



**05/EN
WP108**

**Working Document Establishing a Model Checklist Application for Approval of
Binding Corporate Rules**

Adopted on April 14th, 2005

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, Justice, Freedom and Security Directorate-General.
Website: www.europa.eu.int/comm/privacy

The participation of data protection authorities in the approval of binding corporate rules is entirely voluntary¹. The decision to participate can be made on a case by case basis. No data protection authority would be obliged to participate in any procedures aimed at approval of binding corporate rules. The participation of authorities that do not have the power to authorise international data transfers would be understood as reporting favourably, where appropriate, to the national authority in charge of granting authorisations for international data transfers.

The elements described in this document are no doubt very important but are not carved in stone and the Article 29 Working Party may revisit this document in the future in the light of experience. Companies are invited to use this check-list when submitting BCRs for the consideration of national data protection authorities. Companies should also bear in mind that their proposals may require supplementation to comply with the relevant requirements of the national legal systems concerned, in particular as regards those means being proposed to guarantee that data subjects can exercise their rights under the BCRs.

Those issues not covered by the model check-list will be discussed and dealt with by those authorities concerned as a part of normal consultations during the co-operation procedure. The checklist is intended to encompass all the requirements of the Article 29 Working Party number 74² ("WP 74") and concentrates on the matters that a DPA needs to consider in the assessment of adequacy as laid down by the Article 29 Working Party in WP 74.

¹ References to data protection authorities should be understood as including data protection authorities of EU and EEA countries.

² 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.

1. **What is this checklist for?**
2. This checklist is designed to assist a group of companies when it applies for approval of its binding corporate rules and in particular to help demonstrate how the group complies with WP74³.
3. **Which data protection authority should you apply to?**
 - 3.1. If the ultimate parent or operational headquarters of your group is a company incorporated in a member state of the EU, you should apply to the data protection authority of that member state.
 - 3.2. If it is not clear where the ultimate parent or operational headquarters of your group is situated, or if it is situated outside the EU, you should apply to the most appropriate data protection authority in accordance with the criteria set out below.
 - 3.3. When applying you need to explain in detail why the data protection authority you have applied to is the most appropriate data protection authority. Factors that are taken into account to determine whether you have applied to the most appropriate data protection authority include:
 - 3.3.1. the location of the group's European headquarters.
 - 3.3.2. the location of the company within the group with delegated data protection responsibilities⁴;
 - 3.3.3. 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;
 - 3.3.4. the place where most decisions in terms of the purposes and the means of the processing are taken; and
 - 3.3.5. the member states within the EU from which most transfers outside the EEA will take place.
 - 3.4. Priority will be given to factor 331.
 - 3.5. These are not formal criteria. The data protection authority to which you send your application will exercise its discretion in deciding whether it is in fact the most appropriate data protection authority and, in any event, the data protection authorities among themselves may decide to allocate the application to a data protection authority other than the one to which you applied.

³ WP74 sets out the requirements for binding corporate rules.

⁴ As provided for in the working document number 74, if the headquarters of the corporate group were not in the EU/EEA, the corporate group should appoint a European member with delegated data protection responsibilities in charge of ensuring that any foreign member of the corporate group adjust their processing activities to the undertakings contained in the corporate group, interface with the leading authority where appropriate and pay compensation in case of damages resulting from the violation of the binding corporate rules by any member of the corporate group.

4. What information is required for your application?

4.1. You will need to supply:

4.1.1. A separate document containing:

4.1.1.1. contact details of the responsible person within your organisation to whom queries may be addressed; and

4.1.1.2. all the relevant information to justify the choice of data protection authority including the basic structure of your group and the nature and structure of the processing activities in the EU/EEA with particular attention to the place/s where decisions are made, the location of affiliates in the EU, the means and purposes of the processing, the places from which the transfers to third countries are being made and the third countries to which those data are transferred (this is needed so that the 'entry point data protection authority' can circulate it to the data protection authorities concerned);

4.1.2. A background paper summarising how the required elements of WP74 (as set out below) have been satisfied (this will help the data protection authorities to identify the relevant sections of the documents you are providing);

4.1.3. All relevant documents that comprise the 'binding corporate rules' to be adopted by your organisation (e.g. any policies, codes, notices, procedures and contracts that may be relevant to the application). As well as a general statement of principles, the data protection authorities need to see how personal data is actually handled within your group;

4.1.4. It is important to note that whilst a data protection authority will have duties under its national law not to disclose information received from a data controller as part of the authorisation process without lawful authority, some data protection authorities are also subject to freedom of information legislation. Accordingly, if any documentation submitted in support of your application for authorisation of your binding corporate rules is commercially sensitive, please mark the appropriate documents appropriately. However, the decision on whether to disclose the information will be taken by each data protection authority involved in accordance with national freedom of information legislation. Also, the information that is necessary for the other involved data protection authorities to assess the binding corporate rules will have to be circulated.

5. Evidence that the measures are legally binding:

5.1. The rules must be binding both –

5.1.1. within the organisation and;

5.1.2. externally for the benefit of individuals.

5.2. There are a number of ways in which this requirement may be met and how this is done will depend upon the structure and size of your organisation and the

procedures adopted with regard to other regulatory requirements to which your organisation may be subject. It will also depend upon the national laws in the Member States in which your organisation is located.

5.3. Binding within the organisation

5.4. How are the rules binding between the component parts of the organisation?

5.5. You must ensure compliance with the binding corporate rules by other members of the group. This is particularly important where there is no 'head office' or where the head office is outside the EEA. How this is achieved will depend upon the structure of your organisation but will also be subject to the national laws of the Member States in which your organisation is located.

5.6. The following are suggestions as to how a set of corporate rules may be binding on an organisation but there may be other ways more suited to your proposed arrangements:

5.6.1. Binding corporate or contractual rules that you can enforce against the other members of the group;

5.6.2. Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the group;

5.6.3. Incorporation of other regulatory measures, for example, obligations contained in statutory codes within a defined legal framework; or

5.6.4. Incorporation of the rules within the general business principles of an organisation backed by appropriate policies, audits and sanctions.

5.7. All of the above suggestions may have a different effect in different member states. For example, simple unilateral declarations are not regarded as binding in some member states. You would, therefore, need to take local advice if you intended to rely on such declarations.

Please explain how the rules are binding upon the members of the group.

5.8. How are the rules made binding on employees?

5.9. Employees must be bound by the rules. This might be achieved by way of specific obligations contained in a contract of employment and by linking observance of the rules with disciplinary procedures for example. In addition, there should be adequate training programmes and senior staff commitment, and the title of the person ultimately responsible within the organisation for compliance should be included in your application.

Please explain how the rules are binding upon employees within your organisation and the sanctions for failure to comply with the rules.

5.10. **How are the rules made binding on subcontractors handling the data?**

5.11. You need to show how your binding corporate rules are made binding on subcontractors. Please provide evidence of the type of contractual clauses that you impose on subcontractors and explain how those contracts deal with the consequences of non-compliance.

Please specify how the rules are binding upon subcontractors and the sanctions for failure to comply with the rules.

5.12. **How are the rules binding externally for the benefit of individuals?**

5.13. Individuals covered by the scope of the binding corporate rules must be able to enforce compliance with the rules both via the data protection authorities and the courts.

5.14. Individuals must be able commence 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 .

5.15. Your application will need to show the practical steps a data subject can take to obtain a remedy from your organisation, including a complaint handling process.

5.16. For example, if your headquarters and the lead authority are in Belgium and one of your group companies in Italy breaches your corporate rules, it should be clear to the data subject that he or she can make a claim against the infringing company in Italy and/or the headquarters in Belgium.

5.17. Your application should contain confirmation that the European headquarters of the organisation, or that part of the organisation with delegated data protection responsibilities in the EU, has sufficient assets or has made appropriate arrangements to enable payment of compensation for any damages resulting from the breach, by any part of the organisation, of the binding corporate rules.

5.18. In your application please identify which part of the organisation is responsible for handling claims, and how the individual can access the complaints handling process.

5.19. 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.

5.20. Your application should acknowledge that a data subject will have the rights afforded under Directive 95/46/EC.

- 5.21. Your application should also include confirmation that you will co-operate with the data protection authorities with regard to any decisions made by the supervisory authority and abide by the advice of the data protection authority with regard to interpretation of WP 74.

Please specify how the rules are binding externally

6. Verification of compliance

- 6.1. WP74 states that the binding corporate rules adopted by an organisation must provide for the use of either internal auditors, external auditors or a combination of both.
- 6.2. The data protection audit programme and audit plan need to be clearly set out either in a document containing your data protection standards or in other internal procedure documents and audits provided to a data protection authority upon request. The authority will need to be satisfied that the audit programme adequately covers all aspects of the binding corporate rules including methods of ensuring that corrective actions have taken place. The audit plan should allow for the supervisory authority to have the power to carry out a data protection audit if required.
- 6.3. Data protection authorities neither need nor want to see anything in your audit results that does not relate to data protection. The authorities are not concerned with corporate governance, except to the extent that it affects data protection compliance. Equally, the authorities are not interested in seeing commercially sensitive information. The information provided should be limited to that which is required to satisfy WP 74. However, it is appreciated that issues relating to data protection compliance may be included in reports containing other information and it will sometimes not be possible to separate those elements relating to data protection from other unrelated information.
- 6.4. Please summarise your audit arrangements for data protection matters and the way in which audit reports are handled internally within your organisation (i.e. information as to the recipients of the report and their position within the structure of the organisation).

Please give details of your data protection audit programme and audit plan.

7. Description of processing and flows of information

- 7.1. The binding corporate rules should identify the following:
- 7.1.1. the nature of the data. i.e. whether the binding corporate rules relate to only one type of data, for example, human resource data, or, if the rules relate to more than one type of data, how this is addressed in the binding corporate rules. In any event, there should be sufficient detail included in the application to enable a supervisory authority to assess whether the

safeguards put in place address adequately the nature of the processing being undertaken;

7.1.2. the purposes for which the data are processed;

7.1.3. the extent of the transfers within the group that are covered by the rules. We need to have details of:

7.1.3.1.any group members in the EU from which personal data may be transferred; and

7.1.3.2.any group members outside the EEA to which personal data may be transferred.

7.2. You also need to show whether the binding corporate rules apply only to transfers from the EU only or whether all transfers between members of the group are covered. The data protection authorities need to understand on what basis onward transfers (ie transfers of data from group members outside the EEA to third parties) take place.

Please describe the nature of the data, the purposes for which they are processed and the extent of the transfers within the group.

8. Data protection safeguards

8.1. The rules must contain a clear description of the standard of data protection safeguards applied to the data consistent with Directive 95/46/EC and must set out how these requirements are met within your organisation.

8.2. In particular, the binding corporate rules must address the following;

8.2.1. transparency and fairness to data subjects;

8.2.2. purpose limitation;

8.2.3. ensuring data quality;

8.2.4. security;

8.2.5. individual rights of access, rectification and objection to processing;

8.2.6. restrictions on onward transfer out of the multinational company covered by the rules (although this may be possible under other arrangements facilitating transfers).

Please provide a summary of how this has been addressed in the binding corporate rules adopted by your organisation with supporting documentation e.g. relevant policies.

9. Mechanism for reporting and recording changes

9.1. There must be a system in place for informing other parts of the organisation and the data protection authority of any changes to the rules in line with paragraph 4.2 of WP74. The data protection authorities will only need to see changes that significantly affect data protection compliance. Administrative changes, for example, do not need to be notified unless they impact on the operation of the binding corporate rules. Your lead authority will inform you of any specific requirements to report to or update any data protection authorities.

Please describe the mechanism that your organisation will use to report changes.

Done in Brussels, on April 14, 2005

For the Working Party
The Chairman
Peter Schaar