Binding Corporate Rules, the Accenture experience

ANNE WILKES
Data Privacy Compliance Senior Legal Counsel, EMEA, Accenture, UK

Introduction
As a result of the increased awareness of the need to have effective compliance programs in place, the concept of data privacy has recently become very much a hot topic, regularly referred to in the press as well as in the boardroom. Whilst the European Data Protection Directive ("the Directive")\(^1\) was adopted in 1995, most EU Member States did not have any legislation in place until the late nineties. This legislation forced many companies, acting as data controller, to start looking at what sort of personal data they were processing, to consider in more detail the purposes for processing and to start making available or increase budgets allocated to the implementation of security enhancements for the storage of its personal data. Initially many companies did not consider the risk of exposure sufficiently important to justify internal spending on this. These days however, organisations appear to be much more in tune with the compliance trend. It now gives these companies a competitive edge over other organizations, which is especially obvious in the field of data privacy, as businesses have increasingly started to outsource some of their activities to off shore locations such as India or the Philippines, countries which do not have adequate data protection regimes in place. Moreover, data privacy regulators have been given stronger and more efficient enforcement powers resulting in significant fines across Europe, and the adoption of data privacy legislation in other parts of the world such as Canada, Russia and Australia also added to the global awareness of privacy issues. Of course the many press reports detailing lost or stolen CD’s with thousands (if not millions) of people’s personal details on them have not harmed the cause for robust privacy regimes either.

The current trend towards functional globalisation requires a global response and policies having binding effect on all entities across the world. In Accenture’s case this meant having a uniform compliance program in place which served as a basis for its application for Binding Corporate Rules. The following paragraphs describe the pursuit of obtaining approval of the European regulators in respect of this application.

The Accenture experience
Accenture’s globalisation of functional processes brought the need to assess compliance with data privacy laws and how it can share personal data. The move to a public company in 2001 resulted in further commitments to create, develop and implement a data privacy compliance program as part of a larger regulatory compliance program. This program is global in reach and enforcement and provides a uniform level of data protection

---

\(^1\) 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.
worldwide. For big multi national organisations such as Accenture, this is particularly important in respect of inter company transfers of personal data (controller to controller and controller to processor). The program consists of principally one global data privacy policy—largely based on the Directive in order to apply the most rigorous regime for the protection of its internal data—supported by a comprehensive set of data privacy documentation, procedures, education and communication and is based on a mixture of various data privacy regimes worldwide. Where local law provides for either additional rights for the individual or more obligations for Accenture as a data controller, the release of local supplemental documents setting out the relevant details ensures that these variations become part of Accenture’s binding policy. Accenture’s global data privacy compliance program is mandatory for all Accenture employees and is binding on all Accenture entities. It serves as a basis for Accenture’s application for Binding Corporate Rules, the most comprehensive method of ensuring the lawful transfer of personal data to countries which do not provide an adequate level of data protection.

**Why Binding Corporate Rules?**

Accenture required a structure which would globalise its business processes, functions and technology dealing with client, employee and candidate data, allowing intragroup sharing of personal data. The aim was to achieve a substantial level of compliance with data privacy laws worldwide and establish an ongoing compliance culture. Corporate governance and social responsibility are contemporary notions that large international organisations have placed increased focus on. Accordingly they are under a much higher level of scrutiny than they have been in the past.

Externally, Accenture’s business specialised and continues to specialise in the provision of consulting and outsourcing services. Other technology offerings and solutions also formed emerging business opportunities and the inherent pressure to implement technical and organisational measures, not only expected but required from data processors, meant that a robust data privacy program would provide the company with a fierce competitive edge that could not be ignored. Technological developments such as RFID, the increase in identity theft occurrences and the US developments in the field of security breach also contributed to the decision to adopt a high standard of protection for employees’ privacy.

As the company grew, its functional boundaries replaced national boundaries and the gradual erosion of national boundaries meant that a set of rules was required applicable to the entire global organisation, binding on all entities and all employees. Legally, it became clear that the derogations as summed up in art 26 derogations of the Directive were not sufficient to cover all transfers of personal data (prohibited under art 25 of the Directive but with certain derogations allowed under above mentioned article 26) in the normal course of business within a global organisation as it proved impossible to determine whether every single transfer would fall within the article 26 derogation regime. Mechanisms such as Safe Harbour and the EU Standard Contractual Clauses did not fit the requirements for a worldwide compliance program which was to govern an organisation with a complex corporate structure. At the time the decision to apply for Binding Corporate Rules was made, no precedent had yet been set—although other large multinational companies were initiating similar exercises at around the same time—and the company found itself in previously unchartered waters. An interesting challenge lay ahead.

**Content of Binding Corporate Rules**
The thought behind the Binding Corporate Rules was for the applicant to show national data protection supervisors that they have a good quality global compliance regime in place, and for these data protection authorities to allow the applicant to transfer personal data globally. Of course the fact that a company has BCR in place does not mean that companies are suddenly able to transfer personal data freely. International data transfers must still be restricted to situations where there is a functional reason and need for it. Thus the national regulators set out what they thought a ‘good global compliance regime’ is and should be in WP74, drawing heavily on WP12 which deals with the general requirements for lawful transfers of personal data to third countries and the concept of “adequate protection”, setting out criteria for what constitutes a good data protection compliance regime.

Even before the Article 29 Working Party had released its Working Paper 74, the standard guidance document on the creation and implementation of BCR (at least until the release of more concise and comprehensive version in June 2008), Accenture had created a standard worldwide data privacy policy aimed at its employees and binding on all Accenture worldwide entities and employees. Areas where the processing of personal data and the rules stood to benefit from more in-depth analysis were identified (including IT, HR and Marketing) continue to be guided by supporting documents. Following the release of WP74 by the Article 29WP, a set of submission documents was prepared and submitted to the UK Information Commissioner’s Office in March 2006.

Until such time as the BCR were approved, Accenture relied and continues to rely on its global and binding Data Privacy Policy but also uses additional mechanisms to ensure the lawful sharing of personal data. For instance when joining Accenture, employees sign a consent form which is accompanied by a copy of Accenture’s Global Data Privacy Policy. In addition ad hoc consents prior to the use of certain systems such as the recruitment systems as well the necessity grounds mentioned in article 26 (1) have allowed Accenture to share personal data during its application phases.

On the basis of WP 74, an effective BCR program had to include certain components which were incorporated into the overall structure. The bindingness of the rules requires both a binding nature in law and a practical bindingness (compliance). In other words not only do applicants have to have procedures for redress in place so that the rules can actually be enforced against the organisation under the law, but they should also be binding on all the entities as part of a compliance program. In 2004, the International Chamber of Commerce released a report on Binding Corporate Rules in which it gives further insight into the requirements for BCR application content. In it, it reported the result of a survey about legal enforceability of BCR around the world. Responses came in countries within and outside Europe, including the US, Hong Kong and Japan. The result showed that the variety of principles would lead to legal enforceability and that BCR “are therefore a feasible way to provide a legal basis for data transfers in many jurisdictions around the world”. Interestingly the report found that all responses were in favour of making the BCR enforceable against subcontractors. However, as the report rightly points out, the subcontractors- at least in the vast majority of cases- act as data processors who cannot be bound by BCR as their obligations under the law are restricted to

---

4 ICC Report on Binding Corporate Rules for international transfers of personal data
providing adequate technical and organisational measures to protect personal data and following the processing instructions from the data controller. For these instances, the report foresees the Standard Contractual Clauses to remain the most efficient way of ensuring lawful cross border data transfers.

**Components of a successful BCR application**

One of the requirements laid down in WP 74 is for organisations to have a corporate structure which includes either a European Headquarters or a European entity which is tasked with delegated data protection responsibilities. Accenture did not fulfil this requirement as its corporate structure does not provide for one senior European entity and its compliance program was global in reach and enforcement. The Article 29 Working Party has since relaxed its position on this point as can be concluded from its subsequent release of guidance documents in June 2008\(^5\).

Another condition for a successful BCR application is to have transparent processes and procedures for the benefit of the data subjects in place such as the complaints procedure. Accenture accepted the comments made by the various regulators in respect of their opinion that the right of complaint was not sufficiently spelled out and thus included language in its local policy supplements to clarify the rights for individuals to lodge official complaints.

Furthermore, the data protection authorities also appeared to underline the need for a transparent structure outlining the details of the company’s liability, whereby the data subjects are clearly and specifically informed of their rights to compensation for any damage suffered as a result of the company’s breach of their rights in respect of processing their personal data. On the basis that Accenture does not have a European Headquarters or a European entity tasked with delegated data protection responsibilities, its solution was to place the same level of liability with the data exporter that the entity with delegated responsibilities would have had. This is achieved through a binding intercompany agreement which all Accenture entities are obliged to sign. Hence Accenture changed its BCR in order to accommodate the regulator’s requests for clarification.

In parallel, the US Sentencing Commission had already designed a guidance document back in the early nineties that was now becoming the new model for effective compliance programs for companies to implement, also referred to as the seven standards of an effective compliance program. The analysis detailed the different components of both regulatory documents. Accenture liked to draw analogies between both regulatory documents, enabling it to feel that policies and procedures were in line with internationally recognized compliance standards. Accenture’s Global Data Privacy Policy was scrutinized to check for having in place a governance structure and accountable personnel (in its BCR, this was achieved through the binding nature of the policies on entities and employees), provision of training and communication to the employees (during its BCR application, Accenture drew attention to its mandatory global computer based training on data privacy auditing facilities (existence of a program comprising regular company wide data privacy audits), delegation of authority (all countries having its own accountability for data privacy compliance through a binding agreement) and remedies for those who have suffered a damage (the possibility for data subjects to pursue remedies in the country of the origin of the transfer). Finally, both the

\(^5\) Working Document 153 of 24 June 2008 setting up a table with the elements and principles to be found in Binding Corporate Rules
seven standards and the European regulators demanded the implementation of enforcement practices and procedures which are clearly communicated to the employees. Accordingly Accenture found the content of the seven standards to be in line with the European guidance.

The BCR application process

The co-operation procedure involves appointing a “Lead Authority” who will first approve the BCR from its own national perspective before communicating to the other regulators the intention of the organisation to seek approval for a set of BCR. The Lead Authority is appointed on the basis that either the majority of an organization’s senior management resides in the country of choice, or the country houses the European Head Quarters of an organisation. Its task is to handle the communications with its colleague regulators in Europe and effectively act as a go-between with the applicant organisation. Of course what this means in practice is that every data protection regulator will have its own set of comments to send back to the applicant via the Lead Authority requesting the applicant to answer questions resulting in the applicant having to conduct multiple bilateral discussions either directly or by proxy, all via the Lead Authority.

Some delays in the process of application are inevitable. Some regulators may request changes to be made to the submission documents with different regulators requesting additional changes a few months down the line. Thus, the first regulator has to be re-consulted on those latter modifications, making the co-operation procedure lengthy and complicated when it involves a larger number of regulators, commenting comments at different points in time. Accenture’s application resulted in some comments from regulators on the point of liability but the company deemed it important not to respond straight away in case additional recommendations on the same point would be made by other regulators. The larger the size and presence of the applicant in question, the more complex and potentially extensive the co-operation phase can become.

Whilst regulators have a responsible position in the day to day representation of national privacy interests, often they are found to be understaffed and therefore proposed changes to the current working practices will certainly almost come down to the conclusion that more staff would be required to improve the co-operation procedure in order for stricter time lines to be set and with the Lead Authority being given a stronger role in the consolidation of comments and responses.

In June 2008, the Article 29WP adopted WP153, a new checklist for the BCR application process. On the back of this document, they adopted WP 154\(^6\), although the Working Party is careful to point out that the framework should not be used as a model set of BCR but rather as a guidance document to be adapted to the organisation, structure, the type of processing involved and the policies and procedures that they have in place. The checklist however has been found to be a useful document with regulators referring to this document in their assessment of the applicant’s eligibility to be granted BCR status. On the flipside of the coin, the assessment of an applicant’s BCR could be interpreted narrowly as a result of regulators taking a “checklist” approach, looking only for certain words and phrases which contradicts the original purpose of BCR namely to design a set of BCR according to an organisation’s own infrastructure and policies. For applicants already in the system, the adoption of the checklist could potentially lead to renewed scrutiny and previously held discussions between the applicant and the regulator.

\(^{6}\) Working Document 154 of 24 June 2008 setting up a framework for the structure of Binding Corporate Rules
may need to be revisited. However, it is clear that following the applications from organisations such as Accenture that there is more certainty in the assessment itself, and the points that they determine to be essential. The checklist appears to have incorporated those points into one document which will hopefully lead to more consistency, more certainty for applicants and regulators and therefore eventually resulting in a well oiled application process.

**Living the BCR**

Implementing a global policy within an organisation governed and supported by Binding Corporate Rules means all aspects of the business will sooner or later require privacy advice. To this effect, Accenture’s legal team employs a dedicated data privacy compliance team. Each new system, application and project involving personal data is built and implemented in accordance with Accenture’s Global Data Privacy Policy. Compliance steps such as providing fair processing notices, obtaining consent, access controls and requirements regarding relevance and adequacy of data are rolled out globally. Individuals exercise their rights globally with access requests originating in countries both within and outside the EU. Quite clearly continuous training and awareness raising are part of the compliance program and last year Accenture introduced a worldwide mandatory data privacy training for all employees as part of their required corporate training package with a booster lined up for its first anniversary.

**Conclusion**

Implementing and maintaining effective compliance programs is a must in a today’s competitive business society and with the heightened sensitivities around data security, companies are looking to have more robust privacy policies in place. For large multinational corporation BCR provide a global uniform compliance structure forgoing the continuous administration burden of Standard Contractual Clauses and ad hoc decisions regarding consent. The application process is one that must be streamlined overtime in order to encourage other companies to choose to go down the route of BCR. From Accenture’s point of view, the experience is and continues to be an interesting exercise of discussion with the European privacy watchdogs. Further challenges lay ahead when facing the reality of BCR in day to day corporate life. For now however Accenture continues its wave of application requests and expect that the creation of the checklist will give national data protection authorities a stimulant for providing timely, consistent and clear feedback on the proposed BCR in front of them.

**Anne Wilkes** is a Dutch lawyer who has worked in the UK for the past 8 years as in-house counsel for several large technology companies including PeopleSoft and Business Objects. Anne has worked at Accenture as EMEA privacy counsel for the past 2 years, as part of the legal team focussed on data privacy compliance in EMEA, which is a team in itself.

**Accenture** is a global management consulting, technology services and outsourcing company with currently over 17,000 employees in 49 countries.