International Data Privacy Law Advance Access published November 25, 2011

Binding Corporate Rules: a global solution for international data transfers

Olivier Proust* and Emmanuelle Bartoli**

Introduction

Technological developments and the globalization of the economy intensify the collection and flows of personal data. That increasing phenomenon, that can mainly be observed in multinational corporations, is often due to economic or strategic choices such as the off-shoring of some activities, the relocation to emerging markets or the reorganization of information systems. For instance, many companies decide to centralize all their employees' data in a single database located abroad, most of the time outside the European Union (EU). Others may choose to outsource their data processing activities in countries located outside the EU or to share information systems.

However, under EU law, the transfers of personal data outside the EU are strictly regulated by Directive 95/46/EC.[1] In principle, it is prohibited to transfer personal data outside the European Economic Area (EEA) unless a company can demonstrate that it guarantees an adequate[2] level of protection for personal data being transferred outside the EEA (ie a protection level equivalent to the level offered within the EEA).

In order to comply with this obligation, the European Commission has developed a set of legal instruments which are recognized both by the European Commission and by data protection authorities (DPAs) as providing an adequate level of protection. Companies are already well acquainted with some of these legal instruments (eg standard contractual clauses or Safe Harbor) and have been using them for some time. However, in today's globalized world, it has become increasingly challenging to rely solely on such instruments for frequent and multiple data transfers across jurisdictions.

Abstract

- Transfers of personal data outside the European Union are strictly regulated by the European Data Protection Directive.
- In today's globalized world, it has become increasingly challenging for companies to comply with the restrictions imposed by European data protection law. The existing legal mechanisms approved by the European Commission and the national data protection authorities have become, to a certain degree, ill-adapted to multiple and cross-jurisdictional transfers of personal data.
- In recent years, Binding Corporate Rules (BCR) have become a fast-growing legal mechanism that is more widely recognized by companies as an efficient tool for framing international transfers.
- BCR bring a truly globalized response to the issues associated with international data transfers within the same corporate group. In particular, companies appreciate their pragmatic approach and the fact that they can communicate more openly to their employees, clients, and suppliers about their data processing activities.
- BCR must first be approved by the national data protection authorities before they can be used by companies. To this end, data protection authorities in Europe have developed a cooperation procedure, which aims at recognizing BCR as an effective tool for providing an adequate level of protection to personal data being transferred globally.

* Associate, Hunton & Williams and Member of the Paris Bar, Email: oproust@hunton.com

** European and International Affairs, CNIL, Email: ebartoli@cnil.fr.

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2 By 'adequate' level of protection is meant a personal data protection regime in a third country recognized by the European Commission as equivalent to the level offered by Directive 95/46/EC.

- In the near future, the European Commission may officially recognize BCR as a valid accountability measure that enables international organizations to comply with European data protection regulations.

For this reason, the Article 29 Working Party (WP 29) has developed 'Binding Corporate Rules' (BCR) with a view to providing multinational companies with a legal solution meeting their needs and structure. Since their creation in 2003, BCR have become a fast-growing legal mechanism and are more widely recognized by companies as an efficient tool for framing international transfers. The European Commission is also considering introducing BCR within the revised Directive 95/46/EC. This article describes and explains the goals of BCR, and the required legal steps for a company's BCR to be officially adopted and recognized by the DPAs as a valid legal mechanism for transferring data.

BCR as an alternative solution for exchanging data within the same corporate group

Realizing the shortcomings of the legal instruments guaranteeing an adequate level of protection (ie legal derogations, model clauses, Safe Harbor), the WP 29 deemed it necessary to authorize companies to adopt binding internal rules in order to regulate the transfers of personal data within the same corporate group. The WP 29 views BCR as an alternative solution appealing to multinational companies owing to the guarantees attached to the transfers of personal data within the same group of companies.

A code of conduct regulating intra-company transfers

Binding Corporate Rules are a set of binding legal or legally enforceable rules that apply to international data transfers.[3] As in other legal areas (eg corporate policies for the protection of the environment, the application of best commercial practices, the respect of competition rules on the market, and the fight against corruption and money laundering), BCR constitute a code of conduct[4] setting out the internal policy applicable to intra-company transfers of personal data.[5] So instead of implementing various legal instruments in order to regulate data transfers, BCR may be used as a single instrument regulating all transfers conducted within the same corporate group. Therefore, BCR facilitate data transfers within that group while offering a high level of protection of personal data, regardless of the group entity the data are transferred to.

Binding Corporate Rules also foster data subjects' trust in the data controller. Indeed, a company can use its BCR as an argument when communicating with its consumers, its suppliers, and its clients, and demonstrate that it complies with the European principles of personal data protection. BCR appear, therefore, as a communication tool, if not a marketing tool, enabling the company that has adopted them to stand out against its competitors.

A global data protection policy

More than a set of legal rules, BCR can serve the establishment of an effective global policy, of an 'internal standard'[6] for personal data protection within the group. Indeed, they apply indiscriminately to the whole corporate group, regardless of the establishment of the subsidiaries or of data subjects' citizenship. They contribute to harmonizing practices and, as a result, to alleviating the risks associated with the processing of personal data, in particular within the entities of the group established in countries lacking personal data protection legislation. BCR also enhance the introduction to the company of a set of social values focusing on the protection and security of personal data.

One of the key principles for BCR is their binding nature on employees and on the corporate entities. DPAs pay particular attention to the bindingness of BCR since all entities of the group, and particularly those that are located outside the EEA, must comply with the group's BCR. This bindingness also guarantees that the data subjects may bring a claim against the company in case of a breach of their rights. The manner in which companies may achieve such a result depends on their corporate structure and organization (eg intra-group agreement, unilateral declaration). The DPAs may also interpret bindingness differently as

3 See WP 74, 'Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm> accessed 19 October 2011.

4 For instance a corporate policy implemented by the headquarters or an internal code of conduct supported by a corporate agreement.

5 See CNIL, 'Transferts de données à caractère personnel vers des pays tiers à l'Union européenne', juin 2008, <http://www.cnil.fr/vos-responsabilites/le-transfert-de-donnees-a-letranger/> accessed 19 October 2011.

6 Ibid.

there is no widespread interpretation of this legal concept under EU law. As a consequence, companies are expected to provide specific internal documents and policies in support of the effective binding nature of their BCR in order to demonstrate to DPAs that their BCR are effectively binding.

A set of practical measures aimed at respecting the principles of personal data protection

In practice, the corporate group adopting BCR commits itself to practical measures with a view to respecting the legal principles set out in Directive 95/46/EC.[7] These measures are implemented on a case-by-case basis and may vary depending on the compliance level of each company. For example, the DPAs expect companies to train and educate their employees on data protection matters and may require copies of presentations or training sessions. Companies are also required to implement various corporate policies, such as an employee privacy policy, an information security policy or an acceptable use policy. Other examples of practical measures may include the setting up of a network of data protection officers, the existence of an auditing scheme and the development of an internal complaint handling process. Many companies have already taken such proactive measures and need only materialize their commitments in BCR.

In connection with the review of Directive 95/46/EC, the WP 29 has suggested the introduction of an 'accountability principle' which would impose on data controllers the obligation to take proactive measures for processing personal data so as to be able to demonstrate to the DPAs their compliance with the principles set out in the Directive.[8] If the accountability concept is introduced in the new version of Directive 95/46/EC, companies that have adopted and implemented BCR will already be in a position to display their compliance efforts. Therefore, BCR can serve as an effective accountability tool.

A flexible and tailored mechanism

Binding Corporate Rules offer more flexibility than standard contractual clauses. In practice, the use of standard contractual clauses can prove burdensome for a multinational company that frequently transfers personal data to its subsidiaries (for instance when the same data are being transferred to multiple corporate entities). If standard contractual clauses bring a certain legal certainty to companies (because they were adopted by the European Commission), that certainty is gained at the expense of flexibility in the wording. If the standard clauses are modified, the DPAs reserve the right to accept or to reject the new version. Moreover, their scope is strictly limited to the transfer they apply to. If the scope of the transfer changes (owing to the extension of the categories of data being transferred, new purposes for the transfer, or multiple data recipients), or when a company carries out new transfers, the company must either change its existing clauses or sign a new set of clauses.

On the contrary, in the case of BCR, a company can draft a set of legal rules tailored to its needs, structure, culture, and type of governance.[9] The company defines their geographical (ie the group subsidiaries and the jurisdictions covered) as well as the material scope (ie the nature of the processing, the data categories, and the data subjects) covered by the BCR. It can also draft its BCR in a language and style particular to the company, so as to make them clear and understandable to its employees, its consumers, and business partners. In the end, BCR are a tailored mechanism that the company can adjust to its needs. They therefore offer many advantages for multinational companies, but still must be approved by the DPAs.

Procedure for the approval of BCR by national DPAs

Binding Corporate Rules have the advantage of being officially recognized by all the DPAs within the EEA as an adequate legal mechanism for transferring personal data. Prior to this recognition, the DPAs verify that the commitments taken in the BCR offer an adequate level of protection. This verification is conducted in the course of a so-called 'cooperation' procedure during which a 'lead DPA' is appointed and at the end of which all DPAs recognize the adequacy of the tool adopted by the company.

The designation of a lead authority

In order to spare companies the trouble of reiterating the approval procedure with every DPA, the WP 29 has agreed to nominate a coordinating lead authority at

7 These principles include the lawfulness of the processing, legitimacy, transparency, proportionality, and security.

8 See WP 168, 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', adopted on 1 December 2009, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009_en.htm> accessed 19 October 2011.

9 See ICC, 'Report on binding corporate rules for international data transfers of personal data', prepared by the ICC Task Force on Privacy and Protection of Personal Data, published on 28 October 2004.

the start of the procedure, which coordinates the process and seeks approval of the BCR by its European counterparts. The lead authority is appointed based on specific criteria so as to avoid the controller engaging in forum shopping (eg the country where it has its European headquarters, or the jurisdiction of the company with delegated responsibilities, or else the establishment of the company that is better placed in terms of business, management, or administration for handling the application and implementing BCR within the group). Once the controller has identified the lead authority, it sends the latter a form[10] with the reasons supporting the appointment. That form is in turn forwarded to all DPAs concerned that are required to take position within fifteen days. Past that deadline, the chosen authority is formally appointed as lead authority. Simultaneously, the controller has often begun drafting its BCR and for that purpose can rely on a set of documents prepared by the WP 29.

A toolkit designed to help companies prepare their BCR

In order to assist companies draft their BCR, the WP 29 has adopted a number of documents (commonly referred to as 'BCR toolkit') which define the conditions and contents applicable to BCR. After a first working document (WP 74)[11] setting out the general terms of BCR, the WP 29 adopted a table (WP 153)[12] presenting and explaining the legal principles the company commits itself to. That document also provides the authorities with a common denominator for assessing the level of protection offered by BCR. The WP 29 has also adopted another working document (WP 154)[13] that suggests a possible structure for BCR and tells the company which documents may be annexed (eg internal policies, recommendations, notices, guidance, etc.) in order to demonstrate the actual implementation of BCR within the group. Finally, with a view to answering specific questions that companies may have (eg regarding their liability or the third-party beneficiary clause), the WP 29 has adopted a FAQs document (WP 155).[14] All these documents are designed to facilitate the drafting of BCR while guaranteeing a harmonized approach at the European level. Companies can therefore rely on clear common references recognized as valid by all DPAs.

The time spent preparing the BCR varies depending on the company's level of compliance and its internal approval process. Companies are usually required to obtain approval from their board of managers to receive the go-ahead and to obtain the necessary budget and resources allocated to the project. Due to the likely impact of BCR on businesses and corporate entities, companies are also well-advised to raise awareness and involve key individuals of the group (eg global HR, IT, Ethics & Compliance) at the beginning and throughout the process.

Once the company has drafted its BCR, it sends them for review to the lead authority. The latter can suggest amendments so as to produce a final document meeting the expectations of all DPAs. The finalization of the draft generally requires exchanges between the company and the lead DPA. When the lead authority judges that the BCR are satisfactory, it forwards them to two other designated authorities that have one month to review them and send their comments. This stage lasts for as long as it is necessary to reach an adequate draft. Preparedness and reactivity are two key components that will enable companies to speed up the process. After completion of that first stage, the lead authority sends the draft BCR to all DPAs in the countries concerned (ie the countries the data are transferred from), which marks the beginning of the so-called 'cooperation procedure'.

Speeding up of the cooperation procedure thanks to mutual recognition

The cooperation procedure's aim is to make sure that all DPAs concerned recognize the BCR as providing an adequate level of protection and approve them as such. In order to speed up approval of the BCR by all DPAs, the WP 29 has established a mutual recognition mechanism by which approval by the lead authority equals approval by all the authorities that participate in the

10 See WP 133, 'Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data', adopted on 10 January 2007, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm> acccessed 19 October 2011.

11 See WP 74, 'Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm> accessed 19 October 2011.

12 See WP 153, 'Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules', adopted on 24 June 2008, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm> accessed 19 October 2011.

13 See WP 154, 'Working Document Setting up a framework for the structure of Binding Corporate Rules', adopted on 24 June 2008, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm> accessed 19 October 2011.

14 See WP 155, 'Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules', adopted on 24 June 2008, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm> accessed 19 October 2011.

mechanism.[15] In that way, those authorities acknowledge receipt of the BCR without reviewing them in detail because they rely on the lead authority's prior review. The mutual recognition procedure has also resulted in shortening substantially the approval delay.

Despite the advantages offered by the procedure, up to now not all DPAs have followed it, even though an increasing number of them have done so, thanks to the support of the WP 29.[16] The authorities that have not joined the mutual recognition procedure must therefore review the BCR within a month and can send comments to the lead authority. In practice, those authorities usually do not change the BCR substantially since they rely on the approval initially provided by the lead authority.

After completion of the procedure, the lead authority returns the BCR to the company in order to make the necessary changes required for their final approval. When the cooperation procedure is closed, the BCR are formally recognized by all DPAs as providing an adequate level of protection. From that moment on, the company can rely on its BCR for international data transfers within the corporate group. In this respect, it is worth noting that the approval of BCR does not exempt data controllers from carrying out the prior formalities with the DPAs in the countries where they process personal data and where BCR might be used as a legal basis for transferring data outside the European Union.

Conclusion

The advantages offered by BCR for multinational companies support the increasing popularity of that legal instrument. Several factors contribute to that trend. Companies seem to have realized the risks inherent to international data transfers and demonstrate a stronger willingness to regulate such transfers by providing an adequate level of protection. In addition, compared to other legal instruments (eg model clauses, legal derogations, or Safe Harbor), BCR bring a truly globalized response to the issues associated with international data transfers within the same corporate group. Their pragmatic aspect is highly appreciated by companies that can translate their commitments concretely into a language specific to their needs. BCR also enable companies to communicate more openly with their clients, suppliers, and employees regarding their data processing activities and the protection of personal data. Beyond a legal obligation, BCR are nowadays perceived as a competitive advantage. Finally, the BCR approval procedure by the DPAs, that was once heavily criticized owing to its length and tediousness, has gained in flexibility and speed.

In this context, the time seems to have come for companies to start drafting their BCR. The on-going revision of Directive 95/46/EC could enhance the legitimacy of accountability tools. In the near future, it is likely that companies will have a duty, if not an obligation, to implement proactive measures displaying their compliance with and implementation of the data protection principles set out in the Directive. Companies are also developing more often a sense of 'global privacy compliance', which explains their attractiveness to BCR. In this respect, they understand better the needs and advantages, both internally and externally, to implement adequate measures in order to comply with European data protection principles.

Finally, some DPAs have expressed their willingness to perform more inspections of controllers conducting international data transfers.[17] Thus, companies that have anticipated the risks associated with such inspections (in particular the risk of sanctions) and have adopted BCR will automatically have better visibility of their practices and will be better prepared to demonstrate to the DPAs their commitment to the data protection principles.

doi:10.1093/idpl/ipr023

15 Through 15 May 2011, twenty countries participated in the mutual recognition mechanism, namely: Austria, Belgium, Bulgaria, the Czech Republic, Cyprus, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, Norway, the Netherlands, Slovakia, Slovenia, Spain, and the United Kingdom.

16 In particular, the mutual recognition procedure does not deprive the national data protection authorities of their powers, because they ultimately authorize formally data transfers on the basis of BCR.

17 See CNIL, 'Programme des contrôles 2011: une ambition réaffirmée, des compétences élargies', available at: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews%5BbackPid%5D=2&cHash=91ae300acd> accessed 19 October 2011.