Data protection briefing

First Data's binding corporate rules

Not for the faint-hearted?

On 14 November 2011, the Information Commissioner's Office (ICO) authorised the binding corporate rules (BCRs) of First Data Corporation, a leading electronic commerce and payment processing provider.

First Data is only the 11th company to obtain an authorisation since the ICO started granting authorisations for BCRs in 2005 (*see also News brief "Binding corporate rules: the answer to global data protection", www.practicallaw.com/3-369-8080*).

Protecting transfers of data

Under Article 25 of the Data Protection Directive (*94/46/EC*) (Article 25), personal data cannot be transferred outside the EEA unless adequate safeguards are in place. This is implemented in the UK by the eighth principle in Schedule 1 to the Data Protection Act 1998. In an increasingly globalised world, this restriction poses a significant problem for companies, especially those with a number of affiliates located outside the EEA (for example, in Asia or North America).

Several solutions exist. The European Commission (the Commission) has compiled a "white-list" of countries with laws that provide adequate protection for personal data that are transferred to them. However, so far only nine countries have made it onto the white-list (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey and Switzerland), so this is of limited application.

The most common solution is to enter into agreements based on the EU standard contractual clauses (the model clauses). These are standard agreements approved by the Commission as providing an adequate level of protection to enable companies to transfer personal data outside the EEA. They are suitable for use on an ad hoc basis, and especially where a small number of companies are involved.

However, model clauses are inflexible because they generally should not be amended, so are not suitable for companies that wish to take a specific approach to protecting data privacy. Also, in the context of large multinationals where companies may enter and exit the group frequently, they provide a potentially cumbersome structure.

What are BCRs?

Unlike the model clauses, BCRs are designed to provide a bespoke solution to enable international companies with affiliates in a number of different places to transfer personal data throughout the group. Effectively, BCRs establish a tailored and binding set of privacy principles for a group of companies. They are much more flexible than agreements based on the model clauses, because, if suitably implemented, companies can readily enter and exit the group without needing to amend the BCRs.

It should be noted that BCRs are only available for transfers between group companies, and not for transfers to third parties outside their group. If the BCRs are approved by the data protection (DP) authorities of the EEA countries from which data will be transferred, adequacy will be established and personal data can be transferred outside the EEA throughout the group.

But BCRs are not for the faint-hearted. They are a complex and resource-intensive undertaking, and gaining approval can take a significant amount of time. The BCR process is also in a continual state of change as the DP authorities work on streamlining the authorisation process and best practice. Consequently, it is likely that the requirements that a multinational is asked to satisfy will change during the course of its application. This makes timing especially hard to predict.

First Data's BCRs

First Data handles approximately 60 billion global transactions each year, providing electronic payment transaction processing and other services to more than 6.2 million merchant locations in 80 countries around the world. First Data's services enable consumers to pay by credit, debit or gift cards at these businesses. In addition, it serves over 2000 card issuers (banks and institutions who issue payment cards) across six continents, providing services to more than 700 million consumer card accounts.

Data protection is therefore of critical importance. In 2006, First Data developed a set of corporate privacy principles which were adopted throughout the company. Although it had already obtained a safe harbor certification for its employee data (a solution to the Article 25 restriction for transfers to the US only), and operated under a series of intra-group agreements based on

This article first appeared in the December 2011 issue of PLC Magazine.

the model clauses, First Data was looking for a more bespoke solution which reflected the primacy of data privacy within its business.

John Atkins, First Data's Chief Privacy Officer found that the safe harbor and model clause approach lacked flexibility and created a situation where: "although the business was living by its privacy principles, at the same time, for regulatory purposes, we were required to sign up to a set of standard generic commitments which did not reflect the true importance of data privacy within our business".

First Data was not put off by the fact that the BCRs were going to require a major commitment of time and resources to gain authorisation; nor that it would be taking a step into the unknown.

"At the time we decided to go for BCRs, only two companies had achieved BCR authorisation from the ICO," recalls Tanya Madison Cunningham, First Data's Senior Counsel, Technology, Regulatory Compliance and Privacy. "We knew they were highly experimental and that the regulators were still working out many of the details about how the authorisation process would work. However, given that we are a multinational corporation with a highly complex group structure, and that we had a strong desire to demonstrate our commitment to data privacy at First Data by being best in class, we chose to pursue BCRs."

The platinum standard

Under the BCR application process, DP authorities give enormous scrutiny not just to the BCRs themselves, but to the supporting data privacy infrastructure and policies. The combination of this level of regulatory diligence and the effort that organisations must go to in order to create their BCRs and have them approved means that BCRs provide the platinum standard for data privacy compliance for international organisations seeking to transfer personal data outside the EEA (*see box "Taking the plunge?"*).

Taking the plunge?

The flexibility and recognition of excellence that goes with binding corporate rules (BCRs) means that increasing numbers of companies are now looking at them as a serious alternative to the EU model clauses. However, before embarking on an application, companies need to remember that it is not just a matter of being able make it through a process leading up to authorisation that is likely to span several years: they will then need to live by the BCRs and give effect to the exacting standards of data protection which they require. Key considerations therefore include:

- Are BCRs right for the business? Because of the length of time taken, and resources required, for authorisation to be granted, an organisation should think twice before embarking on BCRs, unless there is a really compelling reason (for example, in terms of operational efficiency or commitment to data privacy) and the business is sufficiently international to justify the effort.

- Is the business ready? The project to create a set of BCRs is almost akin to writing a customised version of the Data Protection Directive (*95/46/EC*). This may be a significant regulatory burden for a non-EU company. BCRs require that they can be enforced both by individual data subjects and by the regulators, so in practice they must be more than a set of paper-based policies which are not adhered to.

- Does the business have the infrastructure to gain authorisation? In practice, this means a developed privacy office and network of privacy officers throughout the group, together with numerous policies to underpin the commitments made in the BCRs, including information security, training, audit, subject access, and internal and external complaints handling procedures.

This is recognised by the ICO, which commended First Data's commitment to the concept of BCRs, and said that it welcomed approaches from multinationals that want to use BCRs to share personal information within their own group, but outside Europe.

The first challenge for an organisation is to produce a set of BCRs which reflect its culture and practices, and, at the same time, afford a level of protection sufficient to enable the DP authorities to conclude that the BCRs provide adequate safeguards.

The Article 29 Working Group (comprising the DP authorities of EU member states) has specified the core requirements for BCRs and a sample BCR framework (*Working Papers (WPs) 153 and 154*). While emphasising that BCRs should be genuinely bespoke, DP authorities will nevertheless expect each and every requirement set out in these WPs to be satisfied (for example, compliance with core EU privacy principles such as transparency, fairness and security).

A host of supporting information must be provided with the BCRs themselves. Much of it is required in the BCR application form (WP 133), but DP authorities will also require information to satisfy themselves on various matters, including the shape and structure of the company's privacy office, that the BCRs are fully binding throughout the group, that third-party data subjects have real rights of remedy exercisable in the EU, and that there is training to ensure that the BCRs are understood throughout the organisation. In addition, DP authorities will need to see supporting policies; this could easily fill up a lever-arch file, or more.

Scott Singer is Head of Technology, Media and Telecoms Sector at SNR Denton UK LLP. First Data were assisted in their application for BCRs by SNR Denton's London office.

This article first appeared in the December 2011 issue of PLC Magazine.