EEA personal computer to collect personal data would involve the processing of such data through equipment located in the EEA. In such case, the implementing law of that state will apply.

**Conclusion**

With a population of 455 million people in 25 countries and a high level of economic and consumer activity, it is difficult to ignore the EU in developing e-commerce-based marketing plans. For persons wishing to operate in that market, it is important to recognize that, for some time, the EU has been leading the world in the adoption of laws to protect the privacy of individuals, with the EU Privacy Directive being generally recognized as the single most important privacy initiative that has been adopted anywhere. Approximately 50 other nations have now adopted legislation that significantly follows the principles set forth in the EU Privacy Directive. At the same time, the EU has been active in defining other, more commercial aspects of e-commerce activities that have broad application.
Although determining whether given Directives apply to specific e-commerce activities of non-EU based companies can sometimes be a complex exercise, the Directives should be recognized as establishing a de facto baseline for major segments of international e-commerce activities. Accordingly, companies engaged in international e-commerce should take the appropriate steps to understand the EU Directives and their potential application to their activities. A sound approach would be to develop standards for the conduct of e-commerce that comply with the Directives and, as to the highly important Directives impacting on privacy, also constitute a code of conduct that is in harmony with the worldwide concern for the eroded privacy of Internet users.

______________

Robert A. Hudson practices in the areas of business, securities and e-commerce law. He is the Chair of Butzel Long’s Business Law Group and Co-Chair of the firm’s Technology and E-Commerce Group. He is the co-editor of the Michigan Business Formbook (Institute of Continuing Legal Education), author of the Formbook’s chapter on Electronic Commerce and E-Business Issues and the author of Developing a Web Site in A Practical Guide to E-Business Law (Institute of Continuing Legal Education). He frequently lectures on topics involving e-commerce, business and securities law issues including special issues relating to emerging high-technology companies. He is listed in The Best Lawyers in America.

His contact information is as follows:

Robert A. Hudson
Butzel Long
150 W. Jefferson, Ste. 100
Detroit, MI 48226-4450
Tel.: (313) 225-7019
Fax: (313) 225-7080
Email: hudson@butzel.com