



1271-00-01/08/EN
WP 154

**Working Document setting up a framework for the structure of 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

The Working Party has already established that international transfers of personal data from the EU but within the corporate group can take place on the basis of Binding Corporate Rules (BCRs) and has provided guidance on what the necessary elements of those rules are in documents WP74¹ and WP108².

To try and further assist and guide organisations in developing BCRs the Working Party has developed the attached framework which is a suggestion of what the BCRs might look like when incorporating all of the necessary elements identified in documents WP 74³ and WP 108⁴.

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 See footnote 1

⁴ See footnote 2

Framework for Binding Corporate Rules (“BCRs”)

WARNING

This framework for BCRs is not a model BCR it is just a suggestion of the content and how the rules might be structured in a single document which can be made binding on the group of companies.

BCRs should be customized to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data. Therefore please note that DPAs will not accept a pure copy and paste of this framework.

The BCRs will in effect become the privacy policy of your group of companies for transfers of EU personal data globally and may become the policy for all personal data processed by the group of companies globally.

Introduction:

- A clear duty for all the members of the Group and for the employees to respect the BCRs.
- A commitment from the company’s board of management that they will ensure compliance with the described rules.
- The objectives of the BCRs (to provide adequate protection for the transfers and processing of personal data by the group of companies).
- Reference to the applicable texts on data protection (EU Directives 95/46/EC and 2002/58/EC).

1 – Scope

A description of the scope of the BCRs application and especially:

- That they will apply to intra-group transfers and processing.
- The geographical scope (only data processed in the EU and transferred outside of the EU or all data).
- The material scope (e.g. type of processing: automated/manual, nature of data: customer/HR/suppliers).

A general description of the data flows and the purposes of the processing including:

- The nature of the data transferred,
- The purposes of the transfer/processing,
- The data importers/exporters in the EU and outside of the EU⁵.

⁵ Please note that some Data Protection Authorities might request more details with respect the description of transfers and processing.

2 – Definitions

A description of the main terms and their definitions:

- The main definitions (personal data, sensitive personal data, data subject, controller, processor, processing, third party, Data Protection Authorities),
- Other relevant definitions might be inserted in a glossary, such as data exporter, data importer, EU headquarters/EU Member with delegated responsibilities, members of the group⁶, privacy officer/function.
- A commitment to interpret the terms in the BCRs according to the EU Directives 95/46/EC and 2002/58/EC.

3 – Purpose limitation

A description of the purposes for which the data are processed and transferred and confirmation that :

- Personal data will be transferred and processed for specific and legitimate purposes
- Personal data will not be further processed in a way incompatible with those purposes.
- Sensitive Data will be provided with additional safeguards such as provided by the EU Directive 95/46/EC.

4 - Data quality and proportionality

A commitment that:

- Personal data must be accurate and where necessary, kept up-to-date.
- Personal data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
- Personal data should not be processed for longer than necessary for the purposes for which they are obtained and further processed.

5 – Legal basis for Processing Personal Data

Personal data should be processed based on the following grounds:

- The data subject has unambiguously given his consent; or
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- The processing is necessary for compliance with a legal obligation to which the controller is subject; or
- The processing is necessary in order to protect the vital interests of the data subject; or
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

⁶ A Member could be Controller or Processor, Data Exporter or Data Importer

6 – Legal basis for Processing Sensitive Data

Processing of sensitive data is prohibited expect if:

- The data subject has given his explicit consent to the processing of those sensitive data, except where the applicable laws prohibit it; or
- The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- The processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
- The processing relates to sensitive data which are manifestly made public by the data subject; or
- The processing of sensitive data is necessary for the establishment, exercise or defence of legal claims; or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

7 – Transparency and information right

A commitment to make the BCR readily available to every data subject.

Moreover, your BCRs shall describe the way data subject are informed of the transfer and processing of their personal data.

A commitment that before their data is processed data subjects will be given the following information:

- The identity of the controller(s) and of his representative, if any;
- The purposes of the processing for which the data are intended;
- Any further information such as:
 - i) the recipients or categories of recipients of the data,
 - ii) the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Where the data have not been obtained from the data subject, the obligation to inform the data subject does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

8 – Rights of access, rectification, erasure and blocking of data:

A commitment that:

- Every data subject has the right to obtain without constraint at reasonable intervals and without excessive delay or expense a copy of all data relating to them that are processed.
- Every data subject has the right to obtain the rectification, erasure or blocking of data in particular because the data are incomplete or inaccurate.
- Every data subject has the right to object, at any time on compelling legitimate grounds relating to their particular situation, to the processing of their personal data, unless that processing is required by law. Where the objection is justified, the processing must cease.
- Every data subject has the right to object, on request and free of charge, to the processing of personal data relating to him for the purposes of direct marketing.

An explanation of how the data subjects can get access to their personal data.

9 – Automated individual decisions

A commitment that no evaluation of or decision about the data subject which significantly affects them will be based solely on automated processing of their data unless that decision:

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
- is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

10 – Security and confidentiality

A commitment that appropriate technical and organizational measures to protect personal data have been implemented against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

In this regard, sensitive data should be processed with enhanced security measures.

11 – Relationships with processors that are members of the group

An explanation of how personal data are protected when using a processor who is a member of the group. In particular a requirement that:

- The controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

- The controller shall instruct the processor by written contractual means in accordance with the applicable law and this contract will among others stipulate:
 - i) That the processor shall act only on instructions from the controller
 - ii) The rules relating to the security and confidentiality to be incumbent on the processor

12 – Restrictions on transfers and onward transfers to external processors and controllers (not members of the group)

An explanation of the measures in place to restrict transfers and onward transfers outside of the group and a commitment that:

- External processors located inside the EU or in a country recognised by the EU Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the processor shall act only on instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures
- All transfers of data to external controllers located out of the EU must respect the European rules on transborder data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other adequate contractual means according to Articles 25 and 26 of the EU Directive).
- All transfers of data to external processors located out of the EU must respect the rules relating to the processors (Articles 16-17 Directive 95/45/EC) in addition to the rules on transborder data flows (Articles 25-26 of Directive 95/46/EC).

13 – Training programme

A commitment to provide appropriate training on the BCRs to personnel who have permanent or regular access to personal data, are involved in the collection of personal data or in the development of tools used to process personal data.

14 – Audit programme

A commitment to audit the group's compliance with the BCRs and in particular that:

- The audit programme covers all aspects of the BCRs including methods of ensuring that corrective actions will take place.
- Such audit must be carried out on a regular basis (specify the time) by the internal or external accredited audit team or on specific request from the privacy officer/function (or any other competent function in the organization)
- The results of all audits should be communicated to the privacy officer/function (or any other competent function in the organization) and to the board of management.
- The Data Protection Authorities can receive a copy of such audits upon request.
- The audit plan should allow the Data Protection Authorities to have the power to carry out a data protection audit if required.
- Each Member of the group shall accept that they could be audited by the Data Protection Authorities and that they will abide by the advice of the Data Protection Authorities on any issue related to those rules.

15 – Compliance and supervision of compliance

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.

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 complains from data subjects, reporting major privacy issues to the chief privacy officer and for ensuring compliance at a local level.

16 – Actions in case of national legislation preventing respect of BCRs

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 function (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

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 Function will take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.

17 – Internal Complaint Mechanisms

A commitment to put in place a complaint handling process where:

- Any data subject may complain that any member of the group is not complying with the BCRs.
- The complaints will be dealt by a clearly identified department/person which must benefit from an appropriate level of independence in the exercise of his/her functions.

18 - Third party beneficiary rights

A clear statement that the BCRs 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).

A statement that the data subjects can choose to lodge claims before:

- The jurisdiction of the data exporter located in the EU, or
- The jurisdiction of the EU headquarters/the EU Member with delegated responsibilities,
or
- Before the competent Data Protection Authorities.

A commitment that all data subjects benefiting from the third party beneficiary rights should also have easy access to this clause.

19 - Liability

A commitment that:

- Either EU headquarters or the EU Member with delegated responsibilities⁷ accept responsibility for and agree to take the necessary action to remedy the acts of other Members of the corporate group outside of the EU and to pay compensation for any damages resulting from the violation of the BCRs by the members of the group.
- The burden of proof stays with either the EU headquarters or the EU Member with delegated responsibilities to demonstrate that the member outside the EU is not liable for the violation resulting in the damages claimed by the data subject.

If the EU headquarters or the EU Member with delegated responsibilities can prove that the member outside the EU is not liable for the violation, it may discharge itself from any responsibility.

20 – Mutual assistance and cooperation with Data Protection Authorities

A commitment that:

- Members of the group shall cooperate and assist each other to handle a request or complaint from an individual or an investigation or inquiry by Data Protection Authorities.
- Entities will abide by the advice of the Data Protection Authorities on any issues regarding the interpretation of the BCRs.

21 – Updates of the rules

A commitment to report any significant changes to the BCRs or to the list of members to all group members and to the Data Protection Authorities to take into account modifications of the regulatory environment and the company structure and more precisely that:

- Some modifications might require a new authorization from the Data Protection Authorities.
- Updates to the BCRs or to the list of the Members of the group bound by the BCRs are possible without having to re-apply for an authorization providing that:

⁷ 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 to define an alternative 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.

- i) An identified person keep a fully updated list of the members of the BCRs 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 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.

A commitment that substantial modifications to the rules will also be communicated to the data subjects.

22 – Relationship between national laws and the BCRs

A explanation that:

- Where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the BCRs.
- 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.

23 – Final provisions

- Effective date
- Transitional period

Documentation to be provided to the DPAs

- 1 - Standard Application Form WP133
- 2 - Any documentation that may show that commitments in the BCRs are being respected, for instance:
 - Privacy policies per processing (e.g. Customer Privacy Policy, HR Privacy Policy) to inform data subjects (e.g. customers, employees) about the way the Company protect their personal data
 - Guidelines for employees having access to personal data so that they can easily understand and apply the rules prescribed into the BCRs (e.g. guidelines on how to respond to a complaint from a data subject, on how to provide information to data subjects, on appropriate security/confidentiality measures to be observed)
 - Data protection audit plan and programme defined with relevant persons (internal/external accredited auditors of the company)
 - Examples and/or explanation of the training programme
 - Documentation showing that the member that is at the origin of the transfer of data outside of the EU and either the EU headquarters or the EU Member with delegated responsibilities has sufficient assets to enable payment of compensation for damages resulting from the breach of the BCRs.
 - Description of the internal complaint system
 - List of entities bound by the BCRs
 - Security policy for IT systems processing EU personal data
 - Certification process to make sure that all new IT applications processing EU data are BCRs compliant.

- Any standard contracts to be used with data processors (member or non member of the Group) processing EU data
- Job description of data protection officers or other persons in charge of data protection in the Company

Done at Brussels, on 24/06/2008

*For the Working Party
The Chairman
Alex TÜRK*