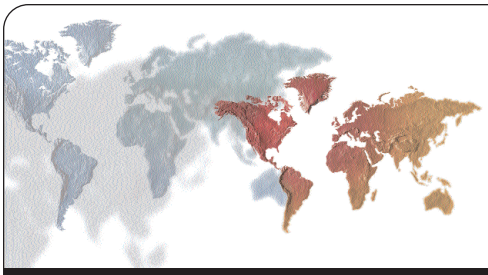


SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

SEPTEMBER 25, 2003

PRIVACY AND DATA PROTECTION ALERT

Privacy, Data Protection and Information Security Practice Group

Sidley Austin Brown & Wood LLP offers clients an inter-disciplinary, international group of lawyers focusing on the complex issues of privacy, data protection, information security, consumer protection and cybercrimes. Members of the Privacy Group are based primarily in Washington, New York, London, Chicago, Brussels, and Los Angeles. The Group includes intellectual property lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, and regulatory and white collar lawyers.

If you would like more information on the Privacy, Data Protection and Information Security Practice Group, please contact:

Alan Charles Raul
202-736-8477
araul@sidley.com

To receive future copies of the Privacy and Data Protection Alert via email, please send your name, company or firm name and email address to lhersh@sidley.com

EU Data Protection: "Binding Corporate Rules" as an Alternative to the "Safe Harbor" for Multinationals that Transfer Data to the U.S.

Global corporations with offices or customers in the European Union should be aware of the latest European Union proposal for compliance with its Data Protection Directive 95/46/EC (EU Directive) with respect to internal transfers of information among members of the same corporate group. Interested parties will be submitting comments through September 30, 2003.

The EU has now indicated that "binding corporate rules" - *i.e.*, a stringent, intra-corporate global privacy policy that satisfies EU standards - may be available as an alternative means of authorizing transfers of personal data (*e.g.*, customer databases, HR information, etc.) outside the EEA.[1] A recent discussion document, "Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers," (click here to view the full document), indicates that the EU is favorably disposed to the idea that multinational companies should be able to establish a global privacy policy that satisfies European data protection requirements.

Current Compliance Options

Under the EU Directive, personal information concerning EU residents may not be transferred to countries, such as the United States, whose data protection laws have not been deemed "adequate" by the EU.[2] This prohibition applies to intra-corporate data transfers from a company's EU offices to its locations in the U.S.

Prior to the EU's recent pronouncement, the main avenues to legitimate data transfers outside the EEA to countries who have not been deemed adequate included: (1) membership in the "Safe Harbor"

[1] The EEA currently consists of the EU Member States (Austria, Belgium, Denmark, Ireland, Finland, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and United Kingdom) together with Iceland, Liechtenstein and Norway. A further ten new Member States will join the EU in 2004.

[2] Currently Canada, Hungary and Switzerland have been deemed adequate by the EU.

negotiated between the U.S. and EU; (2) adoption of "model contract language" to comply with the provisions of the EU Directive; (3) use of *ad hoc* contracts determined to provide adequate protection; (4) meeting one of several specific conditions such as obtaining the unequivocal consent of the data subjects, transferring data when necessary for the performance of a contract with the data subject or in its interest, or when necessary or legally required for legal claims.

Each of these compliance methods is onerous or problematic. For example, the Safe Harbor and model contract approaches are especially incongruous when applied to multinational business entities that operate both inside and outside of the EU, but yet transfer data relatively freely among its units. The Safe Harbor's provisions are indeed structured for the transfer of data between separate entities, building in extra steps of agreements and safeguards that do not comfortably fit the operations of an integrated corporate operation. Meanwhile, the pre-approved model contract provisions introduce complications such as granting outside audit rights and establishing burdensome joint and several liability provisions. Obtaining consent or meeting one of the other specific conditions is also often difficult. Indeed, some data protection authorities have suggested that employee consent to an employer's transfer would not be considered valid.

A New Possibility For Compliance

Aware of these criticisms, the EU has suggested in a recent "Working Document" that "binding corporate rules" - in essence, a unified, international privacy policy - may be an adequate means of addressing the concerns present for international data transfers. The current EU proposal has been published for comment by interested parties, and presumably for Member State Data Protection Authorities, as well as multinational companies, to develop into actual working models. We believe that there is considerable potential in this approach to complying with the EU Directive. Indeed, over two years ago, Sidley advocated "Direct Compliance" strategies that rest on member state recognition of a corporation's own internal review and certification of its privacy practices. *See*, *e.g.*, "The Third Way: 'Direct Compliance': A New Strategy for Complying with the EU Data Protection Directive" (April 12, 2001). Click here to view the document on Sidley's cyberlaw site. The danger, however, is that the EU Working Party - which consists entirely of regulators - will devise a new avenue that is too onerous or prescriptive to be practical.

Under Direct Compliance strategies, or what the EU is calling "binding corporate rules," multinational companies adopt procedures to implement the fundamental principles of the EU Directive throughout the entire organization. Under this approach, related parts of the same business would apply one uniform set of approved rules to their international data transfers. Moreover, these rules could also be drafted to comply with privacy laws in other countries as well. (These are distinct from the codes of conduct under Article 27 of the EU Directive).

Under this approach, a multinational organization adopts a global data protection policy that directs all units of the company, wherever located, to comply with the EU Directive's underlying principles with respect to personal information transferred from the EU. Such a policy brings the organization's data transfer up to the strictest common denominator, and thus has the effect of exporting

EU data restrictions throughout the organization.

The Working Party has indicated that binding corporate rules would need to include substantial required content that may, unless tempered, make the "binding corporate rule" approach too onerous for most corporations. In particular, the Working Paper would require a corporation to adhere to the strictest EU national data protection regime applicable to that company (*i.e.*, the most stringent country in which the company operates).

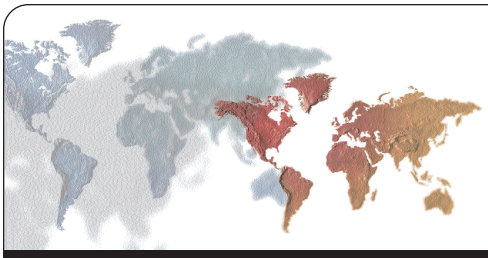
Under the Working Party's suggestions, a single entity would be required to be designated in the EU as the site for coordination, complaints, remedies and compensation. This entity would be potentially subject to data subject suits for violations of the rules, would need to be sufficiently capitalized to pay any suits, and would be required to pledge cooperation with the advice of relevant EU Data Protection Authorities (DPAs). Corporate rules would be submitted for approval to the DPAs of each country from which the company would be exporting personal data. Corporate rules would be required to provide "third party beneficiary" rights to EU data subjects, thereby allowing them to sue to enforce the rules. The EU's proposed binding rules would also be required to contain detailed descriptions of the types of information being collected and processed and the restrictions on such activities.

EU Comment Solicitation

The EU Working Party comment solicitation provides an opportunity to encourage the EU to adopt reasonable "binding corporate rules."

The EU's Working Party has expressed its interest in receiving feedback from interested parties on the use of binding corporate rules. It is also planning a public hearing at the beginning of 2004. The deadline for initial comments, however, is September 30, 2003.

Please let us know if you are interested in more information. Please see the following description of Sidley's Privacy, Data Protection and Information Security Practice Group for additional details on the Firm's expertise in this area.



SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

PRIVACY, DATA PROTECTION AND INFORMATION SECURITY PRACTICE GROUP

International and Inter-Disciplinary

Sidley Austin Brown & Wood LLP offers clients an inter-disciplinary, international group of lawyers focusing on the complex issues of privacy, data protection, information security, consumer protection and cybercrimes. Members of the Privacy Group are based primarily in Washington, New York, London, Chicago, Brussels, and Los Angeles. The Group includes intellectual property lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, and regulatory and white collar lawyers.

In addition to their extensive private practice experience, the Privacy Group's lawyers also draw on significant U.S. Federal Government background in the White House, Executive Office of the President and Department of Justice. Members of the Group include a former FTC Commissioner, three former Associate Counsels to the President, a former General Counsel of the Office of Management and Budget (OMB), a former senior lawyer in the Justice Department's Computer Crime and Intellectual Property Section, and former senior FCC lawyers.

The Firm's Privacy lawyers provide strategic counseling, regulatory compliance and litigation services. For example, the Firm represented the defendant in a landmark privacy case, where the Second Circuit held that transfers of personal information collected by a company do not necessarily cause injury or give rise to cognizable damages (*Conboy* v. *AT&T Corp.*). The Firm's client prevailed over plaintiffs who claimed that it had improperly distributed their customer proprietary network information (CPNI). The Firm also successfully represented a defendant in the Pharmatrak privacy litigation, where plaintiffs in a purported class action sought damages for Internet users who allegedly visited various pharmaceutical company websites that relied on "cookies" to track Internet usage and traffic. The Court granted the Firm's motion for summary judgment on all counts.

Firm lawyers have drafted numerous privacy policies and notices, and have also assisted companies in establishing privacy and security compliance programs, responding to new telemarketing and e-commerce requirements, evaluating membership in the US/EU Data Protection "Safe Harbor," and drafting and commenting on privacy legislation and testimony, and the proposal and adoption of standards, best practices and recommendations by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C).

Members of the Firm's Privacy Group have published numerous articles on privacy and information security topics, including two leading books:

> ***Privacy and the Digital State*** (Kluwer Academic Publishers 2001)
>
> ***Intellectual Property and Computer Crimes*** (Law Journal Press 2003).

The Group publishes many of its articles on data protection and information law topics on the Firm's CyberLaw site at www.sidley.com/cyberlaw.

Lawyers in the group actively monitor and analyze legislative and judicial developments under the following representative legislative authorities:

U.S. Federal and State Laws

- Electronic Communications Privacy Act
- USA PATRIOT Act
- Computer Fraud and Abuse Act of 1986
- Federal Trade Commission Act
- Gramm-Leach-Bliley Act (Title V)
- EU Safe Harbor
- Health Insurance Portability and Accountability Act (HIPAA)
- Stored Wire and Electronic Communications Act
- Fair Credit Reporting Act and similar state laws
- State Unfair or Deceptive Acts and Practices Statutes
- Telemarketing and Consumer Fraud and Abuse Prevention Act
- Telephone Consumer Protection Act
- Fair Credit Reporting Act
- Anticybersquatting Consumer Protection Act
- Lanham (Trademark) Act
- Digital Millennium Copyright Act

EC Legislation

- The Data Protection Directive (1995/46/EC)
- The Distance Selling Directive (1997/7/EC)
- The Electronic Signatures Directive (1999/93/EC)
- The E-Commerce Directive (2000/31/EC)
- The Distance Marketing of Consumer Financial Services Directive (2002/65/EC)
- The Electronic Communications and Privacy Directive (2002/58/EC)
- Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

Statutes Under English law

- Computer Misuse Act 1990
- The Regulation of Investigatory Powers Act 2000
- The Communications Act 2003

Please contact the following lawyers in the Privacy Group for more information:

Washington

Alan Charles Raul
202-736-8477
araul@sidley.com

Andrew J. Strenio
202-736-8614
astrenio@sidley.com

Michael F. McEneney
202-736-8368
mmceneney@sidley.com

Bradford A. Berenson
202-736-8971
bberenson@sidley.com

Frank R. Volpe
202-736-8366
fvolpe@sidley.com

Anita L. Wallgren
202-736-8468
awallgren@sidley.com

Edward R. McNicholas
202-736-8010
emcnicholas@sidley.com

New York

Peter J. Toren
212-839-7355
ptoren@sidley.com

Alan L. Jakimo
212-839-5480
ajakimo@sidley.com

Chicago

Jeffrey S. Rothstein
312-853-7260
jrothstein@sidley.com

Mark Kaufmann
312-853-2221
mkaufmann@sidley.com

Karen Owen Dunlop
312-853-2223
kdunlop@sidley.com

Laura J. Cole
312-853-7725
lcole@sidley.com

Los Angeles

Ron C. Ben-Yehuda
213-896-6668
rbenyehu@sidley.com

London

John M. Casanova
020 7360 3739
jcasanova@sidley.com

William R.M. Long
020 7778 1865
wlong@sidley.com

Susan L. Atkinson
020 7778 1869
satkinson@sidley.com

Brussels

Richard L.A. Weiner
32 2504 6450
rweiner@sidley.com

Maurits J.F. Lugard
32 2504 6400
mlugard@sidley.com