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 14, NUMBER 2 >>> FEBRUARY 2014

Personal Data Transfers from the European Economic Area: Binding Corporate Rules Emerge as Increasingly Attractive Option

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

It is difficult to recall a time when the issue of personal data transfers from the European Economic Area ("EEA") has been as widely and hotly debated as it has over the past year or so. Significant movements during the past year saw not only continued discussion in connection with the draft EU Regulation ("Draft Regulation") to replace the existing EU Data Protection Directive but also concerns following the revelations of former U.S. National Security Agency contractor Edward Snowden, amongst other things. "Where is data going?", "Who is receiving it?", "On what basis are companies transferring data?" and "Are those transfers lawful?" are all questions brought into fresh focus.

In our earlier article, "Personal Data Transfers from the European Economic Area: Time to Consider Binding Corporate Rules 2.0" (*see WDPR, April 2013, page 4*), we proposed that, for a variety of reasons, Binding Corporate Rules ("BCRs") were worthy of fresh consideration by companies operating internationally as a way to adequately safeguard personal data transferred out of the EEA, thereby ensuring that their transfers are compliant with EU data protection laws relating to extra-EEA transfers.

In this article, we consider whether the same is still true, or even more valid, one year on, assessing the current status of other routes to ensuring that transfers are "adequately safeguarded", *i.e.,* the EU-U.S. Safe Harbor Program ("Safe Harbor Program") and Model Contract Clauses ("MCCs").

In concluding that the merits of BCRs have in fact been enhanced over recent months, we also draw upon pan-EU BCR filing experience to provide what we hope is helpful insight into some of the practical aspects of filing a BCR application, and some of the factors to consider when selecting which EU data protection authority to deal with an application.

EU Concerns over the Safe Harbor Program: What Does the Future Hold?

Following strong EU criticism over the last year, some serious question marks have been left hanging over the future of the Safe Harbor Program.

In particular, largely prompted by the alleged acts of Mr Snowden and the U.S. National Security Agency's PRISM Internet surveillance program, the European Commission ("Commission"), the EU executive arm which granted adequacy status to the Safe Harbor Program in 2000, published in autumn 2013 a series of recommendations that it said the U.S. Department of Commerce, the U.S. administrator of the Safe Harbor

Program, should respond to in 2014, or else the program might be suspended, the Commission commenting that it was "not convinced" that U.S. companies, nor the U.S. administration, were respecting the Safe Harbor Program (*see WDPR, December 2013, page 22*).

BCRs seem in many ways the best option for those with a large international footprint and that want to find a longer term solution with respect to their extra-EEA transfers.

These recommendations, in summary, relate to greater transparency on the part of the adhering companies (*e.g.,* a call on Safe Harbor Program-certified companies to publish the privacy conditions in contracts concluded with subcontractors), stricter enforcement (there being deemed by the Commission to be a lack of action on the part of U.S. enforcers) and the inclusion in corporate privacy policies of disclaimers relating to the possibility that mandatory disclosure of data to law enforcement bodies might be required.

In response, the U.S. administration has stood its ground on a number of aspects and defended the Safe Harbor Program, cautioning that not all of the reforms proposed by the EU will be workable.

Given the exchanges, a considerable cloud has been cast over the future of Safe Harbor. Whilst it remains unclear whether suitable agreement across the Atlantic will be reached on the various concerns, there would appear to be considerable merit, in our view, for companies that wish to adopt an updated compliance strategy with respect to their EEA-U.S. transfers to seriously consider an alternative solution to the Safe Harbor Program.

Indeed, could we see a scenario where the many U.S. organisations currently relying on the Safe Harbor Program are left without a robust legal basis for transferring data to the U.S.?

Companies using Safe Harbor should also importantly note a new increased risk that we will see a shift to tougher enforcement. In an apparent attempt to appease the Commission, the U.S. Federal Trade Commission, the U.S. body responsible for enforcement action under the Safe Harbor Program, has committed to increased enforcement action in the near future.

Hugh Stevenson, deputy director of the FTC's Office of International Affairs, promised in December 2013 that there are "matters in the enforcement pipeline, and you can expect to see developments in the coming months".

Delivering on that promise perhaps sooner than might have been expected, the FTC announced in January 2014 that 12 U.S. companies had agreed to settle FTC charges that they falsely claimed they were in compliance with the U.S.-EU and U.S.-Switzerland Safe Harbor programs, when in fact they had let their certifications lapse (*see report in this issue*).

This raises a further red flag, evidencing action by U.S. enforcers against those companies certified under Safe Harbor and found to be non-compliant.

Model Contract Clauses: Recent Developments

So, given Safe Harbor's problem areas, what is the latest position in relation to MCCs?

It should be recalled that MCCs provide another possible extra-EEA data transfer solution by giving an EEA data exporter the ability to contract with a non-EEA importer of the data in a manner that safeguards the treatment and handling of the data to EU-approved standards, the "adequacy" thereby being ensured, provided certain approved clauses are used and adhered to.

It can be argued that the attractiveness of MCCs increased in recent months to the extent that some of the "red tape" traditionally associated with their use in some EU member states was removed. In other member states, MCCs finally became "recognised", another step in the right direction.

For example, in Belgium, a new protocol between the Privacy Commission and the Ministry of Justice was adopted providing data exporters with a streamlined approach to validate transfers on the basis of MCCs (*see WDPR, August 2013, page 26*).

In addition, in the Slovak Republic, it was decided that transfers of data relying on MCCs no longer have to be first authorised by the Slovak data protection authority (*see analysis at WDPR, July 2013, page 13*).

And, in Poland, legislation expected to enter into force early this year would finally recognise MCCs as a basis for the transfer of data (*see analysis at WDPR, December 2013, page 17*).

All such developments are undoubtedly a "victory" for the MCC cause, and make life a little easier for those with multi-jurisdictional operations that seek to use them.

However, MCCs are not without numerous drawbacks, as has been previously discussed, and the traditional disadvantages associated with their use do remain (*e.g.,* they are generally management or senior personnel intensive and very time consuming when a large number are used or a business is large or widely spread, inflexible if the business wants to look to new data use or marketing activities, *etc.*).

In addition, in October 2013, the Committee on Civil Liberties, Justice and Home Affairs ("LIBE") of the European Parliament ("Parliament") also raised doubts over the long term use of MCCs.

More specifically, during the course of voting on amendments to the Draft Regulation, LIBE voted that MCCs should expire after a "sunset period" of two years. In other words, after this period, those relying on MCCs would lose their protection and should revisit their extra-EEA transfers to ensure that they were adequately safeguarded (*see analysis at WDPR, November 2013, page 4*).

 COPYRIGHT © 2014 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. ISSN 1473-3579

Whether this suggestion makes its way into the final draft of the legislation does, of course, depend on the trialogue among the Parliament, the Commission and the EU Council. However, for now, whilst this issue remains open, this development could be described as an additional "thorn in the side" of MCCs going forward.

Binding Corporate Rules Revisited

In light of the various developments mentioned, has the value of BCRs therefore increased?

By way of recap, BCRs are, of course, internal codes/rules which entities within a multinational group can "sign up to", demonstrating that their data privacy and security practices meet EU standards, offering potentially an attractive alternative to the Safe Harbor Program and MCCs.

We would argue that the value of BCRs has indeed increased in light of recent developments, and that the time is ripe for multinational entities to reconsider BCRs. In particular, BCRs seem in many ways the best option for those with a large international footprint and that want to find a longer term solution with respect to their extra-EEA transfers.

We discuss the reasons for this in more detail below.

Debunking Some Myths about BCRs

It has become apparent when talking to many international clients that there remains an outdated and many times incorrect view of what BCRs are or what they entail. It's therefore helpful to consider what the realities are, what's changed and what the procedural formalities associated with filing a BCR application actually are. It also is worth considering the data protection authorities with which one will deal in respect of an application.

BCR Procedural Formalities

There are two types of BCRs which can be utilised: "controller" BCRs, which frame transfers within a group, and "processor" BCRs, which create a "safe area" for data transferred by processors to subprocessors that belong to the same group.

Processor BCRs were introduced in 2013 and are considered to be particularly useful for cloud service providers and other organisations outsourcing their data processing (*see analysis at WDPR, July 2013, page 7*). Throughout the last year, some of the first applications for processor BCRs were submitted.

In terms of the physical application to a data protection authority for "approval" of a set of BCRs, the controller BCRs and the processor BCRs follow a very similar application form and procedure.

Importantly, both applications can seek to rely on the mutual recognition system, of which 21 EEA member states are currently a part.

To recap, under the mutual recognition procedure, an applicant applies to a "lead" data protection authority for approval of the application, which then appoints two additional data protection authorities to further verify that the application meets the requisite standard.

Once "approved", the application is then circulated to the remaining signatory data protection authorities, which confirm their approval of the application.

Of note, during mid-2013, with respect to processor BCRs, the EU Article 29 Data Protection Working Party (the "Working Party") provided further guidance on what the BCRs need to cover and which elements need to be specified in the application form.

BCR 'Forum Shopping'

In terms of selecting the lead data protection authority to which to submit an application, this will, generally speaking, "come out in the wash" and be determined by the key facts, such as the jurisdiction in which the applicant's EU headquarters are based, where the majority of the applicant's data in the EU is processed, where the majority of the applicant's EU employees are based, and so on.

Nevertheless, determining which should be the lead authority can be described as an art rather than a science, and applicants can seek to be a little creative in persuading a data protection authority that it should be, or should not be, the lead authority and in determining which the two additional "sense checking" data protection authorities should be.

Importantly, there may be strategic reasons why a particular data protection authority is selected, or avoided.

For example, if timing of the approval is critical, then it may be a good idea to avoid some of the typically "stretched" data protection authorities that experience a large volume of BCR applications, such as the Commission nationale de l'informatique et des libertés ("CNIL") in France, the Netherlands' College bescherming persoonsgegevens and the Information Commissioner's Office ("ICO") in the U.K. Recent plans at the ICO call for re-routing BCR applications to a greater resourced team within the ICO, but whether this will reduce the time required for application approvals remains to be seen.

Instead, a data protection authority that has only recently begun accepting BCR applications may be chosen (where this is possible, of course), on the assumption that there are fewer applications in the pipeline and there is greater reviewing capacity. The Slovak Republic Office for Personal Data Protection is an example of such a data protection authority. Of course, familiarity with the BCR process may be lower at such authorities, which could be a drawback, and language requirements may also come into play.

Post-approval challenges may also influence the data protection authorities which are sought after.

For example, in some EEA jurisdictions, such as France, Spain, Belgium and Norway, it may still be necessary for data protection authorities to provide a permit for transfers based on the safeguards provided for in a BCR before such transfers can be made. As a result, those hav-

ing to deal with these jurisdictions should be aware of such additional red tape.

In some member states, such as Italy, there are also typically translation requirements and fees to be paid before a request for approval can be considered. As a result, there may be good reason to contact the data protection authority in such countries earlier on in the process rather than later.

There is also merit in listening to the latest noises being made by a particular data protection authority before submitting an application or asking it to be a second pair of eyes.

For example, the data protection commissioner for Berlin, Mr Alexander Dix, recently suggested, in the post-Snowden era, that stringent questions are currently being asked of applicants as to the measures they are taking in order to prevent foreign intelligence services accessing data, and that, if such questions cannot be answered satisfactorily, an application is unlikely to be progressed.

Whilst the European Commission and national data protection authorities have attempted, and in some cases succeeded, in recent years to bring the various moving parts more closely together, either through guidance or initiatives relating to national filing or authorisation of transfers, the reality on the ground can still often prove to be a little confusing, given the numerous different data protection authorities and local laws to contend with.

For example, until fairly recently, BCRs were problematic in Belgium, as although Belgium is part of the mutual recognition scheme, it had been almost impossible to approve BCRs there due to requirements of the Belgian Privacy Act, including the need for a royal decree to authorise a transfer, which subsequently had to be dealt with by a protocol being signed with the Belgian Ministry of Justice.

In terms of BCR "forum shopping", therefore, a detailed and up-to-date analysis of national law, the national data protection authority's approach and any proposed changes is necessary before "cherry picking" which countries are the most suitable fit.

BCRs: The Future Solution?

Given that BCRs are expressly recognised in the Draft Regulation and have continued to be lauded by Commissioner Viviane Reding, who recently said, "I encourage companies of all size to start working on their own binding corporate rules", it can be said with a high degree of certainty that BCRs are not going away anytime soon — a clear advantage of this solution, given everything that is going on in the world of data privacy right now.

Whilst one potential wrinkle to this is the fact that LIBE's proposed amendment to the Draft Regulation excludes processor BCRs from it, given that this flies in the face of the recent work of the Article 29 Working Party and widespread support for processor BCRs across the EU, it is difficult to imagine that the odds of them disappearing are high.

There is a further clear advantage of BCRs, however, if a further proposal of LIBE is carried through to the enacted Regulation.

In particular, LIBE proposed the introduction of a "European Privacy Seal" scheme under the Draft Regulation, whereby data controllers that could demonstrate full compliance with EU privacy law would be issued with a compliance seal. Such a certification would be valid for five years and a public register of certifications would be maintained. It is envisaged that the awarding of such a seal would permit cross-jurisdictional, extra-EEA, intra-group transfers of data in the same way that BCRs do now (as well as having other key advantages, such as a certified company not being subject to fines unless the data breach was intentional or negligent).

Significantly, because it is envisaged that existing BCRs would be an advantage in obtaining a seal, this should mean that doing some upfront work now in terms of getting BCRs in place could pay further dividends down the line.

All of this, in addition to the fact that, under current proposals for the Draft Regulation, a "consistency mechanism" is set to be introduced whereby any data protection authority seeking to approve a BCR application must first refer the application to the proposed European Data Protection Board, means that there may be no better time than the present to consider and look to put in place BCRs.

Summary

Given all of the above, it is fair to say BCRs continue to pull away from earlier criticisms or perceptions and do now have a number of arguable advantages over the Safe Harbor Program and MCCs.

In fact, given the current status of the Draft Regulation, it could be said that BCRs should be considered one of the best solutions — and, in some cases, the best solution — for multinational organisations exporting and importing data globally.

In light of the fact that the BCR application process could possibly become a little more arduous under proposed plans, and given, once approved, that BCRs will remain valid once the Draft Regulation becomes law, it is also fair to say, as a final thought, that consideration of BCRs and possibly making an application now should be high on any board room agenda for those multinationals that have not got the ball rolling already.

Rafi Azim-Khan is a Partner and Head of 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.

 COPYRIGHT © 2014 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. ISSN 1473-3579