



1271-04-02/08/EN
WP 155 rev.04

**Working Document on Frequently Asked Questions (FAQs) related to
Binding Corporate Rules**

Adopted on 24 June 2008
As last Revised and adopted on 8 April 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/06.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

FAQs on Binding Corporate Rules (BCR)

As explained in Working Paper 74 (WP 74)¹, the Article 29 working party considers that BCRs are an appropriate solution for multinational companies and other such groups to meet their legal obligations and ensure a proper level of protection of personal information when transferring data out of the European Union.

The working party/Data Protection Authorities have published these FAQs in light of their experience of the applications made for approval of BCRs and enquiries received about the interpretation of documents WP 74² and WP 108³. The FAQs are intended to clarify particular requirements for applicants in order to assist them in gaining approval for their BCRs.

These FAQs are not exhaustive and will be updated as required.

1 – Do the BCRs have to apply to all the personal data processed by the group?

No, BCRs are a legal means for providing adequate protection to personal data which is covered by Directive 95/46/EC and transferred out of the European Union to countries that are not considered to provide an adequate level of protection. Other personal data processed by the group, which is not processed at some point in the EU, does not have to be covered by the rules.

However, it is strongly recommended that multinational groups using BCRs have a single set of global policies or rules in place to protect all the personal data that they process. Having a single set of rules will create a simpler and more effective system which will be easier for staff to implement and for data subjects to understand. Companies are likely to be respected for demonstrating a firm commitment to a high level of privacy for all data subjects regardless of their location and the legal requirements in any particular jurisdiction.

It should be noted that it is possible for the group to have a single set of rules while at the same time limiting the third party beneficiary rights required in the BCRs only to personal data transferred from the European Union.

2 –Do the BCRs have to apply to data processors who are not part of the group?

No, only processors who are part of the group and are processing data on behalf of other members of the group will have to respect the BCRs as a member of the group. The BCRs could contain particular rules dedicated to members of the group acting as processors as a means of meeting the requirements of Articles 16 and 17 of Directive 95/46/EC.

¹ Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

² See footnote 1

³ Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on April 14, 2005 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

Processors who are not part of the group and act on behalf of a group member are not required to be bound by the BCR. However, those processors should always only act under the instructions of the controller and should be bound by contract or other legal act in line with the provisions of the Articles 16 and 17 of the EU Directive.

If the processors are not part of the group and are based outside of the EU, the members of the group will also have to comply with the Articles 25 and 26 of Directive 95/46/EC on transborder data flows and ensure an adequate level of protection. For instance, the company can seek to adduce adequacy by contractual means such as by making use of the Standard Contractual Clauses adopted by the EU Commission for transfers to a processor outside of the EU or by subjecting the processors to the BCRs' provisions in respect of their data.

The BCRs will need to address these situations.

3 – Where a breach of the BCR occurs outside the EU which member of the group is liable?

Regardless of the existence of any liability under Directive 95/46/EC for the entity that exports personal data from the EU, the BCRs themselves must nominate an entity within the EU who accepts liability for any breaches of the rules by any member of the group outside of the EU. This liability only needs to extend to data transferred from the EU under the rules.

WP74 envisaged that in most cases it would be the headquarters of the group, if EU based, that would accept liability. Where the headquarters of the group is based outside of the EU, WP74 allowed the group to nominate a suitable member in the EU who would accept liability for breaches of the rules outside of the EU. This responsibility includes, but is not limited to, the payment for any damages resulting from the violation of the binding corporate rules by any member outside of the EU bound by the rules.

However, for some groups with particular corporate structures, it is not always possible to impose to a specific entity to take all the responsibility for any breach of BCRs out of the EU. In these cases, the working party accepts that where the group can demonstrate why it is not possible for them to nominate a single entity in the EU they can propose other mechanisms of liability that better fit the organization.

One possibility would be to create a joint liability mechanism between the data importers and the data exporters as seen in the EU Standard Contractual Clauses 2001/497/EC dated June 15, 2001 or to define an alternative liability scheme based on due diligence obligations as prescribed in the EU Standard Contractual Clauses 2004/915/EC dated December 27, 2004. A last possibility, specifically dedicated to transfers made from controllers to processors is the application of the liability mechanism of the Standard Contractual Clauses 2002/16/EC dated December 27, 2001.

Data protection authorities may accept those alternative solutions mentioned above to liability on a case-by-case basis where sufficient and adequate comfort is provided by the applicant. Where any alternative mechanism is used it is important to show that the data subjects will be assisted in exercising their rights and not disadvantaged or unduly inhibited in any way.

4 – Should the BCR always contain a right for the data subject to lodge a complaint before the data protection authority for violation of the BCR?

Yes, despite the fact that in some cases the rules or the third party beneficiary rights in particular may have been limited to data originating from the EU and individuals already have a right in their national law to make a complaint about the exporting entity to the data protection authority it is important to have a right to lodge a complaint on the face of the BCRs for a breach of the rules as a whole by any member of the group.

5 – Should information about third party beneficiary rights be made readily available to the data subjects that benefit from it?

Yes, WP74 requires that both the BCRs and the ways to complain and seek a remedy for a breach of the rules should be easily accessible for the data subject. The existence of third party beneficiary rights and their content is an important option for a data subject when considering what remedies are available to them. Some companies have decided for legitimate reasons not to include the third party beneficiary rights clause in the core document of the BCRs but instead set the rights out in a separate document. In those cases where the rights are in a separate document they should be made transparent and easily accessible to any data subject benefiting from those rights.

6 - Do the BCR themselves have to describe the processing and transfers of personal data within the group and in what level of detail?

Yes, a general description of the main purposes of processing and types of data transfers will need to be included in the BCR.

For example, the group can explain in its BCR that transfers are made to all entities of the group for staff mobility reasons, that HR data are sent to the main data centres of the group in Germany, US and Singapore for storage and archiving, that HR data are sent to the headquarters to define global compensation strategy and benefits planning for the group.

However, when applying for national authorisation and permit requirements, some Member States may require applicants to list the individual transfers that will take place from their jurisdiction to third countries into national filing documents.

7 - Should the BCRs be set out in a single document that creates all obligations of the group and the rights of individuals?

It would greatly facilitate the review of BCRs by Data Protection Authorities and at the same time make BCRs more transparent for data subjects if there was one document showing clearly all obligations and rights which, if necessary, should be complemented by additional and relevant documentation (e.g. policies, guidelines, audit/training programmes). This structure is proposed as an example in the WP.154 adopted in June 24, 2008 providing a framework for BCRs. Although it is not obligatory to have BCRs in a single document.

8 – What terminology should applicants use for drafting their BCR?

As BCR are a tool, with internal and external legal effects, that provide a level of data protection which is adequate under the EU Directive 95/46/EC, the wording and definitions of the BCR key principles (as listed in WP.74, WP.108, WP.153 and WP.154) should be consistent with the wording and definitions of the EU Directive.

This avoids misinterpretation of the BCR and assists when seeking authorisation from a Data Protection Authority as they are easily understood.

This does not prevent companies from using different language – with the same meaning, however – if this is easier for the staff and for client to understand when implementing the BCR into group policies or internal guidelines.

9 – What rights should an individual have under the third party beneficiary rights clause?

An individual whose personal data are processed under the BCR can enforce the following BCR principles as rights before the appropriate data protection authority or court according to the rules defined by the WP. 74, WP. 108, and WP153, in order to seek remedy and obtain compensation if a member of the group has not met the obligations and does not respect those principles.

More specifically, the principles which are enforceable as third party beneficiary rights are as follows:

- Purpose limitation (WP 153 Section 6.1, WP 154 Section 3),
- Data quality and proportionality (WP 153 Section 6.1, WP 154 Section 4),
- Criteria for making the processing legitimate (WP 154 Sections 5 and 6),
- Transparency and easy access to BCR (WP 153 Section 6.1, Section 1.7, WP 154 Section 7),
- Rights of access, rectification, erasure, blocking of data and object to the processing (WP 153 Section 6.1, WP 154 Section 8),
- Rights in case automated individual decisions are taken (WP 154 Section 9)
- Security and confidentiality (WP 153 Section 6.1, WP 154 Sections 10 and 11),
- Restrictions on onward transfers outside of the group of companies (WP 153 Section 6.1, WP 154 Section 12),
- National legislation preventing respect of BCR (WP 153 Section 6.3, WP 154 Section 16),
- Right to complain through the internal complaint mechanism of the companies (WP 153 Section 2.2, WP 154 Section 17),
- Cooperation duties with Data Protection Authority (WP. 153 Section 3.1, WP 154 Section 20),
- Liability and jurisdiction provisions (WP. 153 Section 1.3, 1.4 , WP 154 Sections 18 and 19),

Companies should ensure that all those rights are covered by the third party beneficiary clause of their BCR by, for example, making a reference to the clauses/sections/parts of their BCR where these rights are regulated in or by listing them all in the said third party beneficiary clause.

These rights do not extend to those elements of the BCR pertaining to internal mechanisms implemented within entities such as detail of training, audit programmes, compliance network, and mechanism for updating of the rules. [WP153 Section 2.1, 2.3, 2.4 and 5.1, WP.154 Sections 13 to 15 included and Section 21]

10 – What is the relationship between EEA data protection laws and BCRs?

BCRs do not substitute EEA national data protection laws, applying to the processing of personal data in EEA Member States. Although BCRs shall provide adequate safeguards for the transfers of personal data, they should not be considered as an instrument to replace EEA data protection laws. Indeed, an authorization given by an EEA Member State under Article 26 (2) of Directive 95/46/EC exclusively addresses international transfers from an EEA Member State to third countries and does therefore not certify that the processing activities taking place in the EEA are compliant with EEA national data protection laws.

11 – What does the reversal of the burden of proof mean in practice?

Where data subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCR, it will be for the member of the group in Europe that accepted liability to prove that the member of the corporate group outside of Europe was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place.

Done at Brussels, on 24/06/2008

*For the Working Party
The Chairman
Alex TÜRK*

As last revised and adopted on
08/04/2009

*For the Working Party
The Chairman
Alex TÜRK*