An international summer: are binding corporate rules the way forward?

Date : October 2, 2015

This summer saw significant noise in relation to international transfers of personal data.

In July, the ICO at his annual report launch said that one of the changes to practice he expected to see post implementation of the EU Data Protection Regulation was that the ICO in the UK would have additional oversight over international transfers. Up until now, unlike some other member states, the UK has taken a relatively hands off approach to international transfers, perhaps resulting in a slightly blasé response from businesses from time to time. But that's set to change.

Then, in early September, the EU and US agreed an "Umbrella Agreement", which, once in force, is designed to guarantee a high level of protection of all personal data when transferred between law enforcement authorities across the Atlantic. It will in particular guarantee that all EU citizens have the right to enforce their data protection rights in US courts.

However, later in September, EU/US relations took a hit, when the Advocate General to the European Court of Judgement cast doubt on the validity of Safe Harbor. As we reported at the time, the Advocate-General concluded that national data protection regulators do have the power to undertake investigations into complaints which claim that a country doesn't ensure an adequate level of data protection, even where a European Commission opinion has set out otherwise. If they find that inadequate protection is provided, they can also suspending the contested personal data transfer and suspend data transfers.

But before all of this, back in May, the Article 29 Working Party was busily looking at the prospect of binding corporate rules for data processors, and revising their guidance from 2013. And it's clear that binding corporate rules are going to be given a lot more space in the new Data Protection Regulation. In fact, the fact that they are to be enshrined at all is a significant change in their status.

So what are binding corporate rules?

Binding corporate rules (BCR) are a means of ensuring that intra-group international transfers of personal data are adequately protected for the purposes of European data protection legislation.

They need to be approved in each member state you are exporting data from, although using a mutual recognition process, this requirement is greatly mitigated as powers are delegated to a lead authority (or authorities).

BCR are in essence intra-corporate global privacy policies, which enshrine good practice, processes and guidelines and satisfy EU standards.

While model contractual clauses are usually signed without the need for any particular implementation, BCRs go deeper, and require that you have a sufficiently robust internal data protection regime. This means their implementation will include policies, training, audit and all other pre-requisites for good corporate governance.

So who is doing it?

At the time of writing, 76 entities have managed to agree binding corporate rules, using 13 different lead data protection authorities, with the UK, France and the Netherlands the most commonly used. Some of these entities have approval for using their binding corporate rules when they are processing data, as well as when they are a controller.

It's clear that more than 76 entities transfer data out of Europe within their groups, so why the low take up? That's no so clear.

In some organisations, processes were put in place prior to the concept of binding corporate rules were fully

developed, and a complex structure of model contracts or safe harbour has been developed.

Anecdotally, there are many who continue to transfer data within their group informally, without any legal protections. The arguments behind this vary. In some, it is simply the case that it hadn't come to anyone's attention that this shouldn't happen – although they police their suppliers, internal transfers were not objectively considered. In others, it simply wasn't a high enough risk to require action.

But that's changing. Increased oversight, increased penalties for breach, and increased political scrutiny on international data transfers are now a given.

What are the advantages of BCR?

Binding corporate rules build on something your employees know and understand already – your corporate policies.

Building data protection into standard corporate compliance policies helps individuals grasp the concepts, rather than introducing model form agreements, or adherence to additional voluntary schemes.

They also send a message out to the world at large: we take data protection seriously, and we are happy to open our procedures up to scrutiny.

In addition, BCR for processors will allow organisations who process personal data on behalf of customers transfer their data to group entities who are, in effect, sub-processors of the data. At the moment, this is often a sticking point in outsourcing negotiations, where model term agreements may otherwise be required to be entered into between each sub-processor and the customer.

In this case, the BCR for Processors would be annexed to the data processing agreement, which must still contain all the normal data protection provisions. However, the addition of the BCR for processors would provide adequate safeguards for the data provided by the customer, allowing the customer to comply with applicable EU data protection law.

So what's the problem?

To begin with, implementing BCRs was costly and a very long process. But the length of approval time has been greatly reduced by the mutual recognition procedure, which allows companies to liaise with a lead authority, and with the growing experience of those authorities.

However, whilst the approval process can be more costly than implementing model terms in, for example, the UK, if you are also located in other member states where there are approval requirements for data transfer agreements, or the US and you are using Safe Harbor to gain compliance, you may find that this one-off cost can be largely offset.

Whilst you do also need to ensure that you don't exceed the scope of your authorisation, it is possible to vary your BCRs with the agreement of the lead Data Protection Authority, and the ongoing relationship your business will have with that Authority can in many cases be advantageous.

Conclusion

Binding corporate rules provide some significant advantages for businesses seeking to enhance corporate governance of information management. Whilst benefiting the organisation by allowing them to easily comply with European data protection rules, they also enshrine good practice within the organisation itself, and by their underlying implementation requirements.

In other words, BCR won't be put into a box until the next problem, or the next big outsourcing. They should become the life and soul of your information governance.

Gayle McFarlane and Jonathan Armstrong are lawyers with Cordery in London where their focus is on compliance issues.

Gayle McFarlane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com