WP133

Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data

Adopted on 10 January 2007

Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data[1]

Introduction and Instructions

The Data Protection Directive 95/46/EC allows personal data to be transferred outside the EEA only when the third country provides an "adequate level of protection" for the data (Art. 25) or when the controller adduces adequate safeguards with respect to the protection of privacy (Art. 26). Binding Corporate Rules (BCRs) are one of the ways in which such adequate safeguards (Art. 26) may be demonstrated "by a group of companies in respect of intra group transfers[2]" although the BCR are not a tool expressly listed and set forth in the Data Protection Directive 95/46/EC.

The use of BCRs to provide a legal basis for international data transfers from the EEA requires the approval of each of the EEA data protection authorities (DPAs) from whose country the data are to be transferred. The following form is for use by companies seeking approval of BCRs. The form is based on papers issued by the Article 29 Working Party of European data protection authorities (the "Working Party") and in particular is intended to help applicants demonstrate how to meet the requirements set out in WP 74 and WP 108[3].

General Instructions

- Only a single copy of the form need be filled out and submitted to the DPA you consider to be the lead authority in accordance with Section 3.3. and 3.4. WP 108[4]; this form may be used in all EEA Member States.
- Please fill out all entries and submit the form to the DPA you consider to be the lead DPA.
- You may attach additional pages or annexes if there is insufficient space to complete your responses.

---

[1] This questionnaire takes into account the draft standard application form for approval of Binding Corporate Rules drawn up by the ICC.

[2] see working document WP 74, Section 3.1, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

[3] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

[4] The lead authority is established according to Section (3) of WP 108, see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

The language of the application shall be set up according to WP 107, Section (8), where …"… as a general rule and without prejudicing to other translations where necessary or required by law, first and consolidated drafts should be provided both in the language of the leading authority and in English. The final draft must be translated into the languages of those DPAs concerned".

See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

- You may indicate any responses or materials that is in your opinion commercially sensitive and should be kept confidential. Requests by third parties for disclosure of such information, will, however, be handled by each data protection authority involved in accordance with national legislation.
- The footnotes in the application form indicate the relevant provisions of the Working Party papers WP 74 and WP 108, which contain further clarification of the questions.
- Once you have submitted the form, the DPA you approached will circulate Part 1 of the form to all DPAs from whom you are seeking approval in order to determine who should be the lead DPA;
- You will be informed by the DPA you approached which DPA has finally been appointed by all DPAs involved to act as lead DPA;
- The lead DPA will circulate the remainder of the form including your BCR to all DPAs from whom you are seeking approval in order to comply with the various stages of the Co-Operation Procedure.

PART 1 APPLICANT INFORMATION

Section 1: Structure and Contact Details of the Applicant and of the Group of Companies

- If the Group has its headquarters in the EEA the form should be filled out and submitted by that EEA entity.
- If the Group has its headquarters outside the EEA, then the Group should appoint a Group entity located inside the EEA – preferably established in the country of the presumptive lead DPA - as the Group member with "delegated data protection responsibilities". This is the entity which should then submit the application on behalf of the Group.
- Contact Details of the Responsible Party for Queries:
    - Please indicate a responsible party to whom queries may be addressed concerning the application.
    - This party need not be located in the EEA, although this might be advisable for practical reasons.
    - You may indicate a function rather than a specific person.

Section 2: Short description of data flows

- The applicant should also give a brief description of the scope and nature of the data flows from the EEA for which approval is sought.

Section 3: Determination of the Lead Data Protection Authority

- The lead DPA is the authority in charge of coordinating approval of your application by all DPAs from countries within the EEA which you have named in your application as the origin of transfers of personal data by Group members to third countries.
    - Before you approach one DPA as the presumptive lead DPA you should examine the factors listed in sections 3.3 and 3.4. of WP 108. Based on these factors you should explain in Part 1.3 of your application which DPA should be the lead DPA. The DPAs are not obligated to accept the choice that you make if they believe that another DPA is more suitable to be lead DPA.

PART 2 BACKGROUND PAPER

Section 4: Binding Nature of the Binding Corporate Rules

- In order for the BCRs to be approved for the transfer of personal data, they must be shown to have legally binding effect both internally (between the Group entities, and on employees and subcontractors) and externally (for the benefit of individuals whose personal data is processed by the Group) in accordance with national legislation. These questions elicit the information necessary to determine if your BCRs have such binding effect.
- Your application will need to make clear that the burden of proof with regard to an alleged breach of the rules will rest with the member of the Group at the origin of the transfer or the European headquarters or that part of the organisation with delegated data protection responsibilities, regardless of where the claim originates.
- Regulators in some sectors (such as the financial services industry) may prohibit an entity of the Group in one country from assuming liability for another Group entity in another country. If this is the case for your application, please provide details about this situation in the subsection "Legal claims or actions" and explain any other mechanisms

your Group has implemented to ensure that an aggrieved individual can obtain recourse against the Group.

Section 5: Effectiveness

- Effectiveness (verification of compliance) may be demonstrated by a variety of mechanisms typically implemented by companies, such as a regular audit programme, corporate governance activities, compliance departments, etc. Please respond to the questions on effectiveness based on the verification mechanisms used in your group.
- As not all DPAs have the power to audit under their national law, you will need to confirm that you will permit the DPAs from which you obtained approval to audit your compliance.

Section 6: Cooperation with DPAs

- Section 6 focuses on cooperation with DPAs. You have to specify how your BCRs deal with the cooperation with DPAs.

Section 7: Description of Processing and Data Flows

- In order for the DPAs to assess whether your BCRs provide adequate safeguards for the transfers of data, it is essential that you describe data flows within your Group in a complete yet understandable fashion. This does not preclude providing additional information to EEA DPAs in the context of complying with applicable national notification requirements.

Section 8: Mechanisms for Reporting and Recording Changes

- Both the DPAs having approved of the BCRs and the Group entities must be informed about any changes to the BCRs. This obligation applies only to changes that significantly affect data protection compliance, and not to mere administrative changes (unless they impact the BCRs). In this section, please describe the mechanisms your Group has implemented for reporting and recording such changes.
- The obligation to report changes applies only to the text of the BCRs themselves, and not to any supporting documentation, unless a change to such documentation would significantly affect compliance with the BCRs.

Section 9: Data Protection Safeguards

- In this Section please provide details of how your BCRs address the core data protection safeguards that are necessary to provide an adequate level of protection for the data that are transferred

Annex 1: Copy of the Formal Binding Corporate Rules

- Please attach a copy of your BCRs. These need not necessarily be contained within one document and your BCRs may comprise a number of documents. In the latter case please clearly specify the legal relationship between these documents (e.g. general rules – more detailed rules for a specific area like HRM or CRM).
- You do not need to attach all ancillary documentation at this stage, this may be submitted separately after discussions with the lead authority.

Standard Application for Approval of Binding Corporate Rules

PART 1: APPLICANT INFORMATION

1. STRUCTURE AND CONTACT DETAILS OF THE GROUP

Name of the Group and location of its headquarters (ultimate parent company):
Does the Group have its headquarters in the EEA? ☐ Yes ☐ No

Name and location of the applicant:		
Identification number (if any):		
Legal nature of the applicant (corporation, partnership, etc.):		
Description of position of the applicant within the Group: (e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)		
Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):		
Address:		
Country:		
Phone number:	Fax:	E-Mail:

EEA Member States for which approval of the BCRs is sought:

2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS

Please, indicate the following:

- Nature of the data covered by BCRs, and in particular, if they apply to one category of data or to more than one category (for instance human resources, customers,…)

- Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the group?

- Please specify from which country most of the data are transferred outside the EEA:

- Extent of the transfers within the Group that are covered by the BCRs; including a description of any Group members in the EEA or outside EEA to which personal data may be transferred

3. DETERMINATION OF THE LEAD DATA PROTECTION AUTHORITY (DPA)

Please explain which should be the lead DPA, based on the following criteria:

- Location of the Group's EEA Headquarters

- If the Group is not headquartered in the EEA, the location in the EEA of the Group entity with delegated data protection responsibilities

- The location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the binding corporate rules in the Group

- Country where most of the decisions in terms of the purposes and the means of the data processing are taken

- EEA Member States from which most of the transfers outside the EEA will take place

PART 2: BACKGROUND PAPER[5]

4. BINDING NATURE OF THE BINDING CORPORATE RULES (BCRs)

INTERNAL BINDING NATURE[6]

Binding within the entities of the Group[7]

How are the BCRs made binding upon the members of the Group?

- ☐ Measures or rules that are legally binding on all members of the Group
- ☐ Contracts between the members of the Group[8]
- ☐ Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group
- ☐ Incorporation of other regulatory measures (e.g. obligations contained in statutory codes within a defined legal framework)
- ☐ Incorporation of the BCRs within the general business principles of a Group backed by appropriate policies, audits and sanctions
- ☐ Other (please specify)

Please explain how the mechanisms you indicated above are legally binding on the members of the Group in the sense that they can be enforced by other members of the Group (esp. headquarters):

Does the internally binding effect of your BCRs extend to the whole Group? (If some Group members should be exempted, specify how and why?)

[5] Working Document 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.

[6] See Section 3.3.1. WP74 and Section 5 WP108

[7] See Section 5.3 WP108

[8] See also footnote 11

Binding upon the employees[9]

Your Group may take some or all of the following steps to ensure that the BCRs are binding on employees, but there may be other steps. Please, give details below. - Work employment contract - Collective agreements (approved by workers committee/another body) - Employees must sign or attest to have read the BCRs or related ethics guidelines in which the BCRs are incorporated - BCRs have been incorporated in relevant company policies - Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation Please provide a summary supported by extracts from policies and procedures or confidentiality agreements as appropriate to explain how the BCRs are binding upon employees.

Binding upon subcontractors processing the data[10]

What steps have you taken to require subcontractors to apply protections to the processing of personal data (e.g., through the use of obligations in your contracts with them)? Please specify:
How do such contracts address the consequences of non compliance?
Please specify the sanctions imposed on subcontractors for failure to comply

[9] See Section 5.8 WP108

[10] See Section 5.10 WP108

EXTERNALLY BINDING NATURE[11]

How are the rules binding externally for the benefit of individuals (third party beneficiary rights) or how do you intend to create such rights? For example you might have created some third party beneficiary rights in contracts or unilateral declarations[12].

Legal claim or actions
Explain how you meet the obligations according to the requirement of paragraph 5.14. of WP 108[13]

Please confirm that the European headquarters of the Group, or that part of the Group with delegated data protection responsibilities in the European Economic Area, has made appropriate arrangements to enable itself or the member of the Group at the origin of the transfer payment of compensation for any damages resulting from the breach, by any part of the Group, of the BCRs and explain how this is ensured.
Please confirm that the burden of proof with regard to an alleged breach of the rules will rest with the member of the Group at the origin of the transfer or the European headquarters or that part of the organisation with delegated data protection responsibilities, regardless of where the claim originates.

[11] See Section 3.3.2 WP74 and Section 5.12 WP108

[12] You must be fully aware of the fact that according to civil law of some jurisdictions (e.g. Italy or Spain) unilateral declarations or unilateral undertakings do not have a binding effect. In the lack of a specific legislative provision on bindingness of such declarations, only a contract with third party beneficiary clauses between the members of the Group may give proof of bindingness.

[13] 5.14. Individuals must be able to bring in claims within the jurisdiction of:
5.14.1. the member of the group at the origin of the transfer or,
5.14.2. the EU headquarters or the European member of the group with delegated data protection responsibilities .

Some jurisdictions might, however, insist on a possibility to bring in claims – in all cases - within the jurisdiction of the member of the group at the origin of the transfer.

5. EFFECTIVENESS[14]

It is important to show how the BCRs in place within your organization are brought to life in practise, in particular in non EEA countries where data will be transferred on the basis of the BCRs, as this will be significant in assessing the adequacy of the safeguards.

Training and awareness raising (employees)

- Special training programs

- Employees are tested on BCRs and data protection

- BCRs are communicated to all employees on paper or online

- Review and approval by senior officers of the company

- How are employees trained to identify the data protection implications of their work, i.e. to identify that the relevant privacy policies are applicable to their activities and to react accordingly? (This applies whether these employees are or not based in the EEA)

Internal complaint handling[15]

Do the BCRs contain an internal complaint handling system to enforce compliance?

Please describe the system for handling complaints:

[14] See Section 5.2 WP74 and Section 6 WP108

[15] See Section 5.3 WP74

Verification of compliance

What verification mechanisms does your Group have in place to audit each member's compliance with your BCRs? (e.g., an audit programme, compliance programme, etc)? Please specify:

Please explain how your verification or compliance programme functions within the Group (e.g., information as to the recipients of any audit reports and their position within the structure of the Group).

Do the BCRs provide for the use of:

- Data Protection Officer? Choose by clicking here
- internal auditors? Choose by clicking here
- external auditors? Choose by clicking here
- a combination of both internal and external auditors? Choose by clicking here
- verification by an internal compliance department? Choose by clicking here

Do your BCRs mention if the verification mechanisms are clearly set out in…

- a document containing your data protection standards Choose by clicking here
- other internal procedure documents and audits? Choose by clicking here

6. COOPERATION WITH DPAs[16]

Please, specify how your BCRs deal with the issues of cooperation with DPAs:

Do you confirm that you will permit the DPAs from which you obtained approval to audit your compliance?

Do you confirm that the Group as a whole and each of the companies of the Group will abide by the advice of the competent authority relating to the interpretation and the application of your BCRs?

[16] See Section 5.4 WP 74

7. DESCRIPTION OF PROCESSING AND DATA FLOWS[17]

Please indicate the following:

- Nature of the data covered by the BCRs, e.g. HR data, and in particular, if they apply to one category of data or to more than one category

  - What is the nature of the personal data being transferred?

  - In broad terms where do the data flow to and from?

  - In broad terms what is the extent of the flow of data?

  - What are the purposes of those transfers and the processing that is carried out after the transfers?

- Purposes for which the data covered by the BCRs are transferred to third countries

- Extent of the transfers within the Group that are covered by the BCRs, including a description of any Group members in the EEA or outside the EEA to which personal data may be transferred

Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the Group? Please specify:

[17] See Section 7 WP108

8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[18]

Explain how your BCRs allow for informing other parts of the Group and the relevant Data Protection Authorities of any significant changes to the BCRs that would in principle have an effect on the authorisation (summary):

Please confirm that you have put in place a system to record any changes to your BCRs.

9. DATA PROTECTION SAFEGUARDS[19]

Please, specify with reference to your BCRs how and where the following issues are addressed with supporting documentation where appropriate:

- Transparency and fairness to data subjects

- Purpose limitation

- Ensuring data quality

- Security

- Individual's rights of access, rectification, objection to processing

- Restrictions on onward transfers

- Other (e.g. protection of children, etc.)

[18] See Section 9 WP108

[19] See Section 8 WP108

ANNEX 1:
COPY OF THE FORMAL BINDING CORPORATE RULES

Please attach a copy of your BCRs. Note that this does not include any ancillary documentation that you would like to submit (e.g. specific privacy policies and rules).