

## ***Volume 7 Issue 10 October 2010***

### **Data Transfers: BCRs v model contracts: data transfer compliance**

Companies that transfer personal data across borders face different challenges, depending on their size and the complexity of the transfers they operate. Frédéric Blas, Associate Lawyer at J. Olleros & Asociados, analyses the tools currently available, and discusses the advantages and disadvantages they offer to companies with different needs.

For a global company, to offer services and products with the same quality standards is equally important as the ability to share data and information with its affiliates and subsidiaries.

Companies, regardless of their size, increasingly delegate or outsource part of their services or tasks to other companies that provide this service in a third country outside the EU/European Economic Area (EEA) - call centres, data processing, cloud computing. Much of this information contains personal data, the processing and transfer of which is subject to numerous regulatory constraints. The information that a company holds about employees, customers, business partners, suppliers and providers is a very valuable asset. Exploiting this information correctly is crucial for a company's operations and many applications, but its use on a global basis is strictly regulated by European Union data protection law.

#### Legal issues, strategic and operational challenges

As large multinationals are processing data regardless of where data processing occurs, the transfer of personal data in jurisdictions outside the EU/EEA is a complex legal issue and means to work with 30 different regulatory requirements, adding months to any initiative you want to roll out globally. The transfer of personal data in jurisdictions outside the EU/EEA is prohibited by the EU Data Protection Directive (95/46/EC), which required all Member States to enact comprehensive data protection laws. The result is that each Member State now has its own law, administered by its own Data Protection Authority (DPA).

#### Standard contractual clauses

Standard contractual clauses are standard agreements between a data exporter and one or more data importers which help a company comply with the obligation to ensure adequate protection for personal data when they transfer personal data to processors outside the EU/EEA. The use of standard contractual mechanisms is one of the

most widely-used methods to legitimise global data flows and provide adequate safeguards, fulfilling the requirements of the Data Protection Directive. Such agreements are legally enforceable, as the data exporter and the data importer undertake to process the data in accordance with basic data protection rules and agree that individuals may enforce their rights under the contract, blocking transfer or production of the information at any time.

Three sets of standard contractual clauses are currently available:

- For data transfers from controller to controller - following the European Commission's Decision of 15 June 2001.
- For data transfers from controller to controller - following the European Commission's Decision of 27 December 2004. Developed by the International Chamber of Commerce, these clauses are more business-friendly.
- For data transfer from controller to processor and eventually to sub-processors - following the European Commission's Decision of 5 February 2010. This new set takes account of the whole chain of processing activities and deals with outsourcing of processing to sub-processors.

### ***BCRs and standard contractual clauses - advantages***

<b>BCRs</b>	<b>Standard contractual clauses</b>
One standard for all affiliates	Internal process
Work on functional boundaries instead of national boundaries	Standardised procedure
Tailored to a company's business needs and driven by its culture. The company - not the regulator - determines how the system operates	For many businesses with limited cross border transfers the use of the standard clauses should be sufficient
Allow the launch of global projects and global databases faster and at lower costs	As an agreement between two parties it only exposes the importer to the extent the exporter has ceased to exist or becomes insolvent
Flexible and long-term approach	Streamlined approval process
Only one application to all DPAs involved - mutual recognition	At the moment the only solution for client's outsourcing or joint ventures
Better ability to communicate rules and values to employees - increased awareness	The only legal instrument that provides compliance for third parties cloud computing operations

### ***BCRs and standard contractual clauses - disadvantages***

<b>BCRs</b>	<b>Standard contractual clauses</b>
Do not extend to transfers to companies outside the group: outsourcing & joint ventures	Hundreds of contracts would be necessary to achieve global compliance
Intra-company data transfers only	Administrative nightmare - requirements can be mandatory: filing, power of attorney etc.
No streamlined mechanism for approval	Updating is not possible
The whole group is exposed to damages (DPAs or data subjects)	Compliance on paper as opposed to material compliance

#### **Binding Corporate Rules**

As a complex intra-corporate global privacy policy that allows data to flow freely between a company's affiliates and subsidiaries and satisfies EU standards, BCRs are not a license to unrestricted use of personal information, but allow companies to transfer personal data around the world using a single set of rules, which gives individuals the confidence that their personal data are being processed using a binding and enforceable set of privacy standards. BCRs make compliance less time-consuming and costly, and provide multinational corporations with greater flexibility than most alternative legal bases. While the use of contractual mechanisms in the data protection context is currently focused on international data transfers, BCRs can be used to provide overall compliance within the corporate group - their use is not limited to data transfers.

BCRs are however very difficult to manage, as rules have to be binding within the entire corporate group, parent and subsidiaries and the path to a BCR certification involves significant procedural challenges and substantive hurdles.

The WP29 imposes three substantive requirements on BCR. Firstly, BCRs must identify the nature of the data that will be processed, the purposes of the processing and the data flows - internal processing, external processing, identity of parties involved and locations of processing. Furthermore, BCRs must be legally binding within the corporate group and enforceable by the data subjects - this is fundamental to the entire concept of BCRs. It is necessary to prove to the DPAs that the rules are legally enforceable and can be complied with by the organisation. Evidence that the BCRs are binding on all members of the organisation, and can be enforced by the data subjects as third party beneficiaries, is required. Finally, BCRs must apply to a corporation's entire global structure. The BCR approach is advantageous where a flexible or complex structure of

data processing is in place, so that tailored rules have to be used. It is a responsible approach to handling people's personal information and the best solution for complex corporate structures and complex cross-border data flows. BCRs can accommodate many different practices and organisational structures, from highly hierarchical configurations to loosely assembled groups of entities. It is a global privacy policy rather than a mere international data transfer instrument. The standard contractual approach is not very flexible to deal with some of the objectives of a global corporation but it would fit perfectly within a company with few subsidiaries and/or limited data flows outside the EEA. The choice between the two approaches will depend on the corporate structure, size, activities and amount of data that are being processed. Some corporate giants have already chosen BCRs to improve privacy compliance within their corporation (GE, Philips, Daimler, BP, Accenture), and many more will switch to BCRs in the future.

Frédéric Blas

Associate Lawyer

J. Olleros & Asociados

[fblas@ollerosyasociados.com](mailto:fblas@ollerosyasociados.com)

Unless otherwise stated © 1999-2006 Cecile Park Publishing Ltd.

Close this window