



1271-00-00/08/EN
WP 153

Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules

Adopted on 24 June 2008

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 06/80.

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

INTRODUCTION

In order to facilitate the use of Binding Corporate Rules (BCRs) by a corporate group for its international transfers from the EU to organisations within the same corporate group, the Article 29 Working Party has created the following table:

- clarifying the necessary content of BCRs as stated separately in documents WP 74¹ & WP 108²,
- making the distinction between what must be included in BCRs and what must be presented to Data Protection Authorities in the BCRs application (document WP 133³),
- giving per principle the corresponding text references in documents WP 74⁴ and WP 108⁵ for further details, and
- providing explanations/comments on the principles one by one.

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 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

³ Working Document WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

⁴ See footnote 1

⁵ See footnote 2

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
1 - BINDING NATURE				
INTERNALLY				
1.1 The duty to respect the BCRs	YES	YES	WP74 point 3.3.1 (pages 10-11) + WP 108 point 5.3 to 5.9 (page 5)	The BCRs must contain a clear duty for all the members of the Group and for the employees to respect the BCRs.
1.2 An explanation of how the rules are made binding on the members of the group and also the employees	NO	YES	WP74 point 3.3.1 (pages 10-11) + WP 108 point 5.3 to 5.9 (page 5)	<p>The Group will have to explain in its application form how the rules are made binding :</p> <p>i) Between the companies/entities in the group by one or more of: Intra-group agreement, Unilateral undertakings, Internal regulatory measures, Policies of the group, or Other means</p> <p>ii) On employees by one or more of: Individual and separate agreement/undertaking with sanctions , Clause in employment contract with sanctions, Internal policies with sanctions, or Collective agreements with sanctions</p>
EXTERNALLY				
1.3 The creation of third-party beneficiary rights for data subjects, including the possibility to lodge a complaint before the competent Data Protection Authorities and before the courts (choice of jurisdiction between court of data exporter/ EU headquarters/EU member with delegated data protection responsibilities)	YES	YES	WP 74 point 3.3.2. (pages 11-13), point 5.5.1. (page 18) and point 5.6 (page 19) + WP108 points 5.12 to 5.14, point 5.16, point 5.20 (page 6)	The BCRs must grant rights to data subjects to enforce the rules as third-party beneficiaries. The rights should cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation (see articles 22 and 23 of the EU Directive).

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
<p>1.4 The company accepts liability for paying compensation and to remedy breaches of the BCR.</p>	YES	YES	<p>WP 74 point 3.3.1, § 5-6 (page 11), point 5.5.1 (page 18), point 5.5.2 (pages 18-19), point 5.6 (page 19) + WP108 point 5.17 (page 6)</p>	<p>The BCRs must contain a duty for the EU headquarters, or the EU Member with delegated responsibilities to accept responsibility for and to agree to take the necessary action to remedy the acts of other members linked by the BCRs outside of the EU and to pay compensation for any damages resulting from the violation of the BCRs by members of the BCRs.</p> <p>The BCRs must also state that, if a member of the group outside the EU violates the BCRs, the courts or other competent authorities in the EU will have jurisdiction and the data subject will have the rights and remedies against the member that has accepted liability as if the violation had taken place by them in the member state in which they are based instead of the member of the group outside the EU.</p> <p>If this is not possible for some groups with particular corporate structures to impose to a specific entity to take all the responsibility for any breach of BCRs out of the EU, DPAs might accept other liability mechanisms on a case-by-case basis if sufficient comfort is brought that data subjects rights will be enforceable and they will not be disadvantaged in enforcing them. Such possible liability schemes would be the 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 the 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.</p>
<p>1.5 The company has sufficient assets.</p>	NO	YES	<p>WP 74 point 5.5.2. §2 (page 18) + WP108 point 5.17. (page 6)</p>	<p>The application form must contain a confirmation that the entity that has accepted liability for the acts of other members linked by the BCRs outside of the EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.</p>

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
1.6 The burden of proof lies with the company not the individual.	YES	YES	WP 74 point 5.5.2. § 6 and 7 (page 19) + WP108 point 5.19 (page 6)	<p>BCRs must state that the entity that has accepted liability will also have the burden of proof for demonstrating that the member of the group outside the EU is not liable for any violation of the rules which has resulted in the data subject claiming damages.</p> <p>If the entity that has accepted liability can prove that the member of the group outside the EU is not responsible for the act, it may discharge itself from any responsibility.</p>
1.7 There is easy access to BCRs for data subjects and in particular easy access to the information about third party beneficiary rights for the data subject that benefit from them.	YES	NO	WP74 point 5.7 (page 19)	<p>The BCRs must contain the right for every data subject to have an easy access to the BCRs.</p> <p>All data subjects benefiting from the third party beneficiary right should also have easy access to this clause.</p> <p>For instance, the BCRs may state that the BCRs will be published on the internet or on the intranet (when data subjects are the company staff).</p>
2 – EFFECTIVENESS				
2.1 The existence of a suitable training programme	YES	YES	WP 74 point 5.1. (page 16) + WP108 points 5.8-5.9. (page 5)	<p>The BCRs must state that appropriate training on the BCRs will be provided to personnel that have permanent or regular access to personal data, that are involved in the collection of personal data or in the development of tools used to process personal data.</p> <p>The Data Protection Authorities evaluating the BCRs may ask for some examples and explanation of the training programme during the application procedure and the training programme should be specified in the application.</p>

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
<p>2.2 The existence of a complaint handling process for the BCR</p>	<p>YES</p>	<p>YES</p>	<p>WP 74 point 5.3. (page 17) + WP 108 point 5.15 and 5.18 (page 6)</p>	<p>An internal complaint handling process must be set up in the BCRs. Any data subject should be able to complain that any member of the group is not complying with the rules.</p> <p>The complaints must be dealt by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions.</p> <p>The application form must explain how data subject will be informed about the practical steps of the complaint system, for instance:</p> <ul style="list-style-type: none"> - where to complain, - in which form, - delays for the reply on the complaint, - consequences in case of rejection of the complaint - consequences in case the complaint is considered as justified - consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court/Data Protection Authority)

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
<p>2.3 The existence of an audit programme covering the BCRs</p>	<p>YES</p>	<p>YES</p>	<p>WP 74 point 5.2. (page 16) + WP 108 point 6 (page 7)</p>	<p>The BCRs must create a duty for the group to have data protection audits on regular basis (by either internal or external accredited auditors) or on specific request from the privacy officer/function (or any other competent function in the organization).</p> <p>The BCRs must state that the audit programme covers all aspects of the BCRs including methods of ensuring that corrective actions will take place. Moreover, the BCRs must state that the result will be communicated to the privacy officer/function and to the ultimate parent's board.</p> <p>The BCRs must state that Data Protection Authorities can have access to the results of the audit upon request and give them the authority/power to carry out a data protection audit themselves if required.</p> <p>The application form will contain a description of the audit system. For instance :</p> <ul style="list-style-type: none"> - which entity (department within the group) decides on the audit plan/programme, - which entity will make the audit, - time of the audit (regularly or on specific request from the appropriate Privacy function.) - coverage of the audit (for instance, applications, IT systems, databases that process Personal Data, or onward transfers, decisions taken as regards mandatory requirement under national laws that conflicts with the BCRs, review of the contractual terms used for the transfers out of the Group (to controllers or processors of data), corrective actions, ...) - which entity will receive the results of the audits

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
<p>2.4 The creation of a network of privacy officers or appropriate staff for handling complaints and overseeing and ensuring compliance with the rules.</p>	YES	NO	WP 74, point 5.1 (page 16) and 5.3 (page 17)	<p>A commitment to appoint appropriate staff (such as a network of privacy officers) with top management support to oversee and ensure compliance with the rules.</p> <p>A brief description of the internal structure, role and responsibilities of the network or privacy officers or similar function created to ensure compliance with the rules. For example that the chief privacy officer advises the board of management, deals with Data Protection Authorities' investigations, annually reports on compliance, ensures compliance at a global level and that Privacy officers can be responsible for handling local complaint from data subjects, reporting major privacy issues to the chief privacy officer and for ensuring compliance at a local level.</p>
3 - COOPERATION DUTY				
<p>3.1 A duty to cooperate with Data Protection Authorities</p>	YES	YES	WP 74 point 5.4. (page 17) + WP108 point 5.21 (page 7)	The BCRs should contain a clear duty for all members of the group to co-operate with, to accept to be audited by the Data Protection Authorities and to comply with the advice of Data Protection Authorities on any issue related to those rules.
4 - DESCRIPTION OF PROCESSING AND DATA FLOWS				
<p>4.1 A description of the transfers covered by the BCRs</p>	YES	YES	WP 74 point 4.1 § 4 (page 14) + WP 108 point 7 (pages 7-8)	<p>The BCRs must also contain a general description of the transfers to allow the Data Protection Authorities to assess that the processing carried out in third countries is adequate and more precisely on:</p> <ul style="list-style-type: none"> i) the nature of the data transferred ii) the purposes of the transfer/processing iii) the data importers/exporters in the EU and outside of the EU <p>Some Data Protection Authorities may require more detailed description of the transfers.</p>

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
4.2 A statement of the geographical and material scope of the BCRs (nature of data, type of data subjects, countries)	YES	YES	WP 108 point 7.1.1 and 7.2 (pages 7&8)	<p>The BCRs should indicate if they apply to:</p> <ul style="list-style-type: none"> i) all personal data transferred from the European Union within the group OR, ii) all processing of personal data made within the company group <p>The BCRs must also specify its material scope, for instance, that the BCRs apply to personal data related to employees, customers, suppliers and other third parties as part of company's regular business activities.</p>
5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES				
5.1 A process for updating the BCRs	YES	YES	WP 74 point 4.2. (page 15) + WP 108 point 9 (pages 8-9)	<p>The BCRs can be modified (<i>for instance to take into account modifications of the regulatory environment or the company structure</i>) but they should impose a duty to report changes to all group members and to the Data Protection Authorities.</p> <p>Updates to the BCRs or to the list of the members of the BCRs are possible without having to re-apply for an authorization providing that :</p> <ul style="list-style-type: none"> i) An identified person keeps a fully updated list of the members of the group and keep track of and record any updates to the rules and provide the necessary information to the data subjects or Data Protection Authorities upon request. ii) No transfer is made to a new member until the new member is effectively bound by the BCRs and can deliver compliance. iii) Any substantial changes to the BCRs or to the list of members should be reported once a year to the Data Protection Authorities granting the authorizations with a brief explanation of the reasons justifying the update.

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
-------------------------------	-------------	-------------------------	--------------------	----------

6 - DATA PROTECTION SAFEGUARDS				
6.1 A description of the privacy principles including the rules on transfers or onward transfers out of the EU.	YES	YES	WP 108 point 8 (page 8) + WP74 point 3.1, last § and point 3.2 (page 9)	The BCRs should explain how the following principles are observed in the company: i) Transparency, fairness ii) Purpose limitation iii) Data quality iv) Security including the obligation to enter into contracts with all subcontractors/processors specifying the use of the data and the necessary security measures v) Rights of access, rectification, objection to processing vi) Restriction on transfers and onward transfers to processors and controllers which are not part of the group (Members of the group that are controllers can communicate data to processors/controllers out of the group that are located outside of the EU provided that adequate protection is provided according to Articles 16, 17, 25 and 26 of the Directive 95/46/EC)
6.2 The list of entities bound by BCRs	NO	YES	WP 108 point 7.1.3 (page 8).	See also point 5.1 in this paper the duty for an identified contact of the group to keep a fully updated list of the entities bound by the BCRs and the need to inform the Data Protection Authorities and the data subject in case of modification to the list.
6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs	YES	NO	WP 74 point 3.3.3. (pages 13-14)	A clear commitment that where a member of the group has reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the rules, he will promptly inform the EU headquarters or the EU member with delegated data protection responsibilities or the other relevant Privacy Officer/Function (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments
				In addition, a commitment that where there is conflict between national law and the commitments in the BCR the EU headquarters, the EU member with delegated data protection responsibilities or the other relevant Privacy Officer/Function will take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.
6.4 A statement about the relationship between national laws and BCRs	NO (not required, but welcomed)	NO (not required, but welcomed)	N/A	<p>Even though it is not required by the WP 74 and 108, it is very useful to specify the relationship between the BCRs and the relevant applicable law.</p> <p>The BCRs could state that, where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the BCR.</p> <p>In any event data shall be processed in accordance to the applicable law as provided by the Article 4 of the Directive 95/46/EC and the relevant local legislation.</p>

Done at Brussels, on 24/06/2008

*For the Working Party
The Chairman
Alex TÜRK*