

Privacy Law 2009: A Year of Change

Ann E. Tobin
Senior Privacy Counsel,
UnitedHealth Group Incorporated

**Ross C. D'Emanuele, Barry D. Glazer,
Melissa J. Krasnow and William R. Stoeri**
Dorsey & Whitney LLP



Privacy Laws

State

Data breach notification

Social Security number

Payment card

Encryption
(Nevada)

Encryption
(Massachusetts)

Security procedures

Document destruction

Federal

Federal Trade Commission

Cases

Red Flags Rule

Guidance

Notice of Address Discrepancy Regulation

Fair and Accurate Credit Transactions Act Disposal Rule

Health Insurance Portability and Accountability Act
Health Information Technology for Economic Clinical Health Act

New York Stock Exchange Rule

International

European Union Data Protection Directive

Other European Union Laws



The American Recovery and Reinvestment Act of 2009

- Signed into law February 17, 2009
- Title XIII, Subtitle D (HITECH ACT) significantly expands HIPAA Privacy and Security Law
 - Business Associates
 - Breach Notification
 - Penalties/Enforcement



What is a Business Associate?

- Anyone who, on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information; or
- Provides legal, actuarial, accounting, consulting, management, administrative, accreditation or financial services for the covered entity that involve the disclosure of individually identifiable health information from the covered entity to the person.

45 C.F.R. Section 160.103



HIPAA Security Rules Now Directly Applicable to Business Associates

- Previously, BAs were subject only to the BA Agreement
- ARRA makes BAs subject to direct HIPAA Security regulation by HHS



Security Rules

- Administrative Safeguards – 45 C.F.R. Section 164.308
- Physical Safeguards – 45 C.F.R. Section 164.310
- Technical Safeguards – 45 C.F.R. Section 164.312
- Policies and Procedures and Documentation Requirements – 45 C.F.R. Section 164.316

Compliance Date: February 17, 2010



Breach Notification

Notification must occur upon discovery of a breach of “unsecured” protected health information

Breach occurs if there is “significant risk of harm”

Form and Content of Notice Mandated

May Require Media Notice

Notice to HHS immediately if more than 500 individuals affected; otherwise annual log submitted

74 Fed. Reg. 42740 (August 24, 2009)



Penalties/Enforcement:

- New Tiered Penalties with Potential for \$50K per Violation with no Ceiling
- State AGs Can Enforce
- Audit Authority
- Whistleblower Rules
- HHS Must Impose Penalties if Willful Neglect
- Personal Liability?

13409 – 13411 of HITECH Act



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

Barry D. Glazer
Dorsey & Whitney LLP
London



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

A. Background

1. The first data protection laws in Europe date from the 1970's in Germany and France.
2. In contrast to the United States, the EU approach has been to enact a broad directive governing the protection of personal data rather than industry or sector specific legislation.
3. The EU Privacy Directive (1995/46/EC) enacted in 1995 is the basis for data protection laws implemented in each of the 27 EU member countries.
4. Other EU laws of importance to data privacy are the Directive on Electronic Communications Services (2002/58/EC) relating to security of electronic communications services and the e-Commerce Directive (2000/31/EC).
5. The EU data privacy concepts have on occasion presented challenging conflicts with US law. Recently, however, evolving privacy law in the US has served as a guide to the further expansion of data protection within the EU.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

B. The EU Privacy Directive – Scope and Jurisdiction

1. The Directive applies only to “Personal Data”
 - a) defined as any information relating to an identified or identifiable natural person. Data is identifiable personal data when it allows a person’s identity behind the data to be recovered directly or indirectly;
 - b) excludes corporate data and anonymous data.
2. The Directive covers “Processing of Personal Data”, which includes any operation performed upon personal data, including manual and automatic collection, recording, storage, retrieval, use, disclosure and transmission of personal data.
3. The Directive applies to the processing of Personal Data by a Data Controller (the person who determines the purpose and use of the data processing) or a Data Processor (the person executing the processing for a data controller).



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

B. The EU Privacy Directive – Scope and Jurisdiction (cont'd)

4. The Directive raises complex issues of jurisdiction. As between the data protection laws of the various EU member countries, the country where the processing is carried out and the data controller is established applies. If a data controller is not established in any EU country, the EU privacy laws apply if the processing of personal data makes use of equipment situated within a EU member country unless the equipment is used only for purposes of transit through the country.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

C. The Overall Principles of the EU Data Protection Laws

1. Personal Data must be processed fairly and lawfully;
2. Personal Data must be collected for specific and legitimate purposes;
3. Processing of Personal Data must be relevant and not in excess of the purposes for which the data was collected;
4. The Personal Data must be accurate and where necessary kept up to date; and
5. Personal Data must be kept in identifiable form only as long as necessary for the purposes for which the Personal Data was collected.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

D. Principal Obligations imposed on a Data Controller under EU Law

1. Processing of Personal Data can only take place if :
 - a) the Data Subject has given his unambiguous and explicit consent;
or
 - b) the processing of the Personal Data is necessary for the performance of a contract to which the data subject is a party;
or
 - c) processing meets certain other exemptions allowed by the law.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

- D.** Principal Obligations imposed on a Data Controller under EU Law (cont'd)
- 2.** Sensitive Personal Data is given special treatment and generally may not be processed without the Data Subject's explicit consent. Sensitive Personal Data includes social or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life. Certain exemptions apply, particularly where processing is required to deliver health care services.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

D. Principal Obligations imposed on a Data Controller under EU Law (cont'd)

3. The Data Subject must be provided with information when the his personal data is collected, including:
 - a) the identity of the Data Controller;
 - b) the intended purposes of the data processing;
 - c) any further information necessary to guarantee fair processing, such as the identity of the recipients of the data, whether or not responses to questions are obligatory and the existence of the right of access and correction of the data concerning the data subject.
4. After collection, upon inquiry from the Data Subject, the Data Controller must provide the Data Subject with confirmation that data relating to him is being processed and grant the right to access and correct any inaccurate data.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

D. Principal Obligations imposed on a Data Controller under EU Law (cont'd)

5. The Data Controller must take measures to ensure an appropriate level of security for the Personal Data taking into account the level of risks and nature of the data;
6. If the Data Controller confers processing of the data to a third party, the Data Controller must enter into a binding contract with the Data Processor to assure that the Data Processor only acts on instructions of the Data Controller and adheres to the same security obligations.
7. The Data Controller must notify the appropriate national Data Protection Authority (DPA) prior to commencing data processing operations (subject to various exemptions allowed under national law); and
8. Personal Data cannot be transferred to countries outside the EU unless the third country provides an “adequate level of protection” for Personal Data (subject to certain derogations discussed below).



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

- E.** Transfers of Personal Data Outside the EU – Conflict Resolved?
1. The prohibition in the EU Directive against transfers of Personal Data to countries not according an “adequate” measure of protection to Personal Data has presented problems for US based multinational companies.
 2. The EU has only certified a limited number of countries it considers to have an adequate level of protection (currently Argentina, Canada, Guernsey, Isle of Man and Switzerland). Because the US does not have a general comprehensive data privacy law, the US is not on the approved list.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)

3. Regardless of the country outside the EU to which the Personal Data is to be transferred, the transfer can legally take place if:
 - a) the Data Subject has given his unambiguous consent to the transfer;
 - b) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller;
 - c) the transfer is necessary for the conclusion or performance of a contract between the Data Controller and a third party concluded “in the interest of the Data Subject”;
 - d) the transfer is necessary or required for the establishment, exercise or defense of legal claims; or
 - e) the transfer is necessary to protect the vital interests of the Data Subject.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

- E.** Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)
4. The above exceptions often are problematic. For example, obtaining the consent of all Data Subjects may be impractical in a commercial context. In the case of a US parent's foreign affiliates' employees, some employees may refuse to consent to the transfer of their Personal Data to the US. Additionally, the validity of an employee's consent is not uniformly accepted in all EU countries because of concerns about coercion.
 5. Other means of legally transferring EU Personal Data to the US have been approved by the EU:
 - a) Standard Data Export Contracts (the original form of standard contract approved by the EU for transfer of data from controller to controller or from controller to processor or the ICC alternative model contracts for transfers between controllers).



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)

- i. The Data Controller remains liable to the Data Subject for breaches of security under all of the approved contracts forms; under the original standard contracts the data importer and data exporter have joint liability;
- ii. The contract is normally bilateral and therefore cannot cover a number of data exporters in different EU countries;
- iii. The contracts are subject to prior notice and/or approval requirements in a number of EU countries (e.g. France and the Netherlands); and
- iv. Courts of the EU country where the data exporter is located retain jurisdiction over the parties, including claims by Data Subjects who are third party beneficiaries.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)

b) US Safe Harbor

- i. Provides self-certification of the US data importer that it provides for adequate protection to the specific type of Personal Data listed in the certification;
- ii. Enforcement remains in the US through the FTC (or the Department of Transport if applicable);
- iii. Is not available for use by financial institutions, telecommunication carriers or non-profit organizations;
- iv. Requires adherence to the Safe Harbor Principles, which essentially mirror the EU Data Protection Principles;
- v. Requires annual self-certification, periodic auditing of compliance and the establishment of a dispute mechanism for resolution of disputes brought by Data Subjects.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)

c) Binding Corporate Rules (BCR)

- i. First proposed in 2003, the BCR exemption from the cross-border prohibition on Personal Data transfers is a specifically structured internal code of conduct intended to allow a multinational group of companies to transfer Personal Data intra-group to affiliates anywhere within the world while assuring the security of the data and the rights of the Data Subjects.
- ii. The BCR are subject to the initial authorization of the national data protection supervisory authority in one of EU member countries. Determination of which country's supervisory authority is the "lead authority" is based on a number of factors, including where the group has its European headquarters, where an affiliate with delegated responsibility for data protection matters is located, where the most transfers out of the EU take place and the group affiliate within the EU best placed to enforce the BCR.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont'd)

- iii. The application for approval of the BCR must contain extensive information on the binding nature of the BCR within and outside the group, including details of a data protection audit plan, the security safeguards to be put into place for the personal data, description of the training program to be instituted, the processing and flow of information and the mechanism for reporting and complaints.
- iv. Despite the submission of the application to the lead authority in one EU country, the other EU countries from which personal data will be exported must approve the BCR. Partly as a result of this cumbersome requirement in the past very few multinational companies have sought approval for data transfers on the basis of the BCR exemption.
- v. The BCR must contain a duty for the EU headquarters or the delegated EU affiliate to accept responsibility for and remedy acts of members of the group outside the EU and to pay compensation for any damages resulting from violation of the BCR by group members. Any data subject has the right to bring an action for damages in EU courts for acts in violation of the BCR occurring outside the EU. The burden of proof lies with the company and not the individual Data Subject.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

F. Recent Developments in EU Data Protection Law

1. Binding Corporate Rules

- a) The requirements for the BCR procedure for intra-group Personal Data transfers have been clarified by the issuance of a standard form checklist for the content of a BCR as well as the application form for the lead authority approval.
- b) A mutual recognition procedure has been established whereby the approval of the lead authority in one EU country will satisfy the approval requirement for all other EU countries that have agreed to the procedure, rather than having to obtain the separate approval of each EU country from which data will be exported. At present, 18 of the 27 EU countries have subscribed to the mutual recognition procedure.
- c) As a result of these recent changes, the BCR procedure is likely to be viewed more seriously by multinational companies as a realistic legal means of transferring Personal Data among group affiliates outside the EU.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

F. Recent Developments in EU Data Protection Law (cont'd)

2. Data Breach Notification Requirements – Convergence with US law?

- a) Although the EU Privacy Directive requires that Data Controllers must implement “appropriate technical and organizational measures” to protect personal data against accidental or unauthorized loss, destruction or disclosure, neither the Directive nor most of the national implementing laws impose a specific duty to notify either the national data protection authority or the Data Subject in the case of a data breach.
- b) A number of highly public data breaches within the EU in recent years as well as the increasing regulation of data breaches in the US have brought demands for increasing the obligations of a Data Controller in the event of a data breach in the EU.
- c) The EU has proposed imposing a mandatory notification requirements on public electronic communication service providers (essentially telecommunication and internet service providers) for data breaches, but there are increasing calls for a general US style data breach notification requirement to be added to the EU data privacy laws.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

F. Recent Developments in EU Data Protection Law (continued)

- d) Data breaches are to some extent covered in certain sectors at the national level. For example, financial companies in the UK regulated by the Financial Services Authority (FSA) are subject to fines for lax security procedures and controls. In a recent case, a national savings and loan company was fined nearly £ 1 million as a result of its mishandling of a laptop computer containing sensitive customer data stolen from an employee's home.

3. Sarbanes-Oxley (SOX) Whistleblowing Compliance Schemes – Conflict with EU Privacy Laws?

- a) The SOX requirement for the establishment of a hotline for communicating employee complaints has raised difficult issues under European laws.
- b) One of the most significant conflicts with US law relates to the perceived conflict between the requirement imposed by SOX for the availability of submitting whistleblowing complaints anonymously and the protection of individual employees' labor and data privacy rights.



DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

F. Recent Developments in EU Data Protection Law (cont'd)

- c) Several EU countries, most notably France, the Netherlands and Germany as well as the EU Committee of national data privacy supervisors, have issued guidance notes designed to define the extent to which whistleblowing hotlines can be implemented consistent with EU data privacy concepts. The guidance notes render the hotline less effective.

4. Employer monitoring of employee e-mails

- a) While common in the US, monitoring of employee e-mails in the EU presents data privacy issues in a number of countries, including potential criminal penalties.
- b) The regulatory interpretation of the employer's right to monitor versus the employee's expectation of privacy of communications varies considerably among EU countries.

