Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 4 April 2013

Personal Data Transfers from the European Economic Area: Time to Consider Binding Corporate Rules 2.0

By Rafi Azim-Khan and Steven Farmer, of Pillsbury Winthrop Shaw Pittman LLP, London.

What exactly is the "best" solution for an international business needing to handle and transfer personal data across borders?

This has become an increasingly important and common question as business becomes more global and companies grow, reorganise or merge.

There has been a lot of discussion, not least in the context of the European Commission's proposal for the new EU regulation to replace the EU Data Protection Directive and the EU Article 29 Data Protection Working Party's push towards "privacy by design", about the best way for companies to adequately safeguard personal data which is transferred out of the European Economic Area, thereby ensuring that their transfers are compliant with EU data protection laws relating to extra-EEA transfers.

Many commentators, including some of the key EU regulators, have noted that there remains a lot of confusion, and a fair amount of misinformation, surrounding the pros and cons of the various routes used to ensure that extra-EEA transfers are compliant. It is certainly true in the authors' experience that even quite sophisticated companies and knowledgeable data protection officers can many times have an out of date view, and better solutions are indeed available.

This article looks at some of the common misconceptions and takes a fresh look at the key routes to ensuring compliance. As will be seen, for various reasons, Binding Corporate Rules 2.0, as we might call them, are worthy of fresh consideration, even where they may have been overlooked or discounted as a way to ensure compliance only very recently.

What Does EU Law Say about Extra-EEA Transfers?

By way of recap, the law in the European Union is such that personal data can be transferred to a country or territory outside the European Economic Area only if that country or territory ensures an adequate level of protection for the rights of individuals in relation to the processing. The European Commission has, of course, drawn up a list of countries or territories which are deemed "adequate" for this purpose, this narrow list containing the likes of Argentina, Switzerland, Israel and, more recently, New Zealand. Conspicuous by their absence from this list, however, are a number of large countries where multinationals typically operate or are headquartered, such as the United States. If a company wishes to transfer personal data outside the European Economic Area and an importer is not on

the European Commission's "adequate list" (being based in, say, the United States), then such an exporter has to rely on another "route" to ensure its transfers are compliant with, and not in breach of, EU law.

In terms of the alternative routes available, at least in theory, an exporting entity could form its own view that a third country/importing entity ensures an adequate level of protection. However, the general consensus is that this practice comes with a serious health warning, to the extent that this should be relied on only in the most clear-cut cases. There is absolutely no guarantee that an EU regulator's view would align with the exporting entity's, meaning that entity could find itself in considerable hot water, namely, on the end of an enforcement notice preventing the transfer (which could cause a great deal of inconvenience to even the smallest of businesses with international operations) and/or a fine.

On the issue of fines, one noteworthy development is, of course, that the powers for EU regulators to fine those found to be non-compliant have significantly increased recently. By way of example, the UK Information Commissioner has been empowered to issue on the spot fines of up to £500,000 (U.S.$761,886) for more serious breaches since April 2010, and discussions in the European Union suggest that even larger fines, of up to 2 percent of global turnover (revenue), may well be with us soon.

Another option for an exporter is to try to rely on one of the exceptions which permit a transfer, such as by obtaining the consent of the individual concerned to the transfer. It is fair to say, however, that this is most certainly not as simple as it sounds. In practice, it can be very difficult to get this right, not least because many regulators interpret this very narrowly indeed (the Dutch view, for example, being that there is a presumption that consent can almost never be freely given by an employee to an employer, given the bargaining position of the parties).

So what about the remaining options available to ensure that personal data transfers from the European Economic Area are compliant?

EU-U.S. Safe Harbor Program

Let's look at the EU-U.S. Safe Harbor Program, which for a number of years has been viewed by some as one of the better ways to comply. However, recent developments, and some serious downsides that are often overlooked, should be considered in the mix before choosing this as one's "solution".

Whilst this scheme has relative simplicity as one attraction, and is unlikely to disappear anytime soon, support for the scheme does appear to be waning in some EU quarters, particularly because it is viewed as inadequately dealing with the issue of onward transfers once personal data arrives in the United States.

In addition, it addresses only transfers from the European Economic Area to the United States, and so is of limited help for global companies.

A further important aspect, and one that is often overlooked, is that, by signing up to the scheme, one exposes oneself to liability and enforcement action in the United States.

Of note is the fact that the U.S. Department of Commerce and the U.S. Federal Trade Commission have responded to recent criticism by saying they will be increasing scrutiny and enforcement.

Model Contract Clauses

On this basis then, and taking a more long term view, it could well be argued that exporters should instead look to put in place adequate safeguards in the form of either 1) Model Contract Clauses or 2) Binding Corporate Rules with respect to their transfers. These routes arguably are becoming the options of choice to achieve compliance, even where transfers from the European Economic Area are solely to the United States.

Model Contract Clauses provide one possible solution by giving an EEA data exporter the ability to contract with a non-EEA importer/recipient of the data in a manner that safeguards the treatment and handling of the data to EU-approved standards. The "adequacy" is ensured, provided certain approved clauses are used and adhered to.

However, this route is also not without some material potential downsides. It can often be the case that the clauses are not properly used or are altered/amended, which risks removing the very protection their use is supposed to give.

Further, it can be quite common for a company to lose track of what it covered in various contracts, and uses can often change with time. If the contracts are not kept up to date, or if data is processed in ways beyond the original scope, or if there is some other departure from what was set out, then the company may well be operating under a false sense of security and in a way that unwittingly exposes it to liability. This risk increases the larger the business and the more contracts are used. Many times clients are "drowning" under the obligation of trying to keep tabs on hundreds of contracts and rapidly changing demands from the business as to new data use.

Binding Corporate Rules

An alternative to Model Contract Clauses, Binding Corporate Rules (BCRs) are, of course, nothing new, being internal codes of conduct which entities within a multinational group can "sign up to", demonstrating that their data privacy and security practices meet EU standards.

Developed by the EU Article 29 Data Protection Working Party, they provide a mechanism for transferring personal data throughout an organisation by creating obligations for the group which implements them and rights for individuals. These rights can be exercised before the courts or data protection authorities, the rules being legally binding on the companies within the group, usually by way of unilateral declarations or intra-group agreements.

   ISSN 1473-3579

Although BCRs are referred to as "rules", an organisation does not in fact have to have one set of rules in place; rather, a suite of policies on the issue of privacy will typically make up the BCRs.

When BCRs first arrived on the scene a few years back, a major drawback associated with their use was the fact that they needed to be approved by every EU data protection authority in whose jurisdiction a member of the group would rely on them. So, for example, if a multinational had operations in five EU countries and its EU headquarters were in the United Kingdom, the BCR application would be first submitted to the UK Information Commissioner's Office, which would then liaise with the various other relevant EU regulators in considering whether the application was "approved". As the requirements and practices of different EU member state regulators varied, this caused a fair amount of applicant hair-pulling and, more often than not, meant that the approval process was a long one. This meant that BCRs were, for many, viewed as an attractive solution made unattractive, given this additional "work" and length of time required.

In addition, up until very recently, a further key drawback was the fact that BCRs were not available as a means for data processors to transfer personal data outside the European Economic Area, being available only to data controllers. This further reduced the frequency with which BCRs were taken up, being "unavailable" for those providing outsourced services outside the European Economic Area, such as cloud computing services, to customers within the European Economic Area, for example.

BCRs 2.0

However, this historic view of the pros and cons of BCRs is now out of date, and, for many international businesses, BCRs may well represent their best solution. Many of the key drawbacks traditionally associated with BCRs have fallen away since the introduction of the mutual recognition policy.

The BCR application process has become markedly more streamlined, as one lead data protection authority within the European Union can now assess the adequacy of a group's BCRs, without having to approach each individual country's authority separately and then having to wait for a response from each (providing that the authority is in a territory which follows the mutual recognition policy).

If that lead authority is satisfied that the BCRs put in place adequate safeguards, it can "approve" them on behalf of the other authorities. This, combined with the fact that some authorities have at the same time increased their resources in terms of those reviewing applications, has materially reduced the time taken for an application to be approved.

In addition, since January 1, 2013, BCRs are now also available for exporting data processors.

These various factors have resulted in increasing interest in BCRs.

Given these developments and the fact that, once BCRs are up and running, they generally provide better flexibility than Model Contract Clauses (one does not have to constantly update what can be significant numbers of contracts), this new breed of BCR makes for a more attractive option than before (and for data controllers and data processors alike).

Comment

Whilst BCRs have been an option for data controllers to ensure compliant transfers from the European Economic Area for some time, recent improvements in terms of process, as well as the current emphasis on privacy by design, have meant that BCRs are worth renewed and serious consideration. Companies that looked at compliance options even quite recently may well hold an outdated view of the solutions and benefits that they can offer.

Whilst Model Contract Clauses undoubtedly have a place for certain scenarios and businesses, those that choose BCRs to ensure compliance could significantly reduce the managerial time and cost spent negotiating and documenting the data protection safeguards for each and every data processing activity carried out, whilst also doing away with the supervision associated with managing many such contracts.

The EU-U.S. Safe Harbor Program, as mentioned above, also has a number of drawbacks and limitations in comparison with the new BCRs, not least its limitation to transfers from the European Economic Area to the United States. BCRs can cover transfers wherever around the globe the corporate group may be.

Concerns over cost or initial investment of time for BCRs are also often misplaced or inaccurate. Whilst, of course, there is some initial effort, it should not be forgotten that, both in the European Union and the United States, privacy by design is the new mantra. International companies are being told in no uncertain terms that regulators will expect them to adopt regular reviews of policies, practices, training and so on (updating and enforcing new standards where necessary) and to be able to demonstrate the same if audited. Failure to do this will increase the chances of being fined or facing other enforcement action.

Many companies are now also seeing the value of getting this right from a public relations standpoint, as well as from a good corporate governance standpoint. Given that this is something that needs to be done in any event, it can make a lot of sense to consider updating one's policies and practices as part of a BCR application at the same time.

If you have international operations, it certainly seems the time is right to look at BCRs with fresh eyes.

Rafi Azim-Khan is a Partner and Head of IP/IT & Data Privacy, Europe, and Steven Farmer is a Senior Associate, in the London office of Pillsbury Winthrop Shaw Pittman LLP. They may be contacted at rafi@pillsburylaw.com and steven.farmer@pillsburylaw.com.