New Binding Corporate Rules Now Available for Data Processors

By Steven P. Farmer, Simon J. Lightman, and Meighan E. O'Reardon

In a further push towards "privacy by design," the Article 29 Working Party, which is made up of representatives from the various EU data protection authorities, has recently approved the use of Binding Corporate Rules ("BCRs") for international transfers of personal data by data processors effective as of January 1, 2013.

While BCRs have been an option for data controllers to ensure compliant transfers from Europe for some time, the introduction of BCRs for processors has been welcomed by both data controllers[1] and data processors[2] alike. Significantly, in the outsourcing context, multinational service providers who act as data processors will now have the ability to more simply demonstrate to their data controller customers that their transfers to locations outside of the European Economic Area ("EEA")[3] are compliant.

General Background on EU Data Protection Directive

Article 25.1 of Directive 95/46/EC (the "Data Protection Directive")[4] prohibits the transfer of personal data to a third county (i.e., a country or territory outside the EEA) unless that third country provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The European Commission ("EC") has so far recognized only a handful of countries that offer an adequate level of protection, including Andorra (in 2010), Argentina (2003), Canada (2002), Faroe Islands (2010), Guernsey (2003), Isle of Man (2004), Israel (2011), Jersey (2008) and Switzerland (2000). However, there

1 Under the Data Protection Directive a Data Controller is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ..." In most outsourcing arrangements, the data controller is the customer that has procured services from a third-party service provider.

2 Under the Data Protection Directive a Data Processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." In most outsourcing arrangements, the data processor is the service provider.

3 The EEA comprises the EU Member States plus Iceland, Liechtenstein and Norway.

4 In the United Kingdom, this is enacted through the eighth principle of the Data Protection Act, 1998.

are several mechanisms available to organizations to "legitimize" transfers of personal data outside of the EEA to countries not recognized by the EC as being adequate. These include, for example:

- the use of the approved model clauses between the relevant exporter and importer of data ("Model Clauses");
- in relation to many U.S. organizations, adherence to the Safe Harbor scheme signed between the EC and the U.S. government in 2000; and
- the use of Binding Corporate Rules ("BCRs").

Binding Corporate Rules

BCRs are internal codes of conduct which entities within a multinational group can "sign up to," demonstrating that their data privacy and security practices meet European standards.

In the context of outsourcings and other service arrangements (e.g., the purchase of cloud computing services), BCRs have not previously been used by data processor service providers as a means to transfer personal data outside of the EEA because, prior to January 1, 2013, they were only available to data controllers in relation to internal transfers of their own data. Instead data processor service providers transferring data from the EEA had to rely on other mechanisms to ensure transfers were adequate, including the use of Model Clauses or a U.S. service provider's Safe Harbor membership. However, each of these routes has drawbacks. For example:

- the Safe Harbor scheme is not available to companies in all sectors (e.g., telecommunications companies and financial institutions are not covered by the regime) and is limited to the transfer of data from the EEA into only the United States; and
- reliance on model clauses can mean entering into often complex networks of contracts in addition to the main service agreement. This can lead to protracted negotiations with service provider group members in multiple jurisdictions. The contracts also need to be closely monitored and updated whenever data processing activities change.

New Binding Corporate Rules for Data Processors

To address compliance concerns, specifically among cloud computing providers and outsourcers, the European Data Protection Authorities approved BCRs for data processors, effective January 1, 2013 ("Processor BCRs")[5]. Once a multinational processor has an approved set of BCRs, it will be able to transfer the personal data of its clients under its BCRs outside of the EU while remaining in compliance with the EU data protection rules.

Significantly, a Processor's BCRs can be relied upon by the data controller to demonstrate compliance. The Article 29 Working Party envisions that a Processor's BCRs will become part of the guarantees that a data controller will present to Data Protection Authorities to demonstrate adequate protection and to obtain the necessary authorization for transfers of personal data to different entities of their Processor (notably to foreign data centers).

5 See Article 29 Data Protection Working Party Press Release available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf

The Processor BCRs include many of the same commitments required under the data controller BCRs. Processors must be willing to assume liability for any breaches of personal data transferred within their organization. The Processor BCRs also must grant third-party beneficiary rights to data subjects, meaning individuals will be able to directly enforce the BCRs against the data processor. Finally, Processor BCRs limit forward transfers of personal data to unrelated third parties.

The application procedure for Processor BCRs is broadly the same process currently in place for data controller BCRs. Processors file an application with a lead Data Protection Authority using a form that closely resembles the existing data controller application. Similar to data controllers, data processor applications will also invoke a system of mutual recognition between twenty-one EU States,[6] meaning that once an application is "approved" by a lead authority, it is effectively rubber-stamped in those other territories relevant to the application.

Considerations for Data Processors

IT outsourcing providers, cloud providers and data center providers who implement Processor BCRs will now be able to receive data in Europe from their controller clients and then transfer that data within their group, outside of Europe, while complying with European privacy rules.

For processors who choose BCRs to ensure compliance, this development could significantly reduce the managerial time (and paper) spent negotiating often complicated, data protection safeguards for each and every data processing activity they carry out, while also doing away with the supervision associated with managing such contracts. At the same time, this development offers controllers' clients comfort that the controller will be able to more simply demonstrate that their processing activities comply with European laws by pointing to an approved set of BCRs.

While the use of BCRs for processors is not obligatory, it is expected that they will be widely utilized.

In short, if you are a multinational organization processing data in Europe (or controlling and processing such data), this new BCR framework may offer the opportunity for cost savings for your business, reducing managerial headaches and helping to position the firm as a more attractive option to potential clients.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Steven P. Farmer (bio)
London
+44.20.7847.9526
steven.farmer@pillsburylaw.com

Simon J. Lightman (bio)
London
+44.20.7847.9500
simon.lightman@pillsburylaw.com

Meighan E. O'Reardon (bio)
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

6 Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain, and the United Kingdom.