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 complex question as businesses become 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experience that even quite sophisticated companies and knowledgeable data protection officers can sometimes have out of date views, and better solutions are indeed available.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 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, 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 list of countries or territories which are deemed “adequate” for this purpose, that company must take steps to ensure that its 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 extra-EEA transfers. There is, for example, the so-called “privacy by design” approach, which seeks to ensure that individuals’ personal data is protected from the outset of the data processing activities, and the adoption of Binding Corporate Rules, which seeks to ensure that companies’ data protection policies are properly implemented and that companies’ data protection policies are properly implemented and that companies’ employees are trained in data protection issues.

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, 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 list of countries or territories which are deemed “adequate” for this purpose, that company must take steps to ensure that its transfers are compliant with EU data protection laws relating to extra-EEA transfers.
In terms of the alternatives available, at least in theory, one approach might be to create an entity in a third country, ensuring that entity remains an adequate level of protection. However, the general consensus is that this would be far too costly and time-consuming, particularly because that entity would need to be regulated in the same way as if it were located in the European Union. This in turn raises the question of whether an entity located in a third country, if not subject to EU regulatory intervention, could be relied upon to ensure the adequate protection of personal data. This is particularly relevant to the question of onward transfers once personal data arrives in the United States.

The E.U. V.S. U.S.

The last thing anyone would want is the risk that personal data transfers from the European Economic Area are non-compliant with the E.U. law. So what about the remaining options available to ensure that personal data transfers from the European Economic Area are compliant? Here, the reality is that the BCRs and the EU Approved Standards are nothing new. There are a number of other ways that entities within a multinational group can “sign up to,” demonstrating that their data privacy and security practices meet EU standards. The BCRs provide one possible solution by allowing an EEA data exporter the ability to contract with a non-EEA importer/recipient of the data in a manner 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 comply with, and not in breach of, EU law. 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 on course towards and enforcement.

The 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 seen to be one of the better options available. However, recent developments, and some recent decisions that are making the Safe Harbor Program less attractive, add to the long list of issues which have led to the Safe Harbor Program facing increasing scrutiny and enforcement.

The Safe Harbor Program is a mechanism for transferring personal data from the European Economic Area to the United States. This mechanism is governed by Model Contract Clauses and is in place to ensure that personal data transfers from the European Economic Area to the United States are solely to the United States.

The Safe Harbor Program is a voluntary program, and the companies that participate in the program are required to comply with the principles of data protection and privacy as set out in the EU data protection laws. The program is operated by the U.S. Department of Commerce and the Federal Trade Commission.

The Safe Harbor Program is based on the concept of self-regulation, where companies voluntarily agree to comply with the principles of data protection and privacy as set out in the EU data protection laws. The program is designed to ensure that personal data transferred from the European Economic Area to the United States is protected in a manner that is equivalent to the protection provided under the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program requires companies to provide a mechanism for individuals to exercise their rights under EU data protection laws, including the right to access, rectify, and erase their personal data, and the right to object to the processing of their personal data.

The program also requires companies to provide a mechanism for individuals to lodge complaints with the U.S. Department of Commerce and the Federal Trade Commission, and to provide a mechanism for the European Union to send a request for the transfer of personal data to cease.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is a voluntary program, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is voluntary, and companies are not required to participate in the program. However, companies that participate in the program are required to provide a privacy policy that is publicly available, and to make a commitment to comply with the principles of data protection and privacy as set out in the EU data protection laws.

The Safe Harbor Program is not a self-enforcing program, and it is up to the companies that participate in the program to ensure that their data protection and privacy practices comply with the principles of data protection and privacy as set out in the EU data protection laws.
Although BCRs are referred to as “rules,” an organization does not need to have a set of rules to place a seal of approval on the issue of privacy, nor will anyone wake up at 4 a.m. to check whether the BCR application process has been signed off by a lead data protection authority. When BCRs first arrived on the scene a few years back, a major drawback associated with them was the fact that they needed to be approved by every EU data protection authority in whose jurisdiction the member of the corporate group is located. If the lead data protection authority for each of these jurisdictions is the same, then it may not be an onerous task to ensure the approval of all BCRs is obtained. However, in many cases, the jurisdictions where the BCRs need to be approved are different, so the application process becomes more complicated. This requires the organization to constantly update what can be significant numbers of contracts. This is often viewed as a significant amount of time and resources required.

In addition, the BCR application process has become markedly more streamlined, as one lead data protection authority can now assess the adequacy of BCRs across an entire group, rather than each of the member data protection authorities. This can offer several benefits, including the ability to reduce the frequency of having to submit BCRs for approval by each and every data processing activity carried out, as well as the ability to ensure compliant transfers from the European Economic Area to the United States, privacy by design, the new mantra. In comparison with the new BCRs, not least its limitation to traditional cross-border transfers (one does not have to constantly update what can be significant numbers of contracts) and the need to BCRs for an agreement approach in the event that they need to be approved by multiple EU data protection authorities or for use in BCRs 2.0.

However, this historic view of the solutions and benefits that BCRs were, for many, viewed as an attractive solution made unattractive, given this additional work and length of time required.

Concerns over cost or initial investment of time for BCRs are also often unspecified or inaccurate. While, of course, there is some initial effort, it should not be for companies looking to ensure full compliance with the various other relevant EU regulators in consideration. Companies that looked at this right from a public relations standpoint, as well as the current emphasis on privacy by design, have meant that BCRs are worth renewed interest. Despite the increased scrutiny placed on compliance over the past few years, the history view of the solutions and benefits that BCRs were, for many, viewed as an attractive option than before (and for data controllers and processors), this new breed of BCR makes for a more attractive approach. This means that BCRs can offer.

BCRs 2.0

However, the landscape of the past few years has seen a number of problems associated with traditional BCRs fall away since the introduction of the mutual recognition policy.

The BCR application process has become markedly more streamlined, as one lead data protection authority can now assess the adequacy of BCRs across an entire group, rather than each of the member data protection authorities. This can offer several benefits, including the ability to reduce the frequency of having to submit BCRs for approval by each and every data processing activity carried out, as well as the ability to ensure compliant transfers from the European Economic Area to the United States. BCRs can cover transfers wherever the corporate group may be.

Given these developments and the fact that many BCRs are up and running, that generally provide better terms than Model Contract Clauses (one does not have to constantly update what can be significant numbers of contracts), the need for BCRs makes for a more attractive approach. This means that BCRs can offer.

Comment

While BCRs have been accepted as the standard approach 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 now treated more seriously and serious consideration. Companies that looked at this right from the public relations standpoint, as well as the current emphasis on privacy by design, have meant that BCRs are worth renewed interest. Despite the increased scrutiny placed on compliance over the past few years, the historic view of the solutions and benefits that BCRs were, for many, viewed as an attractive option than before (and for data controllers and processors).

Although BCRs are referred to as “rules,” an organization does not need to have a set of rules to place a seal of approval on the issue of privacy, nor will anyone wake up at 4 a.m. to check whether the BCR application process has been signed off by a lead data protection authority. When BCRs first arrived on the scene a few years back, a major drawback associated with them was the fact that they needed to be approved by every EU data protection authority in whose jurisdiction the member of the corporate group is located. If the lead data protection authority for each of these jurisdictions is the same, then it may not be an onerous task to ensure the approval of all BCRs is obtained. However, in many cases, the jurisdictions where the BCRs need to be approved are different, so the application process becomes more complicated. This requires the organization to constantly update what can be significant numbers of contracts. This is often viewed as a significant amount of time and resources required.

In addition, the BCR application process has become markedly more streamlined, as one lead data protection authority can now assess the adequacy of BCRs across an entire group, rather than each of the member data protection authorities. This can offer several benefits, including the ability to reduce the frequency of having to submit BCRs for approval by each and every data processing activity carried out, as well as the ability to ensure compliant transfers from the European Economic Area to the United States. BCRs can cover transfers wherever the corporate group may be.

However, this historic view of the solutions and benefits that BCRs were, for many, viewed as an attractive option than before (and for data controllers and processors), this new breed of BCR makes for a more attractive approach. This means that BCRs can offer.

BCRs 2.0

However, the landscape of the past few years has seen a number of problems associated with traditional BCRs fall away since the introduction of the mutual recognition policy.

The BCR application process has become markedly more streamlined, as one lead data protection authority can now assess the adequacy of BCRs across an entire group, rather than each of the member data protection authorities. This can offer several benefits, including the ability to reduce the frequency of having to submit BCRs for approval by each and every data processing activity carried out, as well as the ability to ensure compliant transfers from the European Economic Area to the United States. BCRs can cover transfers wherever the corporate group may be.

However, the landscape of the past few years has seen a number of problems associated with traditional BCRs fall away since the introduction of the mutual recognition policy.

The BCR application process has become markedly more streamlined, as one lead data protection authority can now assess the adequacy of BCRs across an entire group, rather than each of the member data protection authorities. This can offer several benefits, including the ability to reduce the frequency of having to submit BCRs for approval by each and every data processing activity carried out, as well as the ability to ensure compliant transfers from the European Economic Area to the United States. BCRs can cover transfers wherever the corporate group may be.

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