



Binding Corporate Rules Frequently Asked Questions

1 What are Binding Corporate Rules (BCRs) designed to achieve?

BCR, are designed to allow multinational companies to transfer personal data from the EEA to their affiliates located outside of the EEA in compliance with the 8th data protection principle and Article 25 of Directive 95/46/EC (the "Directive").

Applicants must demonstrate that their BCRs put in place adequate safeguards for the protection of personal data throughout the organisation in line with the requirements of the Working Party paper on Binding Corporate Rules, known as WP 74 (www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm).

2 What is the procedure for authorising BCRs?

The procedure is designed to avoid the applicant company having to approach each individual DPA separately.

The applicant organisation chooses a Data Protection Authority ("DPA") to be a lead authority. The choice of lead authority depends on the location of the EU headquarters of the applicant company or the location within Europe of that part of the company best placed to take responsibility for global data protection compliance. Detailed criteria as to choice of lead authority are set out in Working Party papers 107 and 108 (www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm).

If the lead authority is satisfied as to the adequacy of the safeguards put in place in the BCRs, that authority circulates the draft BCRs to the other DPAs in Europe from which the applicant requires an authorisation. The lead DPA communicates any comments received to the applicant. The role of the lead DPA is to facilitate the authorisation process.

When submitting an application, companies should use Working Party paper 133, which is an application form based on WP 108, or they can put together their own application. We and other DPA strongly recommend that applicants use WP 133 (www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm).

It is important to note that BCRs do not provide a basis for transfers made outside the group.

3 What are the benefits of BCRs compared with other means of putting in place adequate safeguards to satisfy the 8th Data Protection Principle?

The main advantage of BCRs over other means of providing adequate safeguards is that, once developed and operational, BCRs can provide a framework for a variety of intra-group transfers to meet the requirements of the organisation. The ongoing obligation of a company which has received an authorisation for its BCRs will be to monitor its compliance to make sure that it is operating within the scope of the authorisation. This will include regular audits and a requirement to maintain a training programme for staff handling personal data.

The BCRs should also help the company to address privacy concerns and raise awareness of data protection within the organisation. This is because in the process of putting together an application an organisation has to consider the personal data that it transfers outside the EEA to other members of the same group and how staff are made aware of and respect the requirements of the Directive. An essential part of the authorisation process is the requirement for the applicant to demonstrate how staff in affiliates in third countries are made aware of the implications of processing personal data transferred from the EEA for example, through its staff training programmes.

Provided that the BCRs are drafted widely enough, they should be able to accommodate changes in the company structure and some variation in the types of data flow. Changes within the company which do not affect the authorisation do not need to be notified to the DPAs which have given authorisations. BCRs therefore allow for significant flexibility.

More substantial changes in the organisation which go beyond the scope of the authorisation will result in the company having to obtain a revised authorisation for all or part of its processing.

Another solution available to multinationals as a means of putting in place adequate safeguards is the use of the model contract clauses authorised by the European Commission. However, there are drawbacks with the use of contracts, particularly in multinational companies with complex structures, because sometimes hundreds of contracts are required to cover transfers between all affiliates. The task of making sure that contracts are kept up to date to keep pace with the changing corporate structure can also be difficult and time consuming.

The extent to which individual DPAs will permit the adaptation of the model contracts to allow for multi-party as opposed to bilateral arrangements also varies from one DPA to another limiting the scope for companies to reduce the number of contracts required. There are also situations in which model contracts cannot be used, for example, where the organisation is only one legal entity.

Despite the fact that the model clauses have been approved for use by the European Commission, in some countries there is still a requirement for exporting data controllers to go through a form of authorisation process which can also be time consuming.

Another option open to data controllers is the Safe Harbor scheme, but this is limited to transfers to the US and also does not include certain sectors, such as financial services.

In the UK, the 8th data protection principle allows for data controllers to make their own assessment of adequacy but this, of course, is of limited use to a multinational company that also transfers personal data from other parts of the EEA. The ICO has produced guidance to assist data controllers to make adequacy assessments (www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers).

4 Do other DPAs support the concept of BCRs?

A number of DPAs are actively engaged in promoting BCRs and over time we anticipate that this number will continue to grow.

WP 74 makes it clear that DPAs are free to deal with applications for authorisations in the manner which best fits with their national laws and acknowledges that in some countries the DPAs may lack sufficient resource to deal with such applications. Lack of resource within DPAs is one reason for delays in the authorisation process.

An issue which was mentioned in WP 74 and which has proved to be a problem in practice is that in some Member States the national law does not allow for the concept of unilateral declarations. This is the basis on which some applications are structured to address the way in which the BCRs are binding throughout the group. In these cases, the applicant may have to find another solution which is enforceable under the laws of the Member State in question to deal with this requirement. This is the sort of issue which will have been discussed with the lead DPA before an application is circulated under the co-operation procedure.

In time we foresee that more and more DPAs will become actively engaged in the process but there may be a few which, because of difficulties with their national laws, cannot. At the present time, therefore, BCRs are not the pan-European solution it was hoped they would be.

5 How many applications for authorisation has the Information Commissioner received?

We receive regular queries from companies interested in using BCRs and the number of applications is likely to increase if companies have confidence that the authorisation process is becoming more streamlined, and that there is a realistic prospect of an application being successful.

6 How long does it take to process an application?

One issue that makes companies reluctant to initiate an application is the length of time that the authorisation process is likely to take. We and other DPAs are aware of these concerns and we are working on ways in which to streamline the process.

While we may be able to deal with an application relatively quickly within the ICO, we cannot guarantee that there will not be delays in the authorisation process within other DPAs once an application is launched under the co-operation procedure. At the

moment we are saying that, realistically, from the start of the co-operation procedure, a straightforward application could take 12 months to conclude.

The co-operation procedure (WP 107) does give some timescales within which applications have to be processed but it is often the case that there is some slippage. The ability of the company to react to comments from the DPA and amend documentation will also be a factor.

Using the model application form authorised by the Article 29 Working Party (WP 133) and ensuring you have all of the elements specified in WP153 should also help to speed up the process (see 7 below). We strongly recommend using the model application form.

The time involved in circulating an application under WP 107 also has to be weighed against the time (and cost) incurred by companies having to approach DPAs individually and obtaining authorisations for their transfers.

One positive initiative, which some DPAs have welcomed and the ICO supports, is mutual recognition. Under mutual recognition if the lead authority is satisfied that the BCRs put in place adequate safeguards, other participating DPAs should have confidence in their decision and accept their findings without any further scrutiny or comment. The mutual recognition system is currently under development.

7 How should an application be structured?

The model checklist (WP 108) sets out the requirements for submitting a set of BCRs. These requirements have now been incorporated into WP 133.

WP 133 should help both applicants and DPAs in the authorisation process. The standardisation of the application should give some comfort to applicants that the information they are providing is in line with the requirements of WP 74 and should in turn facilitate the authorisation procedure for DPAs.

While there is no obligation on applicants to use the template application form, as it is intended to help applicants demonstrate to DPAs how they meet the requirements of WP 74 and WP 108, we are of the view that most applicants will wish to use it.

Applicants will have to have all of the elements specified in table of BCR requirements (WP153) in one or more documents which make up the rules and should also refer to the Article 29 working party FAQs (WP 155) which addresses liability and other issues requiring a common interpretation.

The Article 29 working party has produced a BCR framework (WP 154) which illustrates what all the requirements of WP 74 and WP 108 might look like in a single document. Applicants are free to base their BCR on this framework but it is not a requirement.

WP 153, WP 154 and WP155 are available from the European Commission's website (www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm).

8 What about the administrative requirements of many of the Member States? How do these fit in with the authorisation of BCRs?

In the UK an authorisation is given on the basis that the BCRs satisfy the requirements of WP74 in that they provide adequate safeguards within the meaning of Article 26(2) of the Directive. This provides the basis for the authorisation under paragraph 9 of Schedule 4 to the Data Protection Act 1998. Provided that the processing, including the transfer of personal data, is notified to the Information Commissioner, there are no other steps that are required before an applicant company may transfer personal data intra-group on the basis of the authorisation.

In many Member States, however, the DPA has to grant a permit allowing the transfer of data from that Member State to a third country or countries in addition to the authorisation of the BCRs.

This may be seen to defeat the object of the co-operation procedure and the underlying principle of WP 74, but where the national law provides that such permits are required there is nothing that can be done.

9 How does the Information Commissioner handle requests for information relating to BCRs under the Freedom of Information Act 2000?

As the concept of BCR is relatively new, there has been a great deal of interest in the applications we have already dealt with from other companies and their advisors who are interested in putting together an application. As a result, we have received a number of FOI requests for copies of documents.

Organisations seeking authorisation for their BCRs will be treated in the same way as any other data controller seeking compliance advice from the ICO. This means that we cannot disclose the fact that an organisation has approached us with an application without its consent or unless the information has been put into the public domain. Once an authorisation is made, however, this is a matter of public record. Applicants are notified accordingly and authorisations are put on the ICO website.

Some organisations put some of the content of their BCRs into the public domain via their websites (for example, the privacy policy or data protection code) and this obviously helps us deal with an FOI request. However, an application is likely to comprise a substantial amount of commercially confidential information which is not likely to be in the public domain. Such information will be treated in the same way as any other confidential information received by the Information Commissioner as part of his statutory functions.

More information:

If you need any more information about this or any other aspect of data protection, please contact us.

Head Office

Phone: 01625 545 745 or 08456 306 060

Notification helpline: 01625 545 740

E-mail: please use the online enquiry form on our website

Website: www.ico.gov.uk