

# BCR concepts – post-approval requirements and other challenges

2009 was an important year for BCRs, as the mutual recognition procedure matured and three more BCR applications were approved by the Information Commissioner, including the first under mutual recognition (Hyatt Hotels). By **Gary Brooks**.

Since 2003, the EU data protection authorities have made BCR one of their top priorities. The attraction of having a clear, yet flexible, data protection policy and being seen, through the adoption of BCR, to be a privacy-compliant and trustworthy organisation has prompted a number of multinationals to at least consider embarking on BCR programmes. One of the main attractions is the efficiency savings, since BCR enable personal information to be transferred internally on a global basis without having to enter into additional initiatives or project-based contracts on a country-by-country basis. BCR are, however, much more than just a mechanism for facilitating global data transfers. Since they provide a framework for a global compliance programme, enabling the organisation to achieve a higher level of compliance with all aspects of the national data protection laws in each EU country.

Whilst there will undoubtedly be a steady increase in the number of BCR approvals in 2010, the floodgates are not, however, going to open. The vast majority of multinationals and smaller global businesses will not be embarking on BCR programmes in 2010, despite the best efforts of regulators and lawyers to persuade them to do so, but will instead be relying on other means to legitimise their global transfers of personal data.

This article examines some of the reasons for the relatively poor uptake of BCR to date, and explores some of the problematic areas that are becoming evident, particularly in the post-BCR approval phase, as well as considering what needs to change in order for this important model to become more widely used.

## Post-BCR approval – permits for transfers

Let's imagine that your company has completed the EU level co-ordination process and obtained approval for its BCR from the lead authority and from all of the other relevant EU Member States under the mutual recognition procedure. That should be the end of the regulatory marathon and you should now be able to export data lawfully on the basis of your BCR.

However, in many EU jurisdictions, even after EU-wide approval for your BCR under the mutual recognition procedure has been obtained, you will still need to apply to the national data protection authority (DPA) for a permit allowing the transfer of data from that country on the basis of the BCR. This is because the rules on data exports in the relevant national data protection law require such a permit to be obtained before transfers can occur lawfully. This process of applying for an authorisation will often result in further questioning from, and dialogue with, the relevant DPA concerning the nature and extent of the data transfers from that country, together with analysis of the BCR documentation.

For example, in Italy, as part of a subsequent application for a national permit legitimising data transfers, the Italian DPA will typically require additional information (above and beyond what is contained in the approved BCR) concerning the nature and purposes of the processing operations, the types of cross-border transfer for personal data collected in Italy and the data security measures in place, before a decision will be made as to whether the permit will be granted.

Similarly, in the Netherlands, an application for a permit has to be made for each type of transfer (for example employee data or customer data) to the

Dutch DPA comprising a completed application form, a copy of the BCR and a covering letter requesting permit on the basis of BCR.

The precise requirements for obtaining the national authorisation differ in each country. The countries requiring further administrative steps to be taken post-BCR approval include Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Greece, Italy, Latvia, Netherlands, Poland, Romania, Slovakia, Slovenia, Spain and Sweden. The timeframe for obtaining each of these authorisations is typically months rather than weeks. Given the number of countries involved and the differing requirements, the process of obtaining these authorisations is resulting in a significant legal and administrative burden for those companies that have successfully adopted BCR.

Other DPAs adopt a more pragmatic approach. The UK, Germany, Denmark, Hungary and Ireland do not require any further administrative steps to be taken once the BCR have been approved under the mutual recognition procedure.

There is at present no EU-wide guidance or publication from the Article 29 Data Protection Working Party summarising the relevant national requirements post-BCR approval, rather it is up to the data controller to approach each relevant DPA and establish what the particular requirements are for obtaining an authorisation for global transfers from that jurisdiction on the basis of the BCR.

Indeed, it is not clear in some countries what the process actually is for obtaining authorisations for international transfers on the basis of an approved BCR scheme, and some of the DPAs (for example the CNIL in France) are in the process of consid-

ering how to address this issue at present.

This issue needs to be urgently addressed by both the DPAs and the Article 29 Working Party, since it undermines the harmonisation efforts at the EU level (such as mutual recognition) and is not beneficial to BCR becoming a successful and widely used tool for cross border data transfer. After all, one of the main arguments for

question of how to make BCRs binding on an intricate web of group companies (and how to apportion intra-group liability for breaches of the BCR) is one that is particularly challenging in practice, and some multinationals will find that their own internal culture is not aligned with the BCR approach.

BCR cannot therefore be viewed simply as a standalone project, but rather it is a way of operating and

compliance, and this is precisely why more should be done to make them more attractive to both multinationals and smaller companies.

It is of note that initial efforts are being made by privacy practitioners and advocates to extend the concept of BCR to transfers to data processors, (so-called Binding Safe Processor Rules) which would be a very welcome development, given that the practice of transferring personal data outside the company to a third party processor typically presents greater risks to the privacy of individuals' personal information.

---

“...the requirements in many national laws to obtain a permit for data transfers (post-BCR approval) undermines the BCR concept”.

---

adopting BCR to deal with global data transfers (as opposed to EU model contracts) is that it is meant to provide greater efficiency and reduce bureaucracy, as a single harmonised solution.

### **Making BCR attractive to smaller global businesses**

BCR are still largely the preserve of large multinationals at present. The vast majority of businesses in the UK are not multinationals, yet with the Internet and technology facilitating global data flows for all sizes of organisations, there is a need for a solution to the international transfers restriction which is affordable and realistic for smaller businesses with a global presence.

Adopting BCR is a serious commitment, involving significant financial and human resources, and yet the commercial realities are often not fully appreciated. It is at least a 12 month process from start to approval, and indeed the process of achieving full compliance with national laws typically takes considerably longer than that when all the above-mentioned post-approval requirements are taken into account. Ongoing post-BCR approval commitments include implementing internal audit controls and supervision, as well as complaints handling processes.

In addition, the complexity of the legal and commercial issues involved in preparing a BCR application is not to be underestimated. For example, the

behaving that involves embedding good data protection practice at the heart of the organisation's culture and corporate governance. The majority of smaller global businesses simply do not have the internal commitment or resources to engage in such a complex process, particularly where it involves producing customised policies and opening up both existing and BCR-specific policies and procedures to very detailed scrutiny by EU regulators.

The area of intra-group international transfers is relatively “low risk” in data protection terms, and there has not been much enforcement action taken by DPAs for breaching the rules on cross-border transfers. Whilst there are undoubtedly huge benefits for those companies that successfully adopt BCR, many organisations will instead continue to channel their limited resources into ensuring compliance with aspects of data protection that carry more immediate and greater risk, for example transfers of data outside the company to data processors and ensuring that the security measures employed by the processor are adequate. Most global organisations will therefore continue to rely on a combination of model contracts and other less expensive methods in order to comply with the 8th principle in the UK's Data Protection Act.

Of course, BCRs are so much more than just a tool for facilitating transfers since they operate to improve all aspects of a company's data protection

### **Conclusions and commentary**

One of the main reasons for the relatively poor uptake of BCR is that despite recent advancements, the application process is still excessively lengthy, bureaucratic and expensive, and is far from being streamlined, even under the mutual recognition procedure.

The lack of a harmonised approach by the various national DPAs causes difficulties in practice and, in particular, the requirements in many national laws to obtain a permit for data transfers (post-BCR approval) undermines the BCR concept. This problem is then being exacerbated by a lack of resources within some DPAs, which causes delays in analysing BCR applications, particularly amongst those countries that currently sit outside the mutual recognition procedure.

More generally, this problem of having to comply with excessive and divergent administrative requirements in many EU Member States is threatening the effectiveness of both BCR and the EU model contracts and is placing a disproportionate burden on those data controllers who are trying to “get it right”. DPAs ought to be aiming to authorise data transfers on the basis of the approved BCR as a matter of course (without imposing further administrative requirements), or where this is not possible under their national laws, at least produce a BCR-specific process for national authorisations which is as streamlined as possible.

The more pragmatic approach to assessing adequacy that is practised by the UK and Irish DPAs should become the benchmark for other EU DPAs, so that the regulators' resources are

focussed on real areas of data protection risk that are likely to cause harm to individuals, rather than requiring companies to spend an excessive amount of time listing data types and describing data flows in order to meet the formalities of “paper” regulatory compliance, when in practical terms the compliance framework and binding mechanisms (in the form of approved BCR or signed model contracts) are already in place, providing adequate protection for the privacy rights of

individuals.

Mutual recognition and recent Article 29 Working Party documents have undoubtedly helped the process of drafting, adopting and implementing BCR. Yet it is still undoubtedly very complex, onerous and expensive, particularly for smaller global businesses that typically lack the resources and the commitment to implement a BCR programme, when there are more pressing areas of data protection risk to be chosen as the target for their limited

budgets. If the Article 29 Working Party see BCR as the flagship data protection standard, then they have to do more to make it a more realistic and cost-effective option for smaller organisations with a global presence, or else produce alternative mechanisms which address these concerns.

### AUTHOR

Gary Brooks is a solicitor and a PL&B Consultant

# Your Newsletter Subscription Includes

# e-Newsletter

## 1. Six newsletters a year

The *Privacy Laws & Business (PL&B) United Kingdom Newsletter's* scope ranges beyond the Data Protection Act to include the Freedom of Information Act, related aspects of the Human Rights Act and the Regulation of Investigatory Powers Act. It also covers Jersey, Guernsey and the Isle of Man. The newsletter complements the *International Newsletter*, which has been the leading data protection and privacy publication for 23 years.

## 2. Email updates

We will keep you frequently informed of the latest privacy developments.

## 3. Country, Subject, Company Index

Subscribers will receive annually a cumulative subject index of all topics covered. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website [www.privacylaws.com](http://www.privacylaws.com).

## Electronic Option

The newsletter is available in PDF format either for use in one office or for uploading onto your intranet or network. This format enables you to see the newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Please contact the *Privacy Laws & Business* office for more information.

*Privacy Laws & Business has clients in over 45 countries, including the UK Top Ten, eight of the Global Top Ten and seven of Europe's Top Ten in the Financial Times lists; and 10 of the US Top 20 in the Fortune list; and 70% of the top 20 law firms in the London and UK Legal 500 lists.*

# Newsletter Subscription Form

## Subscription Packages

(Please add 17.5% VAT to prices for the PDF format within the EU)

- Print  PDF (please tick preferred delivery format)
- Send a FREE sample of the *UK/International Newsletter*
- PL&B UK* Subscription **£285**
- UK/International Newsletter* Combined Subscription **£595** or an extra **£220** for existing International newsletter subscribers
- Special academic rate – 50% discount on above prices

## Multiple Subscription Discounts

- 2-9 copies: 30% discount (indicate no. of copies .....)

## Intranet Enterprise Licence for uploading onto your network (including additional printed copies)

- PL&B UK* **£1,425**
- PL&B International* **£1,875**
- Both *International/UK Newsletters* **£2,975**
- I wish to receive *PL&B's* FREE email news service

**Data Protection Notice:** *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to be contacted by:  Post  Email  Telephone

Name: .....

Position: .....

Organisation: .....

Address: .....

Postcode: ..... Country: .....

Tel: .....

Email: .....

Signature: .....

Date: .....

## Payment Options

Address of Accounts (if different): .....

Postcode: .....

Purchase Order

Cheque payable to: *Privacy Laws & Business*

Bank transfer direct to our account:  
*Privacy Laws & Business*, Barclays Bank PLC,  
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.  
Bank sort code: 20-37-16 Account No.: 20240664  
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22  
*Please send a copy of the transfer order with this form.*

American Express  MasterCard  Visa

Card Name: .....

Credit Card Number: .....

Expiry Date: .....

Signature: ..... Date: .....

### I am interested in:

- Consultancy/Audits
- In-House Presentations/Training
- Recruitment Service

*Please return to:* Newsletter Subscriptions Department,  
*Privacy Laws & Business*, 2nd Floor, Monument House, 215 Marsh  
Road, Pinner, Middlesex HA5 5NE, UK. Tel: +44 (0)20 8868 9200  
Fax: +44 (0)20 8868 5215, email: [info@privacylaws.com](mailto:info@privacylaws.com)  
web: [www.privacylaws.com](http://www.privacylaws.com) 2/2

**[www.privacylaws.com](http://www.privacylaws.com)**

## Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.