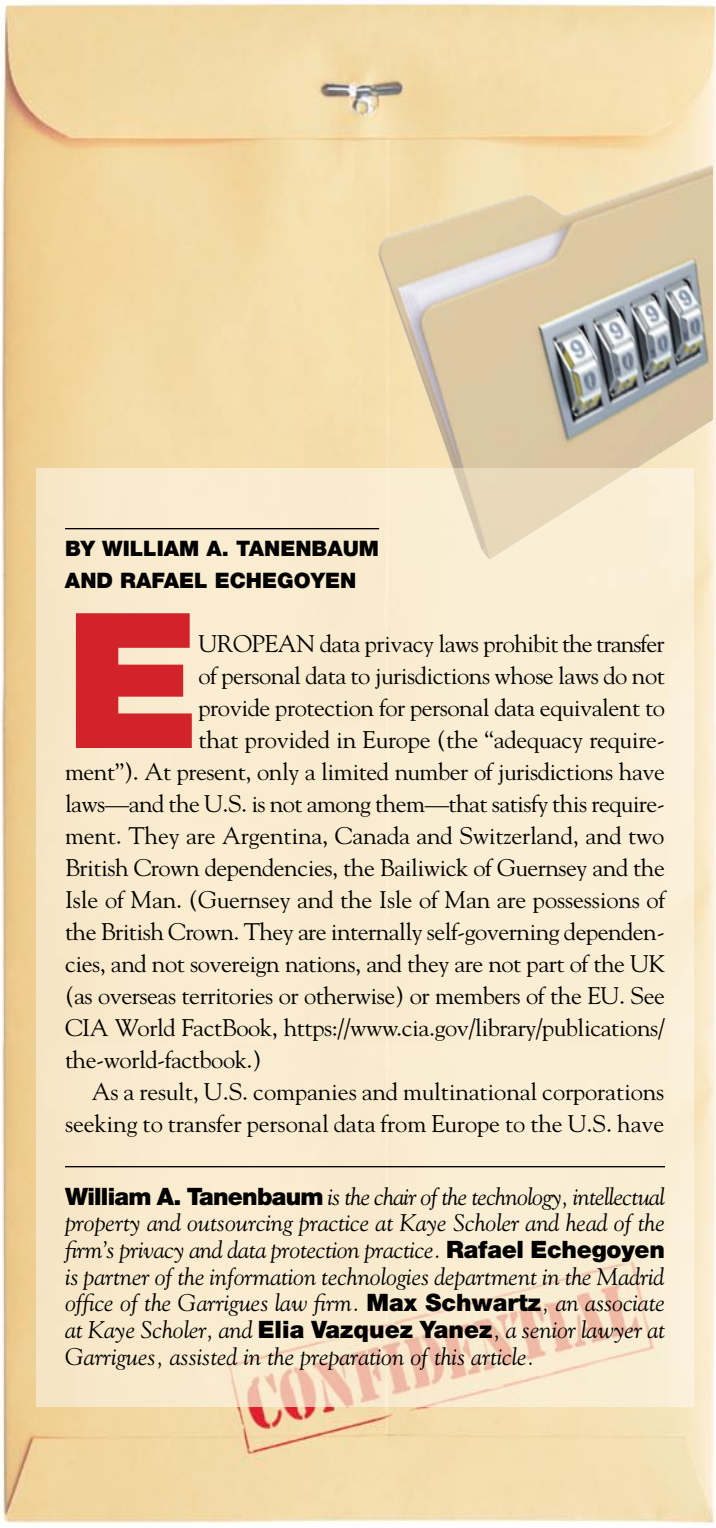
FOR METRO AREA IN-HOUSE COUNSEL

New York Law Journal

ALM

GC New York

Thursday, September 20, 2007



Transferring Personal Data From Europe: Corporations TAKE CHARGE

BY WILLIAM A. TANENBAUM AND RAFAEL ECHEGOYEN

EUROPEAN data privacy laws prohibit the transfer of personal data to jurisdictions whose laws do not provide protection for personal data equivalent to that provided in Europe (the "adequacy requirement"). At present, only a limited number of jurisdictions have laws—and the U.S. is not among them—that satisfy this requirement. They are Argentina, Canada and Switzerland, and two British Crown dependencies, the Bailiwick of Guernsey and the Isle of Man. (Guernsey and the Isle of Man are possessions of the British Crown. They are internally self-governing dependencies, and not sovereign nations, and they are not part of the UK (as overseas territories or otherwise) or members of the EU. See CIA World FactBook, https://www.cia.gov/library/publications/the-world-factbook.)

As a result, U.S. companies and multinational corporations seeking to transfer personal data from Europe to the U.S. have to follow prescribed methods to establish compliance with the adequacy requirement to the satisfaction of the national Data Protection Authorities (DPAs) in the relevant European countries. Achieving compliance is important to U.S.-based multinational companies that use centralized HR and other databases in the U.S. or that use corporate data processing centers in multiple countries to process personal data from Europe.

One of the newest methods of establishing compliance with the adequacy requirement is the use of "Binding Corporate Rules" (BCRs). Broadly stated, with BCRs, a multinational corporate group (referred to as a "Group" under European law) adopts a binding set of corporate rules, has them approved by the DPAs in one or more European countries, as required, and agrees to follow such rules with respect to personal data transferred from Europe and with respect to transfers between companies or business units within the Group outside of the European Economic Area. As discussed further below, an advantage of BCRs is that they allow a multinational company to design its own corporate data protection policies and transfer data from Europe to a U.S. business unit as well as between business units located in different countries, including, significantly, countries outside of Europe and the United States.

BCRs constitute an alternative to the "traditional" methods of complying with the adequacy requirement, which include a "Safe Harbor" certification under U.S. Department of Commerce rules and the use of "Model Clauses," which are contract provisions that have been approved by the European Commission as providing sufficient privacy protection.

William A. Tanenbaum *is the chair of the technology, intellectual property and outsourcing practice at Kaye Scholer and head of the firm's privacy and data protection practice.* **Rafael Echegoyen** *is partner of the information technologies department in the Madrid office of the Garrigues law firm.* **Max Schwartz**, *an associate at Kaye Scholer, and* **Elia Vazquez Yanez**, *a senior lawyer at Garrigues, assisted in the preparation of this article.*

Laws on Privacy

Some background about the European privacy laws is required to put BCRs and the other methods in context. European privacy law is based on European Directive 95/46/EC, entitled "The Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data" and often referred to as the European "Data Protection Directive." The Directive has been implemented through the national laws of the member countries in the European Union, which was recently expanded to include a total of 27 countries, and the national laws of Iceland, Norway and Liechtenstein, which are not EU members. Together these 30 countries are known as the European Economic Area or EEA. For convenience, in this article these countries will be referred to as the "European countries," and the privacy laws of these countries will be referred to as "European law."

To understand the advantages and disadvantages of BCRs, it is necessary to review the advantages and disadvantages of Safe Harbor certification and the Model Clauses. Under the Safe Harbor regime, a company certifies that it will comply with the seven Safe Harbor "principles," which themselves meet the requirements of the European Data Protection Directive. These principles are notice, choice, onward transfer, access, security, data integrity and enforcement.

"Notice" requires organizations to inform individuals about the purpose for which their personal information is to be collected and how that information will be used once collected. "Choice" requires organizations to give individuals the opportunity to "opt out" of having their information disclosed to third parties or used for purposes that the individuals have not previously authorized. "Onward transfer" requires organizations to apply the notice and choice principles before transferring information to third parties, and also requires organizations to ensure that agents who receive information abide by the Safe Harbor principles or an equivalent level of protection.

"Access" requires organizations to permit individuals to review information that organizations have collected about them so that it can be corrected or deleted if inaccurate. "Security" requires organizations to take reasonable measures to protect information from loss, misuse, unauthorized access, disclosure, alteration, and destruction of the information collected. "Data integrity" requires organizations to take reasonable measures to ensure that information is reliable for its intended use and is accurate, complete and current. "Enforcement" requires organizations to provide individuals with a readily available and affordable means of ensuring that the organizations are complying with the Safe Harbor principles.

The U.S. Safe Harbor certification process is a self-certification not a registration process. Re-certification is required annually, and this may entail the cost of yearly privacy audits to verify that certification requirements are met. Certification subjects a company to the jurisdiction of the Federal Trade Commission. There are limitations to the Safe Harbor procedures. Some companies find it difficult to certify because the entire company cannot comply with the Safe Harbor requirements. Only companies subject to the jurisdiction of the FTC or the Department of Transportation are eligible to certify. Financial institutions, for example, are not eligible. Significantly, the Safe Harbor certification only applies to transfers from the EEA to the U.S. It does not apply to transfers from Europe to the business units of a U.S. multinational Group located in other countries whose laws do not satisfy the adequacy requirement.

Accordingly, having a Safe Harbor certification does not in itself enable a multinational corporation to transfer European data to all the countries where it does business. A Safe Harbor-certified company must still adopt other compliance mechanisms to meet the adequacy requirements in order to electronically or otherwise transfer European personal data to databases and corporate operations centers in jurisdictions other than the U.S. (excluding Argentina, Canada, Switzerland, Guernsey and the Isle of Man). Moreover, a Safe Harbor company must still ensure that the collection and processing of data at its European operations meets the requirements of each applicable EEA country's data protection rules, including, for example, laws that require companies to obtain consent to collect information from their own European employees even for employment purposes. (The requirements for employee data collection are discussed at length in a prior column, entitled "Collecting Employee Data in Europe" in the June 21, 2007, issue of GC New York.)

The Model Clauses present another alternative for satisfying the adequacy requirement. The Model Clauses are contract provisions that European data authorities have "pre-approved" for use in data transfer contracts because they adequately protect the rights of European data subjects when their personal information is transferred outside of Europe. There are currently three sets of approved Model Clauses. The set of Model Clauses to be used in a contract depends upon whether the companies to the contracts are deemed to be "data controllers" or "data processors." Such status is imposed by operation of European law. "Data controllers" are companies that determine the reason why and the manner in which personal data is processed. For example, an employer that determines what information will be collected from its employees and how such data will be processed will generally be deemed to be a "data controller." A "data processor," on the other hand, is a company that processes data on behalf of the data controller. "Process" covers a wide range of activities, but does not include determining why personal data is to be collected and how it will be used.

The first set of Model Clauses is contained in form 2001 C2C, which governs "controller-to-controller" transfers of personal data. These are intended for use by companies where each has the status of a controller; "C2C" stands for "controller-to-controller." The second form is 2001 C2P, which is primarily designed to be used where a contracting party located in Europe exports data to another entity that will process the data on the first party's behalf. "C2P" stands for "controller-to-processor." The third form is 2004 C2C, which has been characterized as a more "business friendly" version of form 2001 C2C. It was designed to address the criticisms of the first two sets of Model Clauses.

Many U.S. companies object to all forms of the Model Clauses on several grounds. First, the Model Clauses grant "data subjects" (the individuals to whom the personal data relates) third-party beneficiary rights and a private right of action to enforce the agreement. However, under form 2004 C2C, a data subject can enforce those rights only after the exporter has failed to act to do so for a period of 30 days. Second, the Model Clauses specify that the governing law is the law of the European country from which the data is exported. Third, they require the importer, typically a U.S. company, to submit to jurisdiction in that European country.

Fourth, the first two sets of Model Clauses impose joint and several liability on the parties. Form 2004 C2C does not, but it subjects the importer (generally the U.S. company) to due diligence by the exporter to verify that the importer can perform its obligations under the Model Clauses. Fifth, the Model Clauses give European Data Protection Authorities the right to audit the agreement. The audit provisions are

less onerous in the 2004 form, but an audit right is still imposed on the contracting parties.

In addition, the Model Clauses can prove to be unwieldy. If a large number of business entities are doing business together and exchanging, controlling and processing data in different corporate pairs, then the number of contracts required can quickly multiply into dozens or more. They will also require revisions as the companies or business units of a multinational corporate entity change their data processing—and data control—practices to, among other things, incorporate new technology and outsourcing.

Single Set of Rules

BCRs address many of the limitations of the Model Clauses and the Safe Harbor regime. While the Model Clauses and a Safe Harbor certification provide a way for data to be transferred from Europe to the U.S., BCRs are broader and allow a multinational corporation to transfer personal data among all of its business units on a global basis, even if such business units are located in countries whose laws do not meet the European adequacy requirement.

BCRs allow a corporation or corporate Group to use a single set of rules and, further, allow the corporation to establish its own internal binding rules, provided that they meet European data protection law requirements. This can avoid the multiplicity of contracts that a global business enterprise with many business units would be required to enter into in order to use the Model Clauses. Furthermore, companies in business sectors that are not eligible for Safe Harbor certifications can use BCRs. This makes BCRs particularly advantageous for financial institutions, which are not eligible for Safe Harbor certifications. Moreover, BCRs provide a natural extension of the internal corporate rules that financial institutions establish to comply with various regulatory and exchange requirements in multiple jurisdictions. Overall, BCRs should generally prove less costly and more flexible than Model Clauses and Safe Harbor registrations.

It can be argued that BCRs benefit individual data subjects because BCRs provide a way to increase a corporation's compliance with data protection laws. On the other hand, BCRs potentially increase a company's privacy liability. BCRs must give data subjects the right to enforce their rights. If local law provides greater data protection than the BCRs, the data subject's claim can be based on local law. If, however, the BCRs provide greater protection than the laws in the applicable European country, then the data subject can base his or her claim on the company's rules rather than local law.

An advisory body established under Article 29 of the European Data Protection Directive, consisting of representatives of the Data Protection Authorities in the EEA countries and the EU Commission and known as the "Article 29 Working Party," has issued working documents and model checklists for BCR requirements. Its Working Document 74 (adopted in June 2003) (WP74) requires a Group to establish that its BCRs apply throughout the Group and are binding in practice on the individual Group members (through contracts or unilateral undertakings, for example). It also mandates that BCRs be legally enforceable by data subjects and the relevant Data Protection Authorities and among Group members. This effectively requires corporate business units to police each other's compliance.

WP74 further states that the scope of authorization does not extend to data transfers outside of the Group and that the responsibility for data protection outside of the EEA should be delegated to the Group's headquarters in Europe, or where headquarters are outside of Europe, to a delegate Group company in Europe. Finally, it provides that BCRs must contain a sufficient level of detail to describe the data flows and the purposes for which the personal data will be processed and to allow the relevant DPAs to determine whether the data processing conducted outside of Europe meets the adequacy requirement.

In 2005, the Article 29 Working Party issued a model checklist to assist Groups in complying with WP74. The checklist requires the Group to determine to which country's DPA the BCR application should first be submitted. The checklist criteria provides that this should be the DPA in the country where the Group's parent is incorporated. If the parent is incorporated outside of the EEA, then a number of factors are to be considered, the most important of which is the country where the Group's European headquarters are located.

The checklist also sets out detailed requirements for a BCR application, including that drafts of the binding corporate rules be submitted with the application, that the company have internal audit and compliance programs for the rules and that the Group ensure that the BCRs are legally binding. In addition, the BCRs must provide data subjects with the right to enforce his or her rights in the jurisdiction from which the data transfer occurred as well as the jurisdiction of the Group's European headquarters. The relevant authorities also must be able to audit a Group's compliance with the BCRs.

The major challenge to companies seeking to use BCRs at present is the cumbersome procedure for obtaining DPA approvals. A "Co-Operation Document" was issued at the same time as the checklist, and it set out the principles used to determine which DPAs will authorize and monitor the Group's BCRs. A Group is to determine, based on the Article 29 Working Party's documents, the lead DPA to initially receive and approve the BCRs. However, the DPAs have the right to designate a different lead DPA.

After the lead DPA approves the BCRs, the Co-Operation Document authorizes a relatively long time period for the DPAs of the other applicable countries to grant their approval. The length of time involved may, as a practical matter, make BCRs an attractive method of satisfying the adequacy requirement only for large multinational corporations having sufficient resources to devote to the application process, negotiations with multiple DPAs, and the successive revisions of the BCR documents likely to be required during the approval process. In December 2005, GE became the first U.S.-based company to obtain approval from the UK DPA to transfer employee data outside of the EEA pursuant to binding corporate rules.

Conclusion

BCRs deserve serious consideration because they provide a way for the U.S.-based multinationals to use a single set of internal rules to comply with European privacy laws and make use of intranet sites, databases and other electronic business tools that complicate the application of European laws to global business operations.