THE INTERNATIONAL CHAMBER OF COMMERCE PROPOSES AN ALTERNATIVE FOR LEGITIMIZING INTERNATIONAL TRANSFERS OF PERSONAL DATA FROM THE EUROPEAN UNION

The ICC Report analyzes the use of binding corporate codes to facilitate the transfer of personal data from the EU and other jurisdictions with similar privacy laws to jurisdictions not deemed to offer an adequate level of protection.

There is an increasing awareness of the impact that European Union ("EU") transborder data flow limitations may have on transnational mergers and acquisitions, and the Article 29 Data Protection Working Party[1] has made a commitment to seek substantially greater resources for enforcement of the laws limiting transborder data flows from the EU. Companies with transborder operations need to assess their data transfer policies carefully in light of the increased emphasis on this issue. Alternatives to the complex and sometimes cumbersome methods for dealing with this problem are well worth considering.

The International Chamber of Commerce ("ICC") recently published a report (the "ICC Report") providing guidance on drafting and implementing company policies to facilitate international transfers of personal data between corporate affiliates that are located in countries with laws restricting transborder data flows and those located outside of these countries. Binding corporate rules are sets of rules adopted by a company or corporate group that provide protections for data processing within that company or group. Binding corporate rules can provide a mechanism to facilitate international transfers of data in jurisdictions where privacy legislation imposes restrictions on such transfers. Below, we compare the alternatives available for transferring data under these circumstances.

Background: In 1995, the EU adopted expansive privacy legislation[2] imposing restrictions on businesses that wish to collect, process or transfer "personal data"[3] from an EU Member State

---

1 The Article 29 Data Protection Working Party was established by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is an independent body comprised of data protection regulators from each EU Member State and is intended to advise the European Commission on data protection matters, promote uniformity among the EU Member States and make recommendations to the public concerning data protection issues.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Personal data is defined extremely broadly by the EU Privacy Directive as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity." Article 2(a) of Directive 95/46/EC.

(the "EU Privacy Directive"). The EU Privacy Directive includes restrictions prohibiting the transfer of personal data to other (*i.e.*, non-EU) countries, unless the country "ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data."[4] The EU does not currently view the United States as providing an adequate level of protection. EU Member State laws implementing the EU Privacy Directive have imposed strict restrictions on the transfer of personal data from the Member States to the United States (whether the personal data is transferred to the United States from third parties or the organization's foreign divisions). As noted in the ICC Report, other countries also have enacted privacy legislation based on the EU Privacy Directive or have similar legislation pending.

Many companies that are based in the United States and operate offices or branches abroad collect and process a variety of information, in the EU and elsewhere, that these jurisdictions would regard as personal. U.S. companies routinely transmit this information to the United States. Examples of these data include human resources data, customer information and information on prospective customers. In order to lawfully transfer personal data about a data subject out of Europe (or other jurisdictions with similar privacy laws) to the United States, a company must take steps to ensure that the collection and transfer are lawful. If a company does not adopt one or more of the mechanisms described below to legitimize the transfer, it is possible for a data protection authority to bring enforcement proceedings and impose sanctions, including interrupting the flow of data.

Pursuant to the EU Privacy Directive, transfer of personal data is permitted if the company has obtained the "unambiguous consent" of the data subject to the transfer. (Consent to the transfer is separate from consent to the initial collection and subsequent processing of the data, whether or not the data are transferred abroad.) In the context of consent to transfer, what constitutes unambiguous consent differs among EU jurisdictions. For example, data protection authorities in an increasing number of EU jurisdictions have found that the "unequal relationship" between an employer and its employees precludes an employee from providing his or her consent to an international transfer of many types of data. Also, it may be impractical in many cases to obtain the consent of the data subject prior to the transfer of his or her data. Thus, this method of legitimizing international transfers of personal data, such as from the EU to the United States, is feasible only if it is possible to obtain prior consent from the data subjects. Even if it is practical to obtain consent, such consent may be ineffective in some EU jurisdictions if human resources data are involved.

Companies also may enter into a "transborder data flow agreement" incorporating model contractual clauses adopted by the European Commission in 2001. The model contractual clauses ensure that the data will be treated in accordance with the data privacy rules of the jurisdiction in which the data are collected and grant data subjects the right to enforce the agreement in that jurisdiction. One benefit of this approach is that the local data protection

---

[4] To date, only Argentina, Canada, Guernsey, the Isle of Man, and Switzerland have been found to possess adequate privacy protection by the EU.

authority either will not review the agreement at all or will only engage in a cursory review. A drawback is that the requirements of each EU Member State may differ, and separate agreements could be required for each jurisdiction. If many entities are involved, entering into multiple agreements can be impractical. Companies may enter into transborder data flow agreements that diverge from the EU model clauses but these agreements must generally be affirmatively approved by the data protection authority in the EU Member State.

The European Commission recently approved new model clauses for transferring personal data from the EU to other countries. The new clauses do not replace the clauses adopted by the Commission in 2001; rather they are intended to offer companies seeking to transfer data abroad another option. The new clauses were drafted with input from the international business community and are intended to be more commercially friendly; for example, the new clauses do not require the data exporter and the data importer to be liable for each other's misuse of data, as the 2001 clauses do, and the new clauses contain more flexible auditing provisions. However, the new clauses do not go into effect until April 1, 2005; therefore, it will be some time before it is known how widely accepted and effective the new model clauses are.

Under some circumstances, personal data may be transferred to a third country that does not provide adequate data protection if the transfer is necessary to the performance of a contract. This exception to the prohibition on transfer has not been implemented consistently by the EU Member States. While some jurisdictions permit a somewhat broader reading of this provision, others have limited it to very narrow circumstances. This means of legitimizing a transfer may not be helpful in most cases.

The EU has agreed that personal data may be transferred from the EU to U.S. companies that certify to the U.S. Department of Commerce's Safe Harbor Privacy Principles. Certification to the Safe Harbor requires companies to certify that they provide adequate data protection as defined by the EU Privacy Directive. Once certified, companies are subject to the jurisdiction of the appropriate U.S. government agency (the Federal Trade Commission or other government agency having jurisdiction over the subject matter of the business) if they fall short of their certifications. Response by U.S. companies to the creation of the Safe Harbor has not been overwhelming, with less than 650 companies joining since its creation in 2000. However, the Safe Harbor offers a relatively simple approach to legitimizing EU data transfers for U.S. companies. It should be noted, however, that the Safe Harbor does not address the lawfulness of the collection itself, which remains subject to the local requirements, such as the need for consent and a filing with the data protection authority, of the jurisdiction in which the data are collected.

In 2003, the Article 29 Data Protection Working Party adopted a Working Document that discusses the use of binding corporate rules for international data transfers. The Working Document provides guidance on crafting such rules and concludes that some multinational companies could benefit from codes of conduct for international transfers. However, the Working Party also notes that binding corporate rules should not be considered the only or best mechanism for legitimizing international transfers, but rather could be used when some other mechanism (such as the Safe Harbor or the model contractual clauses) is not practical. In

November 2004, the Article 29 Data Protection Working Party held an initial hearing on binding corporate rules and expressed its willingness to work on developing a cooperation procedure for obtaining approval of binding corporate codes in multiple EU jurisdictions.

The ICC Report: The ICC Report describes the benefits and limitations of using binding corporate rules as an alternative to the approaches described above. The ICC Report observes that binding corporate rules may make compliance with transfer restrictions, in the EU and elsewhere, less time consuming and costly, and provide multinational corporations greater flexibility. In addition, binding corporate rules represent a proactive approach to privacy that could create and sustain a company culture that respects data privacy. On the other hand, binding corporate rules only apply to intra-company transfers, and do not apply to transfers to entities outside of the corporate group. Binding corporate rules would also need to be approved individually by most EU Member States from which the company seeks to transfer personal data. There is currently no streamlined mechanism to obtain approval from the data protection authorities. Because each EU Member State has implemented the EU Privacy Directive somewhat differently, obtaining approval would be time consuming and could result in 25 different versions of a company's corporate code. As discussed above, the Article 29 Data Protection Working Party has expressed its willingness to address this problem in 2005.

The ICC Report acknowledges that there is some uncertainty about the binding nature of binding corporate rules. Corporate rules addressing privacy issues must be made binding both within the organization and externally through the use of mechanisms such as intra-company agreements or, where permitted, unilateral undertakings such as Deed Polls or Declarations of Trust. The Article 29 Working Party has stated that data subjects covered by binding corporate rules must become third party beneficiaries with rights at least equivalent to those granted by the EU's model contractual clauses. Also, the Article 29 Working Party has stated that binding corporate rules must permit data subjects to bring claims against the company in the EU Member State from which the transfer originates or the European headquarters of the company.

Conclusion: As described in the ICC Report, binding corporate rules offer a potentially viable alternative to other mechanisms to ensure uninterrupted data transfers among the offices of a multinational company. However, we believe that until there is more uniformity among EU Member States, it will remain a challenge to utilize corporate rules to address privacy requirements in the EU. Also, other approaches, such as entering into a transborder data flow agreement based on either of the EU's model contractual clauses or certifying to the Safe Harbor may offer more certainty. Also, binding corporate codes do not address transfers from or to companies outside the corporate structure, such as in the case of a corporate restructuring. Multinational companies seeking to ensure that the transfer of personal data between the EU and other jurisdictions is permitted must generally employ a combination of the approaches described above to satisfy differing EU Member State rules. While a binding corporate code may be a useful addition to such approaches, it is not likely to replace other methods of legitimizing data transfers.

* * * * * * * * * * * * * * *

If you have any questions concerning the issues raised in this memorandum or need any further information, please contact Stephen Bell (202-303-1102, sbell@willkie.com), Jennifer McCarthy (202-303-1145, jmccarthy@willkie.com), Sophie Keefer (202-303-1142, skeefer@willkie.com), Jennifer Ashworth Dinh (202-303-1161, jdinh@willkie.com) or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

January 20, 2005