



**Robert Rothman**

President  
Privacy Associates International LLC

### Standard Clause Contracts and Safe Harbor

Many global companies are still considering their options for the transfer of personal information and sensitive personal information out of countries with cross-border restrictions. This is becoming a critical issue as companies consolidate data centers and processes to better manage themselves and service their clients and customers. Bob Rothman recounts some of the options that are in use today that might help you expedite your decision and implementation processes.

**Nymity: What is the first step a global company must take before it can begin to implement an intra-company data transfer program?**

**Rothman:** There are really two steps that are closely related and have to be taken at the same time. The first is to understand what personal data the company must transfer from which countries to which countries and the purpose for each of the transfers. The second is to determine the available legal bases that can be used to cover each transfer as it is revealed. While determining the exact flow of every piece of personal data is ideal, it is often surprisingly difficult in large multinational companies. Sometimes the most practical approach is to determine the major data flows and then choose legal transfer bases that are broad enough to cover those transfers and other likely avenues as well. For instance, if an investigation reveals there are numerous transfers of HR information from European Economic Area (EEA) countries to the US, one might conclude Safe Harbor is a good basis to cover those transfers without having to document each individual HR data flow to the US from each of the EEA countries. Companies typically use a variety of legal bases, including available contractual schemes, to transfer different types of personal information out of countries with cross-border restrictions.

**Nymity: Once these matters are determined, what must one understand about filings (registrations and permits) with the various Data Protection Authorities?**

**Rothman:** Depending on which legal transfer bases have been chosen and which countries are involved, filings with DPAs may have to be made or modified to reflect the new transfers. In some cases no filing is required, in others an informational filing is required and in still others prior approval of the legal basis is required. It is important to check the laws and regulations of the individual countries involved because even within the EEA requirements vary greatly and are sometimes surprising. For instance, even if you are using one of the EU-drafted Standard Contractual Clause agreements as your transfer basis, a number of countries still require approval of the DPA before those transfers may take place (largely to determine the required appendices have been completed with a sufficient level of specificity).

**Nymity: Also, is it necessary to review the existing Privacy Notices provided to each data subject? Why would this be important at this juncture?**

**Rothman:** Absolutely. The current Privacy Notices may not have contemplated such transfers and may no longer be accurate. In such a case, an updated notice may be necessary.

Regardless of the legal basis on which a cross-border transfer is made, domestic law will normally require appropriate notice of the transfer and its purpose to the data subjects. The data subject may then have specific rights to object. For instance, if a transfer is made pursuant to a Safe Harbor certification, the data subject may not have a right to object to the initial transfer to the US, but may have a right to object to the subsequent onward transfer of the data from the US to Japan, even though a Safe Harbor-qualifying onward transfer agreement has been put in place.

Finally, it is extremely important to note that there are often labor considerations applicable to the transfer of employee data out of most European countries that must be addressed prior to any unilateral notice being issued. Typically, consultation with the appropriate Works Council is required, necessitating close coordination between the privacy function and European in-country management. The process can sometimes be a source of some frustration to both the privacy professional seeking to quickly implement the data transfers and the European management responsible for horse-trading with labor representatives on a broad agenda of disparate matters. Wine often helps.

**Nymity: Given this base set of facts, considering only the intra-company contracts, what must be known about the legal structure of the company in each jurisdiction in order to know what legal entities in that country must sign a contract?**

**Rothman:** If a company chooses a contractual solution to the problem of finding a legal basis to the cross-border transfer, the key is to make certain there is an appropriate contract in place between each data exporter and each data importer. To do that, it is necessary to understand all the legal entities involved. To the extent a company can then use one or more multi-party agreements, as opposed to a series of bilateral agreements, that often helps simplify the situation. However, the multiparty approach is not always acceptable.

**Nymity: Which countries require or provide standard contracts addressing the transfer of personal and sensitive personal information for controller to controller flows? For controller to processor flows?**

**Rothman:** With respect to controller to controller transfers, countries normally don't require the use of contracts to make cross-border transfers of personal data, but provide that appropriate contracts constitute one allowable alternative legal basis to legitimize such transfers. The best known of these agreements are, of course, the EU and Standard Clause Contracts. However, other countries (e.g. Australia, New Zealand, Japan, and Argentina) also have contractual solutions that are more flexible than the European approach in that only privacy protection results are specified, words are not dictated. In the US, the onward transfer to most third parties of personal data received from Europe under a Safe Harbor certification requires a contract that qualifies as a Safe Harbor onward transfer agreement.

The situation with controller to processor transfers is different. Even controllers located in Europe have to have contracts in place that qualify as "Article 17 Agreements" before transferring personal data to processors also located in Europe. To transfer to a processor outside of Europe a Standard Clause Contract (Controller to Processor) is normally required. Other countries also require, or in some cases just recommend, contracts with processors that include very specific provisions. Such countries include Australia, Canada, Japan, New Zealand, etc. In the US contracts are sometimes specifically mandated by black letter law (Business Associate Agreements under HIPAA, processors under GLB Safeguards Rule), but should also generally be considered required with respect to consumer data under current Section 5 interpretations by the FTC.

**Nymity: Typically what treatment strategies of personal or sensitive personal information can be grouped together and described to a Data Protection Authority in the Annexes or Appendices of EU Model contracts? What are the key questions asked? Are they similar from jurisdiction to jurisdiction?**

**Rothman:** The allowable description of the purpose of the transfer and categories of data may well vary depending on the country involved. Based on current information, standard clause contracts have to be approved in seven countries (Austria, Czech Republic, Luxembourg, Netherlands, Poland, Romania, and Spain) and have to be filed in another nine (Belgium, Cyprus, Denmark, Finland, France, Greece, Malta, Portugal and Slovakia).

Usually the company will seek to have as broad a description as possible to cover the maximum scope of transfers in a specific area (e.g. "employee information") while at least certain of the DPAs seek as much specificity as they believe is reasonable considering the named purposes of the transfer (e.g. "employee name, work position, social identification number, grade, years employed, etc.").

**Nymity: Which countries have export laws that would prevent the onward transfer of certain types of personal or sensitive personal information? Do such export laws apply to access by a non-foreign national as well regardless of their location? Do such export laws prevent such personal or sensitive personal information being carried out of a jurisdiction on a pc, memory stick, paper document or other medium?**

**Rothman:** In addition to the 27 countries of the EU and the additional 3 countries of the EEA, cross-border transfers of personal information are regulated in Switzerland, Russia, Australia, Japan, New Zealand, Argentina, Uruguay, South Africa and Israel. Additions to this list are made regularly. The restriction on transferring personal information (as defined in the individual national law) is on persons located within the particular jurisdiction. It does not matter whether the transfer is to a national of the jurisdiction residing abroad or to a foreigner; the violation is based on the transfer across the border. Allowing a person outside the jurisdiction to access personal information on a computer located within the jurisdiction is considered a transfer. Transfers made by electronic means, on some electronic media or hard copy are generally treated the same.

**Nymity: What are the basic contract strategies? One contract with exporters and importers? One controller and one data processor contract? Multiple signors on one or two contracts? A set of contracts by region (EU/Asia/Canada/Argentina)? How are the laws of the sending country acknowledged? What about the various Privacy Notices?**

**Rothman:** Most companies seek to minimize the number of contracts that have to be put in place, particularly when the contracts are between or among affiliates. Assume the existence of a medium sized multinational with just one subsidiary in each of the 30 EEA countries and 150 subsidiaries outside the EEA. If that company wants to be able to freely transfer employee information from any of its EEA companies to any other company elsewhere in the world, it will require putting in place a network of close to 4,500 bilateral contracts (companies in countries with EU adequacy determinations would not require contracts). That is because each of the 30 EEA located companies would have to have a Standard Clause Contract (Controller to Controller) with each of the 150 other non-EEA located companies. Additionally, the entity or entities in Argentina might require a contract with each of the 149 other non-EEA companies for an additional 180 non-EU-style agreements that meet Argentine requirements. The same would be true for Japan, perhaps Australia, etc., etc.

As I mentioned before, one strategy is to address this is the use of multilateral contracts, where permitted. Other approaches are the utilization of web based contracts with electronic signatures, where allowed. The inevitable required contract changes are often

handled by companies within a single group by granting powers of attorney to a specific individual or set of individuals within the group to agree on future contractual changes.

The controller to processor situation is more complicated. This is the case in part because of the greater number of entities normally involved, but also because of the different relationship among the parties. A controller to controller situation often involves contracts between or among companies that are members of a single group. Thus, while not minimizing the difficulties involved in concluding agreements, at some point there is an individual who can control both sides of the contracts. The controller to processor situation more often involves a true arms length relationship and therefore orchestrating contract architecture is much more difficult. Finally, there are simply more rules involved in the controller to processor situation than the controller to controller situation.

**Nymity: How are the data protection requirement(s) detailed in the Annex of the controller to controller ICC EU Standard Clause Agreement? In the annex of the new controller to processor EU Standard Clause Agreement? ? In which jurisdiction do you find the most rigorous security and data protection standards?**

**Rothman:** Let me start by saying that there are actually three current versions of EU Standard Contractual Clauses: controller to controller "classic", controller to controller "ICC" and the new controller to processor agreement that has replaced the 2001 version. Both of the controller to controller agreements place responsibility on the foreign data importer to establish and maintain technical, physical and administrative security measures to protect the personal data involved. The measures don't have to be the best possible, but must be appropriate to the risks involved. Thus, there is some cost-benefit analysis involved. The controller to processor agreement is even stricter and places security liability on both the data importer and the data exporter. The specific technical and organizational security measures that are to be taken by the data importer have to be detailed in an appendix to the document. With respect to jurisdictions, Spain has very specific security regulations to worry about and although I have not seen any statistics, anecdotally Spain, Italy, Austria and Poland are known to have particularly vigorous enforcement of privacy rules generally.

While none of this is really new to privacy professionals working in the field, what is new is the interplay between the Standard Contractual Clause agreements and the new American-style breach notification laws being adopted in Europe. Each of the standard contract forms specifically address unauthorized access as one of the security risks that must be guarded against. However, now that at least certain unauthorized accesses have to be notified by EU data controllers to data subjects, I believe we will see significantly more pressure being placed on these provisions, particularly in the controller to processor context. It will be essential for the foreign data processors to put systems in place that will be able to detect when there has been an unauthorized access to personal information – either from the outside or from inside the company itself. It will also be essential for EU data controllers to make certain the data processors actually put these systems in place so the controllers will be able to fulfill their own legal obligations both under the standard processor contract and under the breach notification laws.

**Nymity: What do you recommend regarding training and education regarding global accountability for these adhering to the terms of these contracts?**

**Rothman:** Good point. It doesn't matter how brilliantly the solutions to cross-border transfer restrictions, contractual or otherwise, are constructed, if they are not followed they are useless to both the company and the data subjects. Since personal information is used so broadly within organizations training must be equally broad. To be effective, privacy training must be couched in terms the employee easily understands and must be seen to be relevant to his job. It can't consist of a recitation of complicated, high level, legal concepts that the individual must decipher and try to apply to his day to day work. That may well mean using terminology the organization normally uses, having different versions of training based on the function of the employee (HR, Marketing, etc), and making local language training available. What doesn't work is expecting people to act in compliance with a privacy contract, certification or internal policy if you don't tell those people of its existence and exactly what is expected of them.

**Nymity: In closing, what have we not asked, that would be meaningful for our readers to know about?**

**Rothman:** The subject of cross-border transfers of personal information is one of the most difficult areas for an internal privacy professional to deal with. The rules are in large measure based on old technology from the 1980s and difficult to apply in today's world. Company executives rarely see any real privacy benefit in expending resources to put thousands of formal contracts in place among entities they believe they already control or to make legal promises to governments in exchange for the right to know who they are employing in their own overseas subsidiaries. Enforcement of the rules themselves by DPAs has been spotty at best due to resource constraints within the government, cultural norms, or other reasons, making it that much harder for the internal privacy professional to convince Management to expend money and effort on compliance. Still, being seen as a company with a cavalier attitude toward personal data could have severely adverse business consequences in many markets. Additionally, most of these laws have criminal penalties for extreme violations and putting local employees at risk for this is not something most executives are comfortable doing.

For companies that have not yet taken any steps to comply with the cross-border transfer rules, I strongly suggest that they take whatever measures they can in that direction as soon as possible. Even if a 100% solution can't happen immediately, having started down that road will be of immense assistance should the company be called upon to demonstrate compliance.