II

*(Acts whose publication is not obligatory)*

# COMMISSION

## COMMISSION DECISION

**of 15 June 2001**

**on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC**

*(notified under document number C(2001) 1539)*

**(Text with EEA relevance)**

(2001/497/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1], and in particular Article 26(4) thereof,

Whereas:

(1) Pursuant to Directive 95/46/EC, Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC, the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on Protection of Individuals with regard to the processing of personal data established under that Directive [2] has issued guidelines to aid with the assessment [3].

---

[1] OJ L 281, 23.11.1995, p. 31.

[2] The Internet address of the Working Party is: http://www.europa.eu.intlcomm/internal_market/en/medial/dataprot/wpdocs/index.htm.

[3] WP 4 (5020/97) 'First orientations on transfers of personal data to third countries working document — possible ways forward in assessing adequacy', a discussion document adopted by the Working Party on 26 June 1997.
WP 7 (5057/97) 'Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?', working document: adopted by the Working Party on 14 January 1998.
WP 9 (3005/98) 'Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries', working document: adopted by the Working Party on 22 April 1998.
WP 12: 'Transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive', working document adopted by the Working Party on 24 July 1998, available, in the web-working document site 'europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en' hosted by the European Commission.

(4) Article 26(2) of Directive 95/46/EC, which provides flexibility for an organisation wishing to transfer data to third countries, and Article 26(4), which provides for standard contractual clauses, are essential for maintaining the necessary flow of personal data between the Community and third countries without unnecessary burdens for economic operators. Those Articles are particularly important in view of the fact that the Commission is unlikely to adopt adequacy findings under Article 25(6) for more than a limited number of countries in the short or even medium term.

(5) The standard contractual clauses are only one of several possibilities under Directive 95/46/EC, together with Article 25 and Article 26(1) and (2), for lawfully transferring personal data to a third country. It will be easier for organisations to transfer personal data to third countries by incorporating the standard contractual clauses in a contract. The standard contractual clauses relate only to data protection. The data exporter and the data importer are free to include any other clauses on business related issues, such as clauses on mutual assistance in cases of disputes with a data subject or a supervisory authority, which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.

(6) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. The circumstances of specific transfers may require that data controllers provide different safeguards within the meaning of Article 26(2). In any case, this Decision only has the effect of requiring the Member States not to refuse to recognise as providing adequate safeguards the contractual clauses described in it and does not therefore have any effect on other contractual clauses.

(7) The scope of this Decision is limited to establishing that the clauses in the Annex may be used by a controller established in the Community in order to adduce sufficient safeguards within the meaning of Article 26(2) of Directive 95/46/EC. The transfer of personal data to third countries is a processing operation in a Member State, the lawfulness of which is subject to national law. The data protection supervisory authorities of the Member States, in the exercise of their functions and powers under Article 28 of Directive 95/46/EC, should remain competent to assess whether the data exporter has complied with national legislation implementing the provisions of Directive 95/46/EC and, in particular, any specific rules as regards the obligation of providing information under that Directive.

(8) This Decision does not cover the transfer of personal data by controllers established in the Community to recipients established outside the territory of the Community who act only as processors. Those transfers do not require the same safeguards because the processor acts exclusively on behalf of the controller. The Commission intends to address that type of transfer in a subsequent decision.

(9) It is appropriate to lay down the minimum information that the parties must specify in the contract dealing with the transfer. Member States should retain the power to particularise the information the parties are required to provide. The operation of this Decision should be reviewed in the light of experience.

(10) The Commission will also consider in the future whether standard contractual clauses submitted by business organisations or other interested parties offer adequate safeguards in accordance with Directive 95/46/EC.

(11) While the parties should be free to agree on the substantive data protection rules to be complied with by the data importer, there are certain data protection principles which should apply in any event.

(12) Data should be processed and subsequently used or further communicated only for specified purposes and should not be kept longer than necessary.

(13) In accordance with Article 12 of Directive 95/46/EC, the data subject should have the right of access to all data relating to him and as appropriate to rectification, erasure or blocking of certain data.

(14) Further transfers of personal data to another controller established in a third country should be permitted only subject to certain conditions, in particular to ensure that data subjects are given proper information and have the opportunity to object, or in certain cases to withold their consent.

(15) In addition to assessing whether transfers to third countries are in accordance with national law, supervisory authorities should play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In specific circumstances, the supervisory authorities of the Member States should retain the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the guarantees providing adequate protection to the data subject.

(16) The standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular, where the data subjects suffer damage as a consequence of a breach of the contract.

(17) The governing law of the contract should be the law of the Member State in which the data exporter is established, enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law.

(18) To reduce practical difficulties which data subjects could experience when trying to enforce their rights under the standard contractual clauses, the data exporter and the data importer should be jointly and severally liable for damages resulting from any violation of those provisions which are covered by the third-party beneficiary clause.

(19) The Data Subject is entitled to take action and receive compensation from the Data Exporter, the Data Importer or from both for any damage resulting from any act incompatible with the obligations contained in the standard contractual clauses. Both parties may be exempted from that liability if they prove that neither of them was responsible.

(20) Joint and several liability does not extend to those provisions not covered by the third-party beneficiary clause and does not need to leave one party paying for the damage resulting from the unlawful processing of the other party. Although mutual indemnification between the parties is not a requirement for the adequacy of the protection for the data subjects and may therefore be deleted, it is included in the standard contractual clauses for the sake of clarification and to avoid the need for the parties to negotiate indemnification clauses individually.

(21) In the event of a dispute between the parties and the data subject which is not amicably resolved and where the data subject invokes the third-party beneficiary clause, the parties agree to provide the data subject with the choice between mediation, arbitration or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation and arbitration. Mediation by the supervisory authorities of a Member State should be an option where they provide such a service.

(22) The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided under the standard contractual clauses annexed to this Decision, which has been taken into account in the preparation of this Decision [1].

(23) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

[1] Opinion No 1/2001 adopted by the Working Party on 26 January 2001 (DG MARKT 5102/00 WP 38), available in the website 'Europa' hosted by the European Commission.

HAS ADOPTED THIS DECISION:

*Article 1*

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 9/46/EC.

*Article 2*

This Decision concerns only the adequacy of protection provided by the standard contractual clauses for the transfer of personal data set out in the Annex. It does not affect the application of other national provisions implementing Directive 95/46/EC that pertain to the processing of personal data within the Member States.

This Decision shall not apply to the transfer of personal data by controllers established in the Community to recipients established outside the territory of the Community who act only as processors.

*Article 3*

For the purposes of this Decision:

(a) the definitions in Directive 95/46/EC shall apply;

(b) 'special categories of data' means the data referred to in Article 8 of that Directive;

(c) 'supervisory authority' means the authority referred to in Article 28 of that Directive;

(d) 'data exporter' means the controller who transfers the personal data;

(e) 'data importer' means the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of this Decision.

*Article 4*

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the relevant data protection rules which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses; or

(b) a competent authority has established that the data importer has not respected the contractual clauses; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuation of transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the prohibition or suspension no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall without delay inform the Commission which will forward the information to the other Member States.

*Article 5*

The Commission shall evaluate the operation of this Decision on the basis of available information three years after its notification to the Member States. It shall submit a report on the endings to the Committee established under Article 31 of Directive 95/46/EC. It shall include any evidence that could affect the evaluation concerning the adequacy of the standard contractual clauses in the Annex and any evidence that this Decision is being applied in a discriminatory way.

*Article 6*

This Decision shall apply from 3 September 2001.

*Article 7*

This Decision is addressed to the Member States.

Done at Brussels, 15 June 2001.

*For the Commission*

Frederik BOLKESTEIN

*Member of the Commission*

*ANNEX*

## STANDARD CONTRACTUAL CLAUSES

**for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection**

**Name of the data exporting organisation:** .....

.....

**Address:** .....

**Tel.** ..... **fax** ..... **e-mail:** .....

**Other information needed to identify the organisation:** .....

('the data **exporter**')

and

**Name of the data importing organisation:** .....

.....

**Address:** .....

**tel.** ..... **fax** ..... **e-mail:** .....

**Other information needed to identify the organisation:** .....

('the data **importer**')

HAVE AGREED on the following contractual clauses ('the Clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1:

*Clause 1*

**Definitions**

For the purposes of the Clauses:

a) '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('hereinafter the Directive');

b) the '**data exporter**' shall mean the controller who transfers the personal data;

c) the '**data importer**' shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection.

*Clause 2*

**Details of the transfer**

The details of the transfer, and in particular the categories of personal data and the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

**Third-party beneficiary clause**

The data subjects can enforce this Clause, Clause 4(b), (c) and (d), Clause 5(a), (b), (c) and (e), Clause 6(1) and (2), and Clauses 7, 9 and 11 as third-party beneficaries. The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

*Clause 4*

**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data by him has been and, up to the moment of the transfer, will continue to be carried out in accordance with the relevant provisions of the Member State in which the data exporter is established (and where applicable has been notified to the relevant authorities of that State) and does not violate the relevant provisions of that State;

(b) that if the transfer involves special categories of data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a third country not providing adequate protection;

(c) to make available to the data subjects upon request a copy of the Clauses; and

(d) to respond in a reasonable time and to the extent reasonably possible to enquries from the supervisory authority on the processing of the relevant personal data by the data importer and to any enquiries from the data subject concerning the processing of this personal data by the data importer.

*Clause 5*

**Obligations of the data importer**

The data importer agrees and warrants:

(a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter and to the supervisory authority where the data exporter is established, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) to process the personal data in accordance with the mandatory data protection principles set out in Appendix 2;
or, if explicitly agreed by the parties by ticking below and subject to compliance with the mandatory data protection principles set out in Appendix 3, to process in all other respects the data in accordance with:

— the relevant provisions of national law (attached to these Clauses) protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data applicable to a data controller in the country in which the data exporter is established, or

— the relevant provisions of any Commission Decision under Article 25(6) of Directive 95/46/EC finding that a third country provides adequate protection in certain sectors of activity only, if the data importer is based in that third country and is not covered by those provisions, in so far as those provisions are of a nature which makes them applicable in the sector of the transfer;

(c) to deal promptly and properly with all reasonable inquiries from the data exporter or the data subject relating to his processing of the personal data subject to the transfer and to cooperate with the competent supervisory authority in the course of all its inquries and abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(d) at the request of the data exporter to submit its data processing facilities for audit which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(e) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints.

*Clause 6*

**Liability**

1. The parties agree that a data subject who has suffered damage as a result of any violation of the provisions referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

2. The data exporter and the data importer agree that they will be jointly and severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data exporter or the data importer or both.

3. The parties agree that if one party is held liable for a violation referred to in paragraph 1 by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. (*).

*Clause 7*

**Mediation and jurisdiction**

1. The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third-party beneficiary provision in clause 3, they accept the decision of the data subject:

(a) to refer the dispute to mediation by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration body, if that party is established in a country which has ratified the New York convention on enforcement of arbitration awards.

3. The parties agree that paragraphs 1 and 2 apply without prejudice to the data subject's substantitve or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

**Cooperation with supervisory authorities**

The parties agree to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under national law.

*Clause 9*

**Termination of the Clauses**

The parties agree that the termination of the Clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the data transferred.

*Clause 10*

**Governing Law**

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established, namely .....

.....

*Clause 11*

**Variation of the contract**

The parties undertake not to vary or modify the terms of the clauses.

**On behalf of the data exporter:**

Name (written out in full): .....

Position: .....

Address: .....

(*) Paragraph 3 is optional.

Other information necessary in order for the contract to be binding (if any): .....

.....

.....
(signature)

(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): .....

.....

.....

.....
(signature)

(stamp of organisation)

*Appendix 1*

**to the standard contractual clauses**

**This Appendix forms part of the Clauses and must be completed and signed by the parties.**

(The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.)

*Data exporter*

The data exporter is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

*Data importer*

The data importer is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

*Data subjects*

The personal data transferred concern the following categories of data subjects (please specify):

.....

.....

.....

*Purposes of the transfer*

The transfer is necessary for the following purposes (please specify):

.....

.....

.....

*Categories of data*

The personal data transferred fall within the following categories of data (please specify):

.....

.....

.....

*Sensitive data* (if appropriate)

The personal data transferred fall within the following categories of sensitive data (please specify):

.....

.....

.....

*Recipients*

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify):

.....

.....

.....

*Storage limit*

The personal data transferred may be stored for no more than (please indicate): ..... (months/years)

| Data exporter | Data importer |
|---|---|
| Name: ..... | Name: ..... |
| ..... (Authorised signature) | ..... (Authorised signature) |

*Appendix 2*

**to the standard contractual clauses**

**Mandatory data protection principles referred to in the first paragraph of Clause 5(b)**

These data protection principles should be read and interpreted in the light of the provisions (principles and relevant exceptions) of Directive 95/46/EC.

They shall apply subject to the mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.

1. *Purpose limitation*: data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. *Data quality and proportionality*: data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. *Transparency*: data subjects must be provided with information as to the purposes of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fair processing, unless such information has already been given by the data exporter.

4. *Security and confidentiality*: technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.

5. *Rights of access, rectification, erasure and blocking of data*: as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data are incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

6. *Restrictions on onwards transfers*: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

   (a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer or, in other cases, have been given the opportunity to object.

   The minimum information to be provided to data subjects must contain in a language understandable to them:

   — the purposes of the onward transfer,

   — the identification of the data exporter established in the Community,

   — the categories of further recipients of the data and the countries of destination, and

   — an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals; or

   (b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

7. *Special categories of data*: where data revealing racial or ehtnic origin, political opinions, religious or philosophical beliefs or trade union memberships and data concerning health or sex life and data relating to offences, criminal convictions or security measures are processed, additional safeguards should be in place within the meaning of Directive 95/46/EC, in particular, appropriate security measures such as strong encryption for transmission or such as keeping a record of access to sensitive data.

8. *Direct marketing*: where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to 'opt-out' from having his data used for such purposes.

9. *Automated individual decisions*: data subjects are entitled not to be subject to a decision which is based soley on automated processing of data, unless other measures are taken to safeguard the individual's legitimate interests as provided for in Article 15(2) of Directive 95/46/EC. Where the purpose of the transfer is the taking of an automated decision as referred to in Article 15 of Directive 95/46/EC, which produces legal effects concerning the individual or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc., the individual should have the right to know the reasoning for this decision.

---

*Appendix 3*

**to the standard contractual clauses**

**Mandatory data protection principles referred to in the second paragraph of Clause 5(b)**

1. *Purpose limitation*: data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. *Rights of access, rectification, erasure and blocking of data*: as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data is incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

3. *Restrictions on onward transfers*: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

   (a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer, or, in other cases, have been given the opportunity to object.

   The minimum information to be provided to data subjects must contain in a language understandable to them:
   — the purposes of the onward transfer,
   — the identification of the data exporter established in the Community,
   — the categories of further recipients of the data and the countries of destination, and
   — an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of indidividuals; or

   (b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

---

# COMMISSION DECISION

## of 27 December 2004

## amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries

*(notified under document number C(2004) 5271)*

**(Text with EEA relevance)**

(2004/915/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1], and in particular Article 26(4) thereof,

Whereas:

(1) In order to facilitate data flows from the Community, it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all Member States under a common set of rules. Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC [2] therefore lays down a model set of standard contractual clauses which ensures adequate safeguards for the transfer of data to third countries.

(2) Much experience has been gained since the adoption of that Decision. In addition, a coalition of business associations [3] has submitted a set of alternative standard contractual clauses designed to provide a level of data protection equivalent to that provided for by the set of standard contractual clauses laid down in Decision 2001/497/EC while making use of different mechanisms.

(3) Since the use of standard contractual clauses for international data transfers is voluntary as standard contractual clauses are only one of several possibilities under Directive 95/46/EC, for lawfully transferring personal data to a third country, data exporters in the Community and data importers in third countries should be free to choose any of the sets of standard contractual clauses, or to choose some other legal basis for data transfer. As each set as a whole forms a model, data exporters should not, however, be allowed to amend these sets or totally or partially merge them in any manner.

(4) The standard contract clauses submitted by the business associations aim at increasing the use of contractual clauses among operators by mechanisms such as more flexible auditing requirements and more detailed rules on the right of access.

(5) Moreover, as an alternative to the system of joint and several liability provided for in Decision 2001/497/EC, the set now submitted contains a liability regime based on due diligence obligations where the data exporter and the data importer would be liable vis-à-vis the data subjects for their respective breach of their contractual obligations; the data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (*culpa in eligendo*) and the data subject can take action against the data exporter in this respect. The enforcement of clause I(b) of the new set of standard contractual clauses is of particular importance in this regard, in particular in connection with the possibility for the data exporter to carry out audits on the data importers' premises or to request evidence of sufficient financial resources to fulfil its responsibilities.

[1] OJ L 281, 23.11.95, p. 31. Directive as amended by Regulation (EC) No 1883/2003 (OJ L 284, 31.10.2003, p. 1).

[2] OJ L 181, 4.7.2001, p. 19.

[3] The International Chamber of Commerce (ICC), Japan Business Council in Europe (JBCE), European Information and Communications Technology Association (EICTA), EU Committee of the American Chamber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) and the Federation of European Direct Marketing Associations (FEDMA).

(6) As regards the exercise of third party beneficiary rights by the data subjects, greater involvement of the data exporter in the resolution of data subjects' complaints is provided for, with the data exporter being obliged to make contact with the data importer and, if necessary, enforce the contract within the normal period of one month. If the data exporter refused to enforce the contract and the breach by the data importer still continues, the data subject may then enforce the clauses against the data importer and eventually sue him in a Member State. This acceptance of jurisdiction and the agreement to comply with a decision of a competent court or data protection authority does not prejudice any procedural rights of data importers established in third countries, such as rights of appeal.

(7) In order, however, to prevent abuses with this additional flexibility, it is appropriate to provide that data protection authorities can more easily prohibit or suspend data transfers based on the new set of standard contractual clauses in those cases where the data exporter refuses to take appropriate steps to enforce contractual obligations against the data importer or the latter refuses to cooperate in good faith with competent supervisory data protection authorities.

(8) The use of standard contractual clauses will be made without prejudice to the application of national provisions adopted pursuant to Directive 95/46/EC or to Directive 2002//58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [1], in particular as far as the sending of commercial communications for the purposes of direct marketing is concerned.

(9) On that basis, the safeguards contained in the submitted standard contractual clauses can be considered as adequate within the meaning of Article 26(2) of Directive 95/46/EC.

(10) The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered an opinion [2] on the level of protection provided under the submitted standard contractual clauses which has been taken into account.

(11) In order to assess the operation of the amendments to Decision 2001/497/EC, it is appropriate that the Commission evaluates them three years after their notification to the Member States

(12) Decision 2001/497/EC should be amended accordingly.

(13) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

*Article 1*

Decision 2001/497/EC is amended as follows:

1. In Article 1 the following paragraph is added:

'Data controllers may choose either of the sets I or II in the Annex. However, they may not amend the clauses nor combine individual clauses or the sets.'

2. In Article 4 paragraphs 2 and 3 are replaced by the following:

'2. For the purposes of paragraph 1, where the data controller adduces adequate safeguards on the basis of the standard contractual clauses contained in set II in the Annex, the competent data protection authorities are entitled to exercise their existing powers to prohibit or suspend data flows in either of the following cases:

(a) refusal of the data importer to cooperate in good faith with the data protection authorities, or to comply with their clear obligations under the contract;

(b) refusal of the data exporter to take appropriate steps to enforce the contract against the data importer within the normal period of one month after notice by the competent data protection authority to the data exporter.

[1] OJ L 201, 31.7.2002, p. 37.
[2] Opinion No 8/2003, available at: http://europa.eu.int/comm/privacy

For the purposes of the first subparagraph, refusal in bad faith or refusal to enforce the contract by the data importer shall not include cases in which cooperation or enforcement would conflict with mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, in particular sanctions as laid down in international and/or national instruments, tax-reporting requirements or anti-money-laundering reporting requirements.

For the purposes of point (a) of the first subparagraph co-operation may include, in particular, the submission of the data importer's data processing facilities for audit or the obligation to abide by the advice of the data protection supervisory authority in the Community.

3. The prohibition or suspension pursuant to paragraphs 1 and 2 shall be lifted as soon as the reasons for the prohibition or suspension no longer exist.

4. When Member States adopt measures pursuant to paragraphs 1, 2 and 3, they shall without delay inform the Commission which will forward the information to the other Member States.'.

3. In Article 5 the first sentence is replaced by the following:

'The Commission shall evaluate the operation of this Decision on the basis of available information three years after its notification and the notification of any amendment thereto to the Member States.'.

4. The Annex is amended as follows:

1. After the title the term 'SET I' is inserted.

2. The text set out in the Annex to this Decision is added.

*Article 2*

This Decision shall apply from 1 April 2005.

*Article 3*

This Decision is addressed to the Member States.

Done at Brussels, 27 December 2004.

*For the Commission*
Charlie McCREEVY
*Member of the Commission*

*ANNEX*

**'SET II**

**Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)**

*Data transfer agreement*

between

_____ (name)

_____ (address and country of establishment)

hereinafter "data exporter")

and

_____ (name)

_____ (address and country of establishment)

hereinafter "data importer"

each a "party"; together "the parties".

**Definitions**

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. **Obligations of the data exporter**

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. **Obligations of the data importer**

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions [1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data [2], or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: _____

Initials of data importer: _____;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. **Liability and third party rights**

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

IV. **Law applicable to the clauses**

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. **Resolution of disputes with data subjects or the authority**

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. **Termination**

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. **Variation of these clauses**

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. **Description of the Transfer**

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: _____

| | |
|---|---|
| _____ | _____ |
| FOR DATA IMPORTER | FOR DATA EXPORTER |
| ..... | ..... |
| ..... | ..... |
| ..... | ..... |

*ANNEX A*

**DATA PROCESSING PRINCIPLES**

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

*ANNEX B*

**DESCRIPTION OF THE TRANSFER**

*(To be completed by the parties)*

**Data subjects**

The personal data transferred concern the following categories of data subjects:

.....

.....

.....

.....

**Purposes of the transfer(s)**

The transfer is made for the following purposes:

.....

.....

.....

.....

**Categories of data**

The personal data transferred concern the following categories of data:

.....

.....

.....

.....

**Recipients**

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

.....

.....

.....

**Sensitive data** (if appropriate)

The personal data transferred concern the following categories of sensitive data:

.....

.....

.....

.....

**Data protection registration information of data exporter** (where applicable)

.....

.....

**Additional useful information** (storage limits and other relevant information)

.....

.....

**Contact points for data protection enquiries**

| **Data importer** | **Data exporter** |
|---|---|
| ..... | ..... |
| ..... | ..... |
| ..... | ..... |

**ILLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)**

*Indemnification between the data exporter and data importer:*

"The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.".

*Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause):*

"In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be [ ]. The number of arbitrators shall be [ ]."

*Allocation of costs:*

"Each party shall perform its obligations under these clauses at its own cost."

*Extra termination clause:*

"In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter's choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours." '.

# COMMISSION DECISION

## of 5 February 2010

## on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

*(notified under document C(2010) 593)*

**(Text with EEA relevance)**

(2010/87/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1], and in particular Article 26(4) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on the protection of individuals with regard to the processing of personal data established under that Directive has issued guidelines to aid with the assessment.

(4) Standard contractual clauses should relate only to data protection. Therefore, the data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.

(5) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision should only have the effect of requiring the Member States not to refuse to recognise, as providing adequate safeguards, the standard contractual clauses set out in it and should not therefore have any effect on other contractual clauses.

(6) Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC [2] was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection.

(7) Much experience has been gained since the adoption of Decision 2002/16/EC. In addition, the report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries [3] has shown that there is an increasing interest in promoting the use of the standard contractual clauses for international transfers of personal data to third countries not providing an adequate level of protection. In addition, stakeholders have submitted proposals with a view to updating the standard contractual clauses set out in Decision 2002/16/EC in order to take account of the rapidly expanding scope of data-processing activities in the world and to address some issues that were not covered by that Decision [4].

[1] OJ L 281, 23.11.1995, p. 31.

[2] OJ L 6, 10.1.2002, p. 52.

[3] SEC(2006) 95, 20.1.2006.

[4] The International Chamber of Commerce (ICC), Japan Business Council in Europe (JBCE), EU Committee of the American Chamber of Commerce in Belgium (Amcham), and the Federation of European Direct Marketing Associations (FEDMA).

(8) The scope of this Decision should be limited to establishing that the clauses which it sets out may be used by a data controller established in the European Union in order to adduce adequate safeguards within the meaning of Article 26(2) of Directive 95/46/EC for the transfer of personal data to a processor established in a third country.

(9) This Decision should not apply to the transfer of personal data by controllers established in the European Union to controllers established outside the European Union which fall within the scope of Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [1].

(10) This Decision should implement the obligation provided for in Article 17(3) of Directive 95/46/EC and should not prejudice the content of the contracts or legal acts established pursuant to that provision. However, some of the standard contractual clauses, in particular as regards the data exporter's obligations, should be included in order to increase clarity as to the provisions which may be contained in a contract between a controller and a processor.

(11) Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.

(12) Standard contractual clauses should provide for the technical and organisational security measures to be applied by data processors established in a third country not providing adequate protection, in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

(13) In order to facilitate data flows from the European Union, it is desirable for processors providing data-processing services to several data controllers in the European Union to be allowed to apply the same technical and organisational security measures irrespective of the Member State from which the data transfer originates, in particular in those cases where the data importer receives data for further processing from different establishments of the data exporter in the European Union, in which case the law of the designated Member State of establishment should apply.

(14) It is appropriate to lay down the minimum information that the parties should specify in the contract dealing with the transfer. Member States should retain the power to particularise the information the parties are required to provide. The operation of this Decision should be reviewed in the light of experience.

(15) The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party without the prior written consent of the data exporter. The data exporter should instruct the data importer throughout the duration of the data-processing services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses.

(16) The report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries recommended the establishment of appropriate standard contractual clauses on subsequent onwards transfers from a data processor established in a third country to another data processor (sub-processing), in order to take account of business trends and practices for more and more globalised processing activity.

[1] OJ L 181, 4.7.2001, p. 19.

(17) This Decision should contain specific standard contractual clauses on the sub-processing by a data processor established in a third country (the data importer) of his processing services to other processors (sub-processors) established in third countries. In addition, this Decision should set out the conditions that the sub-processing should fulfil to ensure that the personal data being transferred continue to be protected notwithstanding the subsequent transfer to a sub-processor.

(18) In addition, the sub-processing should only consist of the operations agreed in the contract between the data exporter and the data importer incorporating the standard contractual clauses provided for in this Decision and should not refer to different processing operations or purposes so that the purpose limitation principle set out by Directive 95/46/EC is respected. Moreover, where the sub-processor fails to fulfil his own data-processing obligations under the contract, the data importer should remain liable toward the data exporter. The transfer of personal data to processors established outside the European Union should not prejudice the fact that the processing activities should be governed by the applicable data protection law.

(19) Standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract.

(20) The data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action, and, where appropriate, receive compensation from the data importer in those cases, arising out of a breach by the data importer or any sub-processor under it of any of its obligations referred to in the paragraph 2 of Clause 3, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent. Exceptionally, the data subject should be also entitled to take action, and, where appropriate, receive compensation from a sub-processor in those situations where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent. Such third-party liability of the sub-processor should be limited to its own processing operations under the contractual clauses.

(21) In the event of a dispute between a data subject, who invokes the third-party beneficiary clause, and the data importer, which is not amicably resolved, the data importer should offer the data subject a choice between mediation or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation. Mediation by the data protection supervisory authorities of the Member State in which the data exporter is established should be an option where they provide such a service.

(22) The contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law. The same law should also govern the provisions on data protection of any contract with a sub-processor for the sub-processing of the processing activities of the personal data transferred by the data exporter to the data importer under the contractual clauses.

(23) Since this Decision applies only to subcontracting by a data processor established in a third country of his processing services to a sub-processor established in a third country, it should not apply to the situation by which a processor established in the European Union and performing the processing of personal data on behalf of a controller established in the European Union subcontracts his processing operations to a sub-processor established in a third country. In such situations, Member States are free whether to take account of the fact that the principles and safeguards of the standard contractual clauses set out in this Decision have been used to subcontract to a sub-processor established in a third country with the intention of providing adequate protection for the rights of data subjects whose personal data are being transferred for sub-processing operations.

(24) The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided under the standard contractual clauses annexed to this Decision, which has been taken into account in the preparation of this Decision.

(25) Decision 2002/16/EC should be repealed.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

*Article 1*

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC.

*Article 2*

This Decision concerns only the adequacy of protection provided by the standard contractual clauses set out in the Annex for the transfer of personal data to processors. It does not affect the application of other national provisions implementing Directive 95/46/EC that pertain to the processing of personal data within the Member States.

This Decision shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as processors.

*Article 3*

For the purposes of this Decision the following definitions shall apply:

(a) 'special categories of data' means the data referred to in Article 8 of Directive 95/46/EC;

(b) 'supervisory authority' means the authority referred to in Article 28 of Directive 95/46/EC;

(c) 'data exporter' means the controller who transfers the personal data;

(d) 'data importer' means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(e) 'sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer and who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for the processing activities to be carried out on behalf of the data exporter after the transfer in accordance with the data exporter's instructions, the standard contractual clauses set out in the Annex, and the terms of the written contract for sub-processing;

(f) 'applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(g) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Article 4*

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.

*Article 5*

The Commission shall evaluate the operation of this Decision on the basis of available information three years after its adoption. It shall submit a report on the findings to the Committee established under Article 31 of Directive 95/46/EC. It shall include any evidence that could affect the evaluation concerning the adequacy of the standard contractual clauses in the Annex and any evidence that this Decision is being applied in a discriminatory way.

*Article 6*

This Decision shall apply from 15 May 2010.

*Article 7*

1. Decision 2002/16/EC is repealed with effect from 15 May 2010.

2. A contract concluded between a data exporter and a data importer pursuant to Decision 2002/16/EC before 15 May 2010 shall remain in force and effect for as long as the transfers and data-processing operations that are the subject matter of the contract remain unchanged and personal data covered by this Decision continue to be transferred between the parties. Where contracting parties decide to make changes in this regard or subcontract the processing operations that are the subject matter of the contract they shall be required to enter into a new contract which shall comply with the standard contractual clauses set out in the Annex.

*Article 8*

This Decision is addressed to the Member States.

Done at Brussels, 5 February 2010.

*For the Commission*

Jacques BARROT

*Vice-President*

*ANNEX*

**STANDARD CONTRACTUAL CLAUSES (PROCESSORS)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation:

.....

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

**Definitions**

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

**Obligations of the data importer** [1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

**Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

*Clause 7*

**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

*Clause 9*

**Governing law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely .....

*Clause 10*

**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

**Sub-processing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [1]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....

[1] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

**Obligation after the termination of personal data-processing services**

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

*Appendix 1*

**to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

.....

.....

.....

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

.....

.....

.....

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

.....

.....

.....

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

.....

.....

.....

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

.....

.....

.....

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: .....

Authorised Signature .....

*Appendix 2*

**to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

.....

.....

.....

.....

**ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)**

**Liability**

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim [1].

[1] Paragraph on liabilities is optional.

# Assessing Adequacy

# International data transfers

## Data Protection Act

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of DPA can be found in The Guide to Data Protection. This is part of a series of guidance, which goes into more detail than the Guide to DPA, to help you to fully understand your obligations, as well as promoting good practice.

This guidance explains how a data controller should carry out an assessment of the adequacy of the protection available in respect of his proposed transfer of personal data outside the EEA.

## Overview

A data controller may only transfer personal data outside the EEA to a country whose data protection laws have not been approved by the European Commission as providing adequate protection for data subjects' rights if there is an adequate level of protection for the rights of data subjects.

The adequacy of the level of protection associated with a particular transfer may be ensured in a number of ways. The data controller may:

- carry out his own assessment of the adequacy of the protection;
- use contracts to ensure adequacy;
- obtain Commission approval for a set of Binding Corporate Rules governing intra-group data transfers; or
- rely on one of the exceptions to the prohibitions on transfers of personal data outside the EEA.

This guidance considers how a data controller may carry out his own assessment of the adequacy of the protection available in respect of

a particular proposed transfer of personal data outside the EEA.

## What the DPA says

The eighth data protection principle provides that:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data"
>
> (Part 1 of Schedule 1 to the DPA).

If you decide you need to transfer personal data outside the EEA, and the recipient is not in a country subject to a positive finding of adequacy by the Commission, nor signed up to the Safe Harbor Scheme, you will need to:

- conduct a risk assessment into whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects; or
- if you do not find there is an adequate level of protection, put in place adequate safeguards to protect the rights of the data subjects, possibly using Model Contract Clauses or Binding Corporate Rules; or
- consider using one of the other statutory exceptions to the Eighth Principle restriction on international transfers of personal data.

This paper provides advice on the first of these options - assessing whether there is an adequate level of protection for a proposed transfer of personal data.

## Adequacy criteria

The Data Protection Act (Schedule 1, Part II paragraph 13) provides that, when considering whether there is 'an adequate level of protection' for the purposes of the eighth principle, the level of protection must be one which is "adequate in all the circumstances of the case". In addition, in assessing adequacy, particular consideration should be given to specific listed criteria. For ease of reference these criteria may be divided into two groups; 'general adequacy criteria' and 'legal adequacy criteria'.

If an assessment of the 'general adequacy criteria' has revealed that, in the particular circumstances of the case, the risk to the rights of data subjects associated with the transfer is low, an exhaustive analysis of the 'legal adequacy criteria' may not be necessary. If a high risk is identified (e.g. if the data is particularly sensitive) then a more comprehensive investigation of the legal adequacy criteria will be required.

## General adequacy criteria

- The nature of the personal data

  The transfer of some types of personal data will pose little risk to the rights and freedoms of individuals (e.g. the transfer of a list of internal telephone extensions to overseas subsidiaries of a multinational company would not be considered to be high risk as it is unlikely that a data subject would suffer significant damage if his business telephone number was obtained by an unauthorised recipient). Conversely, if a data exporting controller is proposing a transfer of sensitive personal data (e.g. health records) the level of protection required for the data (and the rights of the data subjects) will clearly be higher.

- The purposes for which the data are intended to be processed

  Some purposes for which data are processed will carry greater risks to the rights of the individuals than others. For example, if the data are to be processed for internal company or group purposes only (such as the internal company telephone list as described above) the transfer of such data may involve less risk to the rights of the data subjects than if the data transferred is to be distributed more widely (e.g. customer contact details to be used in marketing or on an internet site).

- The period during which the data are intended to be processed

  If the data are only to be processed once or for a short period of time and then destroyed, the risks arising from any lack of protection for data subjects' rights may be less than if the data are to be processed on a long-term basis. However, that is not to say that one-off transfers may be carried out without putting appropriate protection in place. It merely means that the data protection arrangements (such as regular reporting on security arrangements or security audits) may be less onerous n relation to such transfers or indeed may not be required at all.

- The country or territory of origin of the information contained in the data

  Consideration must be given to the country of territory from which the information originates (note that this is not necessarily the same as the country or territory from which the data is to be transferred). Where information has been obtained in a third country (i.e. outside the EEA) this will be a relevant factor as the data subjects may have different expectations as to the level of protection that will be afforded to their data than if the information been obtained in the EEA.

  Where the country (or territory) of origin of the information is outside the EEA it is important to remember that the DPA is not intended to provide a different level of protection for the data subjects rights than that provided by the data protection regime, if any, in the non-EEA country of origin.

- The country or territory of final destination of the information

  Transfers may be made in several stages involving transfers to one, then another, and then another country. Where it is known that there will be a further transfer to another country or territory, the level of protection given in the country of final destination will be relevant in assessing the adequacy of the protection associated with the transfer.

- Any security measures taken in respect of the data in the country or territory of destination

  Organisations exporting data may be able to ensure that the personal data are protected by means of technical measures (such as encryption or the adoption of information security management practices such as those in ISO27001/ISO27002. In practice, security is often a key factor in the commercial considerations of the parties.

## Legal adequacy criteria

It will not always be necessary to carry out a detailed consideration of the legal adequacy criteria where consideration of the general adequacy criteria indicates that the risk to the rights of data subjects associated with the proposed data transfer is low. Where consideration of the general adequacy criteria indicates a higher risk, the legal adequacy criteria come into play. For example, where the exporting data controller is proposing to set up a permanent

operation in a third country and anticipates making regular, large-scale transfers to that country.

To make a legal adequacy assessment, consider the following:

- The law in force in the country or territory in question

  Consider whether the third country:

  - Has a data protection regime in place which meets the standards set out in the Article 29 Working Party document adopted on 24 July 1998 (WP 12).

  - Has any legal framework for the protection of the rights and freedoms of individuals generally.

  - Recognises the general rule of law and, in particular, the ability of parties to contract and bind themselves under contracts.

- The international obligations of the recipient country or territory

  Consider whether the third country has:

  - Adopted the OECD Guidelines[1] and put in place appropriate measures to implement the Guidelines.

  - Ratified Convention 108[2] and established appropriate mechanisms for compliance with the Convention.

- The rules or codes of practice which govern the processing of personal data in the third country.

  Consider whether the recipient country has in place any relevant codes of conduct or other rules (general or sectoral) enforceable in that country or territory (whether generally or by special arrangement in particular cases).

## Can the transfer proceed?

[1] 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' – Organisation for Economic Co-operation and Development, 1980
[2] Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, Strasbourg 1981

If adequacy is established further to your adequacy assessment, then the transfer can proceed from the UK to the third country in compliance with the eighth principle.

If transfers are taking place from more than one European jurisdiction then local advice should always be sought as there may be different requirements which apply depending on the jurisdictions in question.

If adequacy cannot be established it may be possible to put in place adequate safeguards or use one of the other exceptions to the Eighth Principle as discussed on the ICO International Transfers web page Can I Send Personal Data Overseas?

## Other considerations

Carrying our an assessment of the adequacy of the level of protection for the rights of data subjects is only one method of ensuring a transfer of personal data outside the EEA complies with the Directive.

Guidance on other transfer arrangements is available:

- Using Standard Contractual Terms (Model Contract Clauses)
- Binding Corporate Rules
- International outsourcing arrangements

## More Information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please Contact us: see our website www.ico.gov.uk.

ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 245

# EU-US PRIVACY SHIELD
# F.A.Q. FOR EUROPEAN BUSINESSES

**Adopted on 13 December 2016**

**EU-US PRIVACY SHIELD**
**F.A.Q. FOR EUROPEAN BUSINESSES**

Q1. **What is the EU-U.S. Privacy Shield?**

Q2. **Which US companies are eligible to the EU-U.S. Privacy Shield?**

Q3. **What to do before transferring personal data to an U.S. based company which is or claims to be Privacy Shield certified?**

Q4. **Where can I find guidance regarding the registration of U.S. subsidiary companies of European businesses?**

## Q1. What is the EU-U.S. Privacy Shield?

The EU-U.S. Privacy Shield[1] is a self-certification mechanism for U.S. based companies that has been recognized by the European Commission as providing an adequate level of protection for personal data transferred from an EU entity to U.S. based self-certified companies and thus as an element for offering legal guarantees for such data transfers.
Here are some relevant links for more information:

- The Adequacy decision as published in the official Journal of the EU
- The Guide to the EU-US Privacy Shield developed by the European Commission
- The Privacy Shield program website as administrated by the US Department of Commerce.

## Q2. Which US companies are eligible to the EU-U.S. Privacy Shield?

In order to be entitled to self-certify to the Privacy Shield, an U.S. based company must be subject to the investigatory and enforcement powers of the Federal Trade Commission ("FTC") or of the Department of Transportation ("DoT"). Other U.S. statutory bodies may be included in the future.

This means that, for example, non-profit organizations, banks, business of insurances and telecommunication service providers (with regard to common carrier activities) do not fall under the jurisdiction of the FTC or DoT and therefore cannot self-certify under the Privacy Shield.

The Privacy Shield applies to any type of personal data transferred from an EU entity to the US including commercial, health or human resource related data, as long as the recipient US Company has self-certified to the Framework.
You might find additional information on https://www.privacyshield.gov/

[1] The decision on the adequacy of the EU-U.S. Privacy Shield Framework ("Privacy Shield") or ("Framework") was adopted by the European Commission on July 12, 2016. It was designed by the European Commission and the U.S. Department of Commerce to replace the Safe-Harbor-Decision 2000/520/EC which were declared invalid by the European Court of Justice in 6 October 2015.

**Q3. What to do before transferring personal data to a U.S. based company which is or claims to be Privacy Shield certified?**

Before transferring personal data to a U.S. based company which claims to be Privacy Shield certified, European businesses also have to ascertain that the U.S. based company holds an active certification (certifications need to be renewed annually) and that the certification covers the data in question (in particular: HR data, respectively, Non-HR data).

To verify whether or not a certification is active and applicable, European companies need to consult the Privacy Shield List, published on the U.S. Department of Commerce's website (https://www.privacyshield.gov/welcome).

All U.S. based companies having successfully completed the self-certification process are listed. The Privacy Shield List also provides information on the types of personal data a U.S. based company has certified for (HR or non-HR data) and provides details on the services it offers.

The US Department of Commerce is also listing companies that are no longer members of the Privacy Shield. Those companies are not allowed to receive personal data of EU individuals under the Privacy Shield after the end of their participation, but have to continue to apply the Privacy Shield principles to data transferred while their participation was active.
For the transfer of personal data to companies that are not or no longer members of the Privacy Shield, other EU approved transfer mechanisms such as Binding Corporate Rules, Standard Contractual Clauses, may be used for the transfer of personal data of EU individuals to U.S. based businesses.

The fact that the recipient in US is member of the EU-US privacy Shield will enable European businesses to comply with the national laws implementing article 25 of the EC Directive 95/46, but all other requirements as set up by the national data protection law remain applicable;

- For transfers to U.S. based company acting as controller

Before transferring personal data, European businesses acting as Controllers need to ensure compliance of the transfer with applicable data protection law. In the first step, European businesses can only share personal data with a U.S. based company if the transfer will benefit from a legal basis (i.e. if it complies with national law implementing articles 7 and 8 of the EC Directive 95/46/EC). Moreover, all other general requirements from EU data protection law towards the data transfer/s need to be met (e.g. purpose limitation, proportionality, quality, information obligations towards data subjects). If data is to be transferred to a certified U.S. based company, the European business transferring the data also needs to inform the data subjects about the identity of the recipients of their data and about the fact that the data benefits from protection by the Privacy Shield.
European businesses should take note that commercial contractual clauses (e.g. with their business partners) could restrict them in their possibilities to transfer personal data to other businesses outside the EU or EEA.

- For transfers to U.S. based company acting as processor

When a European based company acting as data controller transfers data to a U.S. based data processor, acting on its behalf for processing purposes only (storage, IT maintenance, helpdesk etc.), according to Art. 17 of EC Directive 95/46/EC the two companies are obliged to conclude a data processing contract regardless of whether the data processor is a member of the Privacy Shield or not.

The conclusion of a contract is required in order to ensure that the U.S. data processor commits to:

- act only on instructions received from the data controller;

- provide appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed[2]. Having regard to the state of the art and the cost of their implementation, such security measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. ; and

- by taking into account the nature of the processing, assists the controller in responding to individuals exercising their right to access their personal data.

Please note that under the EU Data Protection Directive national, data protection law may impose additional requirements, for example require EU businesses to include additional content into their data processing contracts. Your national Data Protection Authority can provide you with further guidance.

For instance, it is advisable that the EU Business indicates if it agrees or not that the US processor may sub process the personal information to third party processors and the applicable conditions (in terms of transparency, liability). Moreover, it might also be useful for the EU Business to get assurance about the notification of security breaches and commitments about deletion of the data once the service contract is terminated.

**Q4. Where can I find guidance regarding the registration of US subsidiary companies of European businesses?**

For information on the registration of US subsidiary companies of European businesses in the Privacy Shield, please visit the U.S. Department of Commerce corresponding webpage: (https://www.privacyshield.gov/article?id=U-S-Subsidiaries-of-European-Businesses-Participation-in-Privacy-Shield ).

Registration to the Privacy Shield is available on the U.S. Department of Commerce website (https://www.privacyshield.gov/welcome ).

[2] For more information on onward transfers by U.S. based data processors, please visit the section "*Obligatory Contracts for Onward Transfers*" of the Privacy Shield and see Question 4.

A guide to the self-certification process, is also provided thereby: (https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 ).

In any case, data protection principles applying under the Privacy Shield Framework will have to be complied with by the US self-certified entity.

ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 246

# EU-US PRIVACY SHIELD
# F.A.Q. FOR EUROPEAN INDIVIDUALS

**Adopted on 13 December 2016**

**EU-US PRIVACY SHIELD**
**F.A.Q. FOR EUROPEAN INDIVIDUALS**[1]

## What is the Privacy Shield?

The Privacy Shield[2] is a self-certification mechanism for US based companies. This framework has been recognized by the European Commission as providing an adequate level of protection for personal data transferred from an EU entity to US based companies and thus as an element for offering legal guarantees for such data transfers.

The EU-US Privacy Shield mechanism is in full effect since the 1st of August 2016.

The Privacy Shield applies to any type of personal data transferred from an EU entity to the US including commercial, health or human resource related data, as long as the recipient US company has self-certified to the Framework.

## How do I benefit from the Privacy Shield?

The Privacy Shield relies on commitments taken by US companies to respect the principles, rules and obligations laid out by the Privacy Shield framework.

This framework grants you a certain number of rights when your personal data have been transferred from an EU entity to the US. Notably, you have the right to be informed of such transfer and to exercise your rights of access, for example of correction and of deletion of your personal data transferred[3]. You can verify whether a US based company has certified by checking the online Privacy Shield list, available here: www.privacyshield.gov.

It is encouraged to address possible queries regarding the processing of your data to the US company, first.

If your concern has not been resolved by the Privacy Shield company or you have reasons to not address it directly, your national data protection authority will stand ready to help you to resolve the matter.

## How do I lodge a complaint?

In case you think that the US Privacy-Shield company has violated its obligations stemming from the EU-US Privacy Shield Framework or has violated the rights entitled to you under the Privacy shield principles, you can complain about it.

---

[1] In this context, European individuals means any natural person, regardless of his/her nationality, whose personal data have been transferred to a US company under the EU-US Privacy Shield.

[2] The decision on the adequacy of the EU-U.S. Privacy Shield Framework ("Privacy Shield") or ("Framework") was adopted by the European Commission on July 12, 2016. It was designed by the European Commission and the U.S. Department of Commerce to replace the Safe-Harbor-Decision 2000/520/EC which were declared invalid by the European Court of Justice in 6 October 2015.

[3] For more detailed information as to the guarantees for the data transferred and as to your rights under the EU-U.S. Privacy Shield, please consult the Guide to the EU-US Privacy Shield published by the European Commission.

If you want to lodge a complaint regarding an US Privacy Shield certified company, or a company that claims to have been certified, please use the common complaint form available here (soon available) or contact your national DPA[4]. Please provide your national DPA with as many details on the matter as possible, enabling your DPA to handle your complaint in the best way.

An informal panel of EU DPAs will be set up in order to handle complaints concerning human resources personal data transferred from an EU entity to an US Privacy Shield company in the context of employment relationship, or when the US recipient company has voluntarily chosen to commit to cooperate with the EU DPAs.
The informal panel of EU DPAs will launch an investigation during which both parties will have the possibility to express their views. If necessary in order to resolve the case, the informal panel can issue an "advice" which is a binding decision that the US Privacy Shield company will have to comply with.

Where the informal panel of EU DPAs is not competent, EU DPAs have the possibility to refer the complaint to US authorities (notably, the FTC committed to give priority consideration to those referrals and the DoC has a clear deadline to act on complaints). In any cases, depending on the circumstances of the case, the competent national DPA may also directly exercise its powers (such as prohibition or suspension of data transfers) toward the EU data exporter.

For getting more information about the possibility to lodge a complaint, you may ask further information to your national data protection authority.
The data protection authorities are currently developing a common complaint form that may be used by EU individuals to submit a complaint. The complaint form will be provided as soon as possible. The complaint form will be optional, so you can lodge a complaint already by contacting your national DPA.

*Please note that requests relating to* ***access by US public authorities for intelligence activities*** *are subject to another procedure. Please contact your national DPA for more information.*

[4] Whenever the words "national data protection authority", "EU DPA" or "EU handling authority", this also refers to the EDPS, which will be the EU handling authority in case where your personal data have been transferred to an US Privacy Shield certified company by an EU institution.

# The eighth data protection principle and international data transfers

## Data Protection Act

## Contents

# Introduction

1. The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. Except to the extent that a data controller is able to claim an exemption from any of the principles they will apply to all personal data processed by a data controller. The principles are set out in Schedule 1 to the DPA.

2. An overview of all of the Principles and the main provisions of the DPA can be found in The Guide to Data Protection.

3. This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers to fully understand their obligations and promote good practice.

4. This guidance considers the provisions of the eighth data protection principle (the eighth principle) of the DPA relating to international transfers of personal data[1] made by a data controller based in the UK to recipients based outside the European Economic Area (see 'What does the DPA say?' below). Where transfers outside of the EEA originate from other European Member States, the advice and guidance of the relevant data protection authority ('DP authority') in those countries should always be sought as the implementation of the Directive and its interpretation by these other DP authorities varies.

5. The views of the Information Commissioner (the Commissioner) are informed by continuing discussions with international businesses, fellow EU Data Protection Commissioners and non-EU authorities. This guidance and the Commissioner's website will be amended from time to time to reflect any developments in this area including any future Community findings as to which countries give adequate protection for the purposes of the eighth principle.

6. To the extent that the Commissioner is required to examine any transfer in the context of the eighth principle, she will expect to see evidence that the data controller making the

[1] Definitions of the key terms in the Data Protection Act 1998 (the DPA) can be found in the Key Definitions section of The Guide to Data Protection.

transfer has followed the approach and the various criteria set out in this guidance.

7. This guidance is concerned only with the eighth principle but it should be remembered that data controllers transferring personal data are required to comply with the principles and the DPA as a whole.

8. In addition, before making a transfer of personal data, a data controller should consider whether it is possible for it to achieve its objectives without processing personal data at all and examine options such as the anonymisation of such data. If the data does not relate to identifiable individuals then this brings such data outside the scope of the DPA and means that any transfer could be made freely and without reference to the eighth principle.

## More information

10. Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

11. This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Commissioner, Tribunals and courts.

12. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

13. If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.

# Overview

- The structure of this guidance follows the Commissioner's good practice approach to transfers of personal data outside of the EEA. Namely:
    - Step 1 – consider whether there will be a transfer of personal data to a third country;
    - Step 2 - consider whether the third country and the circumstances surrounding the transfer ensure that an adequate level of protection will be given to that data;
    - Step 3 - consider whether the parties have or can put into place adequate safeguards to protect that data (for instance, by entering into model clauses or establishing binding corporate rules); and
    - Step 4 - consider if any of the other derogations to the eighth principle specified in the DPA apply (such as the consent of the data subject to the transfer).
- In addition, section 5 expands on some of these issues in the context of international outsourcing to data processors and its interaction with the eighth principle.

# Step 1 – Will there be a transfer of personal data to a third country?

## What does the DPA say?

14. The eighth principle provides that:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data"[2]

15. The European Economic Area (the EEA) consists of the EU Member States together with Iceland, Liechtenstein and Norway. Any other country or territory is considered to be a 'third country' for the purposes of the eighth principle.

## The Directive

16. The eighth principle is derived from a requirement in the European Communities Directive 95/46/EC (the Directive) on the protection of individuals with regard to the processing of personal data and the free movement of such data. Article 25(1) of the Directive, requires that:

> "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if …the third country in question ensures an adequate level of protection."

## Are all international movements of data covered? Transfer or transit?

17. Once it has been established that it will be necessary to process personal data and that it will be going out of the EEA to a third

[2] Part 1, Schedule 1 to the DPA.

country, the next question to ask is whether this movement of data represents a 'transfer' for the purposes of the eighth principle.

18. The DPA does not define 'transfer' but the ordinary meaning of the word is transmission from one place, person, etc to another. Transfer does not mean the same as mere transit. Therefore the fact that the electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country does not bring such transfer within the scope of the eighth principle.

19. Section 1(3) of the DPA requires that the transfer of information which is not initially personal data but is intended to be processed automatically or as part of a 'relevant filing system'[3] only after it has been transferred should be afforded the protection of the DPA. An example of this would be where information is provided by someone in the UK over the telephone to someone in a third country who then enters the information on a computer.

20. In the case of Bodil Lindqvist v Kammaraklagaren (2003) (Case C-101/01), the European Court of Justice held that there was no transfer of personal data to a third country where an individual loaded personal data onto an internet page in a Member State using an internet hosting provider in that Member State, even though the page was accessible via the internet by people based in a third country. Instead, a transfer was only deemed to have taken place where the internet page was actually accessed by a person located in a third country.

21. In practice, a data controller often uploads data to the internet in order to make it accessible to people in third countries. When the data is accessed in a third country, it is likely that an international transfer of data will have taken place and this would need to be carried out in compliance with the requirements of the DPA.

22. However, in situations where there is no intention to transfer the data to a third country and no transfer is deemed to have taken place as the information has not been accessed in a third country (ie the eighth principle does not apply), data controllers will still need to ensure that the processing complies with all of

[3] Section 1(1) of the DPA. Further guidance on the definition of relevant filing systems is available in the Key Definitions section of The Guide to Data Protection.

the other principles. In particular, data controllers must consider the requirement in the first data protection principle that the processing must be fair which may be contravened by making the data so widely accessible.

# Step 2 – Does the third country and the circumstances of the transfer ensure an adequate level of protection?

## Is there an adequate level of protection?

23. Having established that there is a transfer of personal data to a third country, the data controller must then ask whether that third country ensures an adequate level of protection to the personal data[4] taking into account all the circumstances of the transfer ('adequacy').

24. A decision of whether or not there is adequacy may be based on a Community finding of adequacy or after an assessment of adequacy made by the data controller itself.

## Community findings of adequacy

25. Article 25(6) of the Directive (and Schedule 1, Part II, Para 15 of the DPA) requires that, where the European Commission (the Commission) has made a finding that a third country does, or does not, ensure adequacy, any question as to whether there is adequacy will be determined in accordance with that finding.

26. As at May 2016, the Commission has made positive full findings of adequacy in relation to the following countries.[5]

| | |
|---|---|
| Andorra<br>Argentina<br>Guernsey<br>Isle of Man<br>Israel | Jersey<br>New Zealand<br>Switzerland<br>Uruguay |

[4] Working document (WP237) Justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data 16/EN WP 237 – adopted 13 April 2016.
[5] An up-to-date list of Community findings is available on the European Commission website or the ICO website.

27. The Commission has made partial findings of adequacy in relation to Canada (commercial organisations)[6] and US for data transfers under the Privacy Shield Framework.

28. Historically a Decision of the European Commission in 2000 found that the US-EU "Safe Harbor" framework provided adequate protection for personal data transferred from the EU to US companies that were members of Safe Harbor.

29. On 6 October 2015 the Court of Justice of the European Union (CJEU) issued its judgment in Schrems v Data Protection Commissioner (Ireland) ("Schrems"). This judgment removed the assurance that using Safe Harbor gave businesses, ruling that it did not provide adequate protection. Further information on the replacement for the Safe Harbor framework, the EU-US Privacy Shield, can be found in our guidance on Using the Privacy Shield to transfer data to the US.

## Data transfers to the US and the Privacy Shield

30. On 12 July 2016, the European Commission issued its formal adequacy decision on the EU-US Privacy Shield. The Shield places stronger privacy requirements on the US companies certified by the scheme and gives greater redress mechanisms for individuals. The US Department of Commerce will oversee certification under the scheme.[7] If the company you want to transfer the data to is not certified, you cannot rely on the Privacy Shield protections.

31. Further guidance can be found in our guidance on Using the Privacy Shield to transfer data to the US.

## Assessing adequacy

32. Where the data protection regime in the third country has not been subject to a Commission finding of adequacy, it is for exporting controllers to assess adequacy in a way which is consistent with the Directive and the DPA. In carrying out this assessment of adequacy, the Commissioner would expect exporting controllers to be able to demonstrate how they have addressed the various criteria set out in this guidance.

---

[6] In relation to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act).
[7] Further information is available on the Privacy Shield website.

33. In the Directive, the basis of any assessment of adequacy is contained in Article 25(2), which states:

> "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

34. Article 25(2) has been implemented by the DPA at Schedule 1, Part II paragraph 13, which states that:

> "An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to:
>
> (a) the nature of the personal data;
> (b) the country or territory of origin of the information contained in the data;
> (c) the country or territory of final destination of that information;
> (d) the purposes for which and period during which the data are intended to be processed;
> (e) the law in force in the country or territory in question;
> (f) the international obligations of that country or territory;
> (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
> (h) any security measures taken in respect of the data in that country or territory."

35. The above adequacy criteria, for the purposes of this guidance, are divided into two categories – the 'general adequacy criteria' and the 'legal adequacy criteria'. The general adequacy criteria (described in more detail below) are factors which the exporting data controller will be able to identify easily; for example, the nature of the personal data being

transferred and purpose for which the data are to be processed. General adequacy criteria should be assessed in detail on every occasion. The legal adequacy criteria (see 'Legal adequacy criteria' below), may be more difficult for the controller to assess as they are factors relating to the legal system in force in the third country.

36. An exhaustive analysis of the legal adequacy criteria may be unnecessary if an assessment of the general adequacy criteria has revealed that in the particular circumstances the transfer is low risk. Conversely, if the general adequacy assessment reveals a high risk transfer (e.g. if the data is particularly sensitive), then a more comprehensive investigation of the legal adequacy criteria will be expected.

## Adequacy test – general adequacy criteria

37. As stated above, the 'general adequacy criteria' should be assessed in every case as the information will be in the knowledge of the exporting controller and therefore relatively straightforward to assess. These are:

    - the nature of the personal data;
    - the purpose(s) of the proposed transfer;
    - the period during which the data are intended to be processed;
    - any security measures taken in respect of the data in the third country;
    - the country of origin of the personal data; and
    - the country of final destination of the personal data.

### The nature of the personal data

38. The transfer of some types of personal data will pose little risk to the rights and freedoms of individuals. For instance, the transfer of a list of internal telephone extensions to overseas subsidiaries of a multinational company would not be considered to be high risk as it is unlikely that the data subject would suffer significant damage if his business telephone number was obtained by an unauthorised source. Conversely, if an exporting controller is proposing to transfer sensitive

personal data such as health records, the threshold of protection required in order for it to be adequate will clearly be higher.

### The purposes for which the data are intended to be processed

39. Some purposes for which data are processed will carry greater risks to the rights of the individuals than others. For instance, if the data are processed for internal purposes only (such as for an internal company telephone list as described above) this may carry with it less risk than if the details were more widely distributed, for instance in marketing brochures or on an internet site.

### The period during which the data are intended to be processed

40. If the data are only going to be processed once or for a short time and then destroyed, then the risks arising from any lack of protection may be less than if the data are being processed on a long-term basis.

### Any security measures taken in respect of the data in the third country

41. Exporting controllers may be able to ensure that the personal data are secure from any outside interference by means of, for example, technical measures such as encryption.[8] In practice, security is often a key factor in the commercial considerations of the parties.

### The country or territory of origin of the information contained in the data

42. This is not necessarily the same as the country or territory from where the transfer originates but rather the country or territory from which the data originate. In most cases this is likely to be the country or territory from where the information was originally obtained. Note that where the information has been obtained in a third country, this will be a relevant factor to consider because the data subject may have different expectations as to the level of protection that will be afforded to their data than they would have had if the information had

[8] For further information, please see the Encryption section of The Guide to Data Protection.

been obtained in the EEA. Where a third country is the country (or territory) of origin of the information contained in the data, the DPA is not intended to provide a different level of protection to a citizen of that country (or territory) than is provided by the data protection regime, if any, in the country (or territory) of origin.

**The country or territory of final destination of that information**

43. This is not necessarily the same as the destination country in relation to the particular transfer in question. In some cases it is known that there will be a further transfer to another country or territory which may or may not be outside the EEA. If this is the case, then the protection given in that ultimate destination will be relevant in assessing adequacy.

## Legal adequacy criteria

44. These are criteria that relate particularly to the third country in question. Namely:

    - the law in force in the third country;
    - the international obligations in that third country; and
    - any relevant codes of conduct or other rules which are enforceable in that country or territory.

45. As discussed above, the extent to which exporting controllers conduct an exhaustive analysis of the legal adequacy criteria will be for them to assess in the light of all the circumstances of the case and their assessment of the general adequacy criteria discussed above.

46. Even in those cases where they do not conduct an exhaustive analysis, exporting controllers will be expected to be able to recognise countries where there would be real danger of prejudice because of, for example, instability in the third country at the time of the transfer, and they will be expected to assess this danger in light of the general adequacy criteria.

47. An example of a situation where an exporting controller might reasonably be expected to have undertaken a detailed analysis of the legal adequacy criteria would be where the exporting controller is proposing to set up a permanent operation in a

third country and anticipates making regular, large-scale transfers to that country. Conversely, where the data transferred have a low level of sensitivity, such as the internal telephone list example discussed in 'General adequacy criteria' above, an exhaustive legal adequacy test may not be necessary.

48. When legal adequacy is assessed, an exporting controller should consider, in particular, the following questions:

- Has the third country adopted the OECD Guidelines[9] and, if so, what measures has it taken to implement them?
- Has the third country ratified Convention 108[10] and are there appropriate mechanisms in place for compliance with it?
- Does the third country have a data protection regime in place which meets the standards set out in the Article 29 Working Party document adopted on 24 July 1998 (WP 12)[11]
- Does the third country have any legal framework for the protection of the rights and freedoms of individuals generally?
- Does the third country recognise the general rule of law and, in particular, the ability of parties to contract and bind themselves under contracts?
- More specifically, are there laws, rules or codes of practice (general or sectoral) which govern the processing of personal data?

[9] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' – Organisation for Economic Co-operation and Development, 1980.
[10] Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, Strasbourg 1981.
[11] Working document (WP12) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive - Article 29 Working Party (DGXV D/5025/98 WP 12) - adopted 24 July 1998. This sets out certain principles - such as the 'purpose limitation principle', the 'transparency principle' and the 'security principle' - which the Working Party believe should be embodied in a data protection regime in order for it to be considered to be adequate.

## Proceed with transfer?

49. If adequacy is established further to either (i) a Community finding of adequacy or (ii) the data controller's adequacy assessment, then the transfer can proceed from the UK to the third country in compliance with the eighth principle. Note that if transfers are taking place from more than one European jurisdiction then local advice should always be sought as there may be different requirements which apply depending on the jurisdictions in question.

50. If adequacy is not established under (i) or (ii) above then the exporting controller should proceed to Step 3 and examine the suitability of implementing the adequate safeguards described.

# Step 3 – Have or can the parties put into place adequate safeguards?

## Use of model clauses or binding corporate rules

51. If it is not possible for an exporting data controller to satisfy itself that there is adequacy (as described in Part 2 above), the use of Commission-authorised standard contracts (model clauses) or specific, approved binding corporate rules (BCR) enable the transfer to be made exempt from the restrictions of the eighth principle on the basis that the model clauses or set of BCR provide adequate safeguards for the rights and freedoms of data subjects.

52. This derives from Article 26(2)[12] of the Directive which states that:

> "a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection…where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses…"

53. Transfers which are exempt by virtue of Article 26(2) ensure conditions whereby the individuals in question continue to be protected as regards processing of their data even after the data have been transferred. For this reason, it is good practice to attempt to satisfy one of these Article 26(2) derogations before considering the derogations which derive from Article 26(1)[13] (which do not ensure such a high level of protection - see Step 4 below).

## Model clauses

54. Further to Article 26(4) of the Directive, the Commission is empowered to recognise standard contractual clauses as offering adequate safeguards for the purposes of Article 26(2)

[12] Implemented by paragraphs 8 and 9 of Schedule 4 to the DPA.
[13] Implemented by paragraphs 1 to 7 of Schedule 4 to the DPA.

and it has approved model clauses further to the following decisions:

- Commission Decision 2001/497/EC,[14] dated 15 June 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set I controller-controller).

- Commission Decision 2002/16/EC,[15] dated 27 December 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data processors outside the EEA (controller-processor).

- Commission Decision 2004/915/EC,[16] dated 27 December 2004 – in which the Commission approved an alternative set of model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set II controller-controller).

55. The Commissioner has issued authorisations under s54(6) of the DPA in relation to each of the model clauses (on 21 December 2001, 8 March 2003 and 27 May 2005, respectively) providing that, for the purpose of paragraph 9 of Schedule 4 to the DPA, the eighth principle does not apply where the transfer has been made using any of the model clauses. This means that an exporting controller who uses these model clauses does not need to make a separate assessment of adequacy in relation to the transfer.

56. The model clauses contain obligations on both the data exporter and data importer to ensure that the transfer complies with the standards required by the Directive and the data subject has a right to directly enforce its rights under them. Under the Set I controller-controller model clauses, the data exporter and data importer are jointly and severally liable to the data subject for any damage it suffers as a result of a breach by either party of those of the model clauses under which the data subject is a beneficiary (third party beneficiary clauses). This differs from the Set II controller-controller model clauses under which the data subject can only enforce its rights against the party who is responsible for the relevant

[14] The clauses are an annex to the Decision which approves them.
[15] The clauses are an annex to the Decision which approves them.
[16] The clauses are an annex to the Decision which approves them.

breach.[17] Under the controller-processor model clauses, the data exporter is liable to the data subject for any breach by either party of the third party beneficiary clauses except in limited circumstances. However, if the breach was caused by the data importer, the data importer is required to indemnify the data exporter to the extent of its liability to the data subject.

57. In addition to the greater flexibility inherent in the Set II controller-controller model clauses, these clauses also give the data importer greater discretion in deciding how to comply with data protection laws and how to respond to subject access requests. However, it should be noted that: "to prevent abuses with this additional flexibility…data protection authorities can more easily prohibit or suspend data transfers based on the Set II controller-controller model clauses in those cases where the data exporter refuses to take appropriate steps to enforce contractual obligations against the data importer or the latter refuses to cooperate in good faith with competent supervisory data protection authorities."[18]

58. None of the versions of the model clauses may be amended but the parties are free to include any other clauses on business related issues provided that they do not contradict the model clauses. Indeed, the Set II controller-controller model clauses include some suggested commercial clauses to be incorporated (e.g. an indemnity provision, dispute resolution clause and extra termination right). The Set II controller-controller clauses also allow the parties to update the description of the transfer that the parties will have originally set out in Annex B, to reflect changes as the relationship develops.

59. Use of any of versions of the model clauses, whether as a stand-alone contract or incorporated into another contract, where the wording is changed but without altering the intended meaning or effect of any clause, does not amount to use that is authorised by the Commissioner under paragraph 9 of Schedule 4 to the DPA. However, this does not prevent the data controller from taking the view that the transfer is made on terms which provide adequacy (as defined above), and

[17] Note that under Set II the data importer must provide the data exporter with satisfactory evidence of its ability to meet its liabilities with details of any insurance coverage etc (section 1(f) of the Set II controller-controller model clauses).
[18] Paragraph 7 of the Commission Decision 2004/915/EC dated 27 December 2004.

indeed the use of different terms with the same meaning or effect as those in the model terms would be a significant factor were the Commissioner required to assess the adequacy of any protection given to the data.

60. Note that if the only change to the model clauses is to make the contract between more than two parties (e.g. where there is more than one data importer) rather than remain a bilateral agreement between one data exporter and importer then the Commissioner is of the view that this **does** remain within the scope of the Commissioner's authorisation provided that the obligations of all the parties remain clear and legally binding.

## Binding corporate rules (BCR)

61. BCR are internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards for the rights and freedoms of data subjects for the purposes of paragraph 9 of Schedule 4 to the DPA. They are designed to be a global solution for multinational companies by ensuring their intra-group transfers comply with the eighth principle and providing a simple mechanism for obtaining the necessary authorisations across the EU. BCR must be submitted for approval by the Commissioner in order to obtain an authorisation which provides that transfers from the UK may be made within the group on the basis of the BCR (further details of the authorisation process is set out in below).

62. The concept of using BCR to create adequate safeguards for the purposes of Article 26(2) was devised by the Article 29 Working Party in its working document on binding corporate rules, adopted on 3 June 2003 (WP74).[19]

63. Subsequently, to assist with compliance, the Article 29 Working Party has developed the following documents:

    - Model checklist on the content of a BCR application to DP authorities (model checklist).[20]

[19] 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, 11639/02/EN WP 74.
[20] Working document (WP 108) Establishing a Model Checklist Application for Approval of Binding Corporate Rules 05/EN WP 108 – adopted 14 April 2005.

- Co-operation procedure to facilitate the authorisation process (the co-operation procedure).[21]

- Standard application form based on the model checklist (the application form).[22]

- Table of BCR requirements (this is a summary of WP 74 and WP 108 in an easy-to-follow table format).[23]

- Framework BCR (a suggestion of what a BCR application might look like).[24]

- BCR FAQs - a working document that is constantly being updated in the light of new questions and experience.[25]

64. Applications for the authorisation of BCR to the Commissioner must be made in accordance with the application form and applicants will be required to demonstrate that adequate safeguards are in place within the organisation and must include:
    - evidence that the measures are binding, both internally and externally;

    - details of a data protection audit plan;

    - a description of processing and flows of information;

    - a description of the data protection safeguards in place; and

    - details of a mechanism for reporting and recording changes.

65. The Commissioner will only give an authorisation where she is satisfied that such adequate safeguards can be delivered.

---

[21] Working document (WP 107) Setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules 05/EN WP 107 – adopted 14 April 2005.
[22] Recommendation 1/2007 (WP 133) on the standard application for approval of binding corporate rules for the transfer of personal data - adopted 10 January 2007.
[23] Working document (WP 153) setting up a table with the elements and principles to be found in BCR 1271-00-00/08/EN WP 153 - adopted 24 June 2008
[24] Working document (WP 154) setting up a framework for the structure of BCR 1271-00-01/08/EN WP 154 - adopted 24 June 2008.
[25] Working document (WP 155) on frequently asked questions related to BCR 1271-00-02/08/EN WP 155 rev.01 - adopted on 24 June 2008; revised on 1 October 2008.

66. Where a data controller wishes to use BCR to export data out of the EEA from a number of different European jurisdictions, WP 74 provides a mechanism whereby the exporting data controller can, in the first instance, deal with one DP authority who then co-ordinates the authorisation process from other DP authorities in all the other European jurisdictions in which that company operates. For this purpose, the data controller will need to propose the DP authority in one jurisdiction as the 'lead authority' who will then liaise with the other relevant DP authorities in accordance with the co-operation procedure with a view to getting the BCR approved by them all.[26]

67. The co-operation procedure suggests that the decision on which DP authority should be the 'lead authority' should be based on criteria such as the location:

    - of the group's European headquarters;
    - of the company within the group that has delegated data protection responsibilities;
    - of the company within the group best placed to deal with the application and enforce the BCR;
    - where most decisions are taken in relation to the processing; and
    - where the most transfers outside the EU take place.

68. Some DP authorities have signed up to a policy of mutual recognition where they have agreed to authorise the BCR without further comment or amendment at the point at which it is circulated by the lead authority with an opinion that it provides an adequate level of protection as described in the working party documents. At this point not all DP authorities in the EEA have signed up to this policy and so the co-operation procedure will still be used in many cases alongside mutual recognition.

69. Once a set of BCR have been approved by the DP authorities as part of the co-operation procedure or as a result of mutual recognition, and any national permits obtained and necessary

[26] However, the Data Protection Authorities may among themselves decide to allocate the lead authority to another Data Protection Authority than the one proposed by the applicant.

notifications made, transfers falling within their scope can take place from the countries from which authorisations have been received, provided it is for a purpose and in a manner that is compliant with any national data protection or other relevant laws in that country.[27]

70. The Commissioner's website contains details of the BCR which it has approved and further information as to how to make an application for the authorisation of BCR.[28]

## Proceed with transfer?

71. If the model clauses are used, or the Commissioner has approved a set of BCR which would govern the transfer, the transfer from the UK to a third country can take place without further authorisation. However, if neither of these methods is appropriate in relation to the transfer and the exporting controller is unable to adduce adequacy further to Step 2 then it should consider whether any further derogations apply, as described in Step 4.

[27] Although transfers made under intra-group codes which have not been submitted for approval by the Commissioner as BCR will not be exempt from the eighth principle, such codes may enable data controllers to establish adequacy as part of any adequacy assessment they carry out as described in Part 2 to this guidance.
[28] Please see the Binding Corporate Rules section of The Guide to Data Protection.

# Step 4 – Do any other derogations to the eighth principle apply?

## The derogations

72. As set out in Part 3 above, the use of BCR and model clauses are two derogations from the eighth principle derived from Schedule 4 of the DPA. There are also a number of other derogations in Schedule 4 which may be considered. They are as follows:

    - The data subject has consented to the transfer.
    - The transfer is necessary for the performance of, or for the taking of steps at the request of the data subject with a view to entering into, a contract between the data subject and the data controller.
    - The transfer is necessary for the performance of, or entering into, a contract between the data controller and a third party entering into the contract at the request, or in the interests, of the data subject.
    - The transfer is necessary for reasons of substantial public interest.
    - The transfer is necessary in connection with legal proceedings, advice or rights.
    - The transfer is necessary to protect the vital interests of the data subject.
    - The transfer is of part of the personal data on a public register.[29]

73. Each of these derogations is discussed in more detail below. Unlike BCR or model clauses, where these derogations are used there is not necessarily any protection in place in relation to the data being transferred. Instead, these provisions reflect the fact that there are instances where it will be justifiable to transfer data even though there will be a lower level of

[29] Schedule 4, paras 1-7 (equivalent to Article 26(1) of the Directive).

protection given to those data. As such, in interpreting these provisions, the derogations should be narrowly construed.

74. In addition, when applying the derogations, exporting controllers should be aware that just because the eighth principle does not apply, it does not mean that the other seven principles do not apply to the data and these should always be considered in addition to the eighth principle in the context of international data transfers.

## Consent

75. Article 2(h) of the Directive defines consent as "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed". Consequently, exporting controllers should be able to produce clear evidence of the data subject's consent in any particular case and may be required to demonstrate that the data subject was informed as required.

76. Similarly, valid consent means that the data subject must have a real opportunity to withhold their consent without suffering any penalty, or to withdraw it subsequently if they change their mind. This can be particularly relevant if it is employee consent which is being sought.

77. For these reasons, consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or structural transfers of data to a third country. As the Article 29 Working Party states in its paper on the interpretation of Article 26(1): "relying on consent may…prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome".[30]

## Necessary for a contract between data controller and data subject or data controller and third party

78. In order to fall within these two derogations it needs to be shown that the transfer is *necessary* for the performance or entering into of the contract. If it is a third party entering into the contract, rather than the data subject, then it has to be

[30] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 11.

clearly shown that they are entering into it at the request of the data subject or that it is clearly in the data subject's interests.

79. An example given by the Article 29 Working Party[31] of a contract that falls within this category is where there is a transfer to a third country by travel agents of personal data of their clients to hotels or to other commercial partners that will organise the clients' stay. This is contrasted with the transfer of employee data from an EEA subsidiary to a non-EEA parent company in order to centralise a multinational group's HR and payment functions which, it has been argued, is necessary for the data subject's employment contract with the data controller.

80. Although such a transfer may provide a cost-efficiency which may indirectly benefit the employee, it would be difficult to show that the centralisation of payment functions is objectively necessary for the performance of the data subject's employment contract and could not be carried out elsewhere. Therefore it is likely that in these circumstances the derogation would not apply.

81. Note that this does not mean that this arrangement is not permitted at all – for instance, it may satisfy the adequacy criteria discussed in Step 2 and comply with the eighth principle under those grounds – merely that this particular derogation is unlikely to be applicable in these circumstances.

82. Similarly, where the contract is between the data controller and a third party, not only does the data controller need to show that the transfer is necessary for that contract, unless the contract has been entered into at the data subject's request, the data controller needs to show "a close and substantial connection between the data subject's interests and the purpose of the contract".[32] This derogation is discussed further in the context of outsourcing below.

[31] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 13.
[32] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 14.

## Substantial public interest

83. To qualify for this derogation, the transfer must be "necessary for reasons of substantial public interest".[33] This is subject to the same strict interpretation as that applied to the other derogations discussed in this section and is a high threshold. The Secretary of State may by order specify circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest. No such orders are in force to date.

84. Recital 58 of the Directive gives examples of cases where international exchanges of data might be necessary "between tax or customs administrations in different countries" or "between services competent for social security matters". The transfer should be in the public interest in the Member State itself rather than the third country.

## Legal matters

85. This derogation will apply where the transfer is necessary:

    - for the purpose of, or in connection with, any legal proceedings[34] (including prospective legal proceedings);
    - for the purpose of obtaining legal advice; or
    - for the purposes of establishing, exercising or defending a legal right.

86. Once again, the emphasis in using this derogation is on necessity and the need to balance the legal rights at the centre of the advice or action with the data subject's rights in relation to their personal data.

87. An example given by the Article 29 Working Party of where this derogation may apply would be where a parent company based in a third country is sued by an employee of the group based at one of the European subsidiaries, and the company requests the European subsidiary to transfer certain data relating to the employee if the data are necessary for the defence.[35]

---

[33] Schedule 4, para 4(1).
[34] Including legal proceedings outside the UK (e.g. in the third country).
[35] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 15.

## Vital interests of the data subject

88. The Commissioner considers that this exception to the eighth principle may only be relied upon where the data transfer is necessary for matters of life and death such as a medical emergency. For instance, it would clearly be essential to be able to transfer data if the data subject is in urgent need of medical attention in a third country and only their usual doctor based in a Member State can supply this data. The derogation could not be relied upon, by contrast, if the data are not transferred for the purpose of treating the data subject but instead are to be used for general medical research in the future.

## Public registers

89. This derogation may be relied upon if the transfer is of part of the personal data on a public register in a Member State and any conditions to which the register is subject are complied with by any person to whom the data are or may be disclosed after the transfer. Note that the data transferred should only be of part of the data and "not involve the entirety of the data or entire categories of the data contained in the register".[36]

## Proceed with transfer?

90. If the transfer falls under any of the derogations discussed above then it is exempt from the eighth principle and may proceed without any further requirements or prior authorisation. However, if adequacy has not been adduced in line with Step 2 or the derogations described in Steps 3 and 4 do not apply, the transfer may not proceed without being in breach of the eighth principle. Remember also that compliance with the eighth principle is only one aspect of satisfying the requirements of the DPA and a data controller should ensure that it complies with all the principles when processing and transferring personal data.

91. The final part of this guidance, section 5, deals with issues which may arise in relation to a particular type of data transfer – namely, transfers to data processors located in a third

---

[36] Recital 58 of the Directive.

country – and provides further illustration of how the eighth principle operates in practice.

# Section 5 – International outsourcing to data processors located in a third country

92. Increasingly, UK data controllers are using data processors[37] in third countries to carry out processing on their behalf. A transfer to a data processor in a third country will be caught by the eighth principle.

93. Where a transfer is made to a data processor in a third country by a UK data controller, the exporting controller remains the data controller in the UK for the purposes of the DPA. This means that the data controller remains subject to the Commissioner's powers of enforcement and is responsible for protecting individuals' rights under the DPA in relation to the overseas processing of the personal data by the data processor.

## The seventh principle

94. Where there is a transfer to a data processor, wherever that processor is located, a data controller must comply with the requirements of all the principles, including the seventh data protection principle (the seventh principle) which states that:

> "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

95. The seventh principle (at paragraph 11 of Part II of Schedule 1 to the DPA) requires that where a third party undertakes processing on behalf of a data controller, that data controller must:

    - choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

[37] Defined in section 1(1) of the DPA.

- take reasonable steps to ensure compliance with those measures (such as conducting regular audits and reviews).

96. In addition, a data controller will not be regarded as complying with the seventh principle unless the processing is carried out under a contract "made or evidenced in writing",[38] and under which the data processor is to act only on instructions from the data controller and which contains an obligation on the part of the data processor to comply with provisions equivalent to those imposed on a data controller by the seventh principle.

## Use of model clauses and assessment of adequacy

97. One form that such a contract "made or evidenced in writing" may take is the data controller-data processor model clauses discussed in 3.2 above which have been approved by the Commission as offering adequate safeguards for the purposes of Article 26(2).[39] The use of these terms can simultaneously satisfy the requirement for a contract in the seventh principle and fall under a derogation from the eighth principle and, for that reason, may be attractive in data controller-data processor international outsourcings.

98. However, a data controller in the UK need not necessarily use these controller-processor model clauses when entering into a contract with a data processor in a third country provided that any contractual arrangement satisfies the requirements of the seventh principle and the data controller has successfully complied with, or derogated from, the eighth principle by another means. The model clauses are merely one method of addressing the requirements of the eighth principle and there are many other methods which have been discussed in this guidance which may be more appropriate in the circumstances.

99. In particular, the model clauses will not be necessary if the data controller establishes that there is adequacy as described in Step 2 of this guidance. In this respect, the Commissioner's guidance is that compliance with the seventh principle will go some way towards satisfying the adequacy requirements of the eighth principle (given the continuing contractual relationship between the parties and the data controller's continued liability for data protection compliance under the

[38] Schedule 1, Part II, paragraph 12(a)(i).
[39] Commission Decision 2002/16/EC dated 27 December 2001.

DPA). However, the Commissioner would still expect the data controller to make due diligence checks in relation to the data processor and conduct some examination of the type of matters usually looked at in relation to adequacy (e.g. the nature of the data, the country in which the data processor is located and the security arrangements in that third country).[40] If such due diligence and analysis did not reveal any particular risks in relation to the transfer, then the controller-processor relationship and the security measures implemented further to compliance with the seventh principle would be likely to ensure adequacy and, therefore, the transfer would be able to proceed in compliance with the eighth principle.

## Use of "necessary for contract in the interests of data subjects" derogation

100. As discussed at 4.3.3 above, there is a derogation from the eighth principle where the transfer is necessary for the conclusion or performance of a contract between the data controller and a person other than the data subject where such a contract is entered into at the data subject's request or is in the interests of the data subject.[41] It is sometimes argued by data controllers that a transfer which is necessary for an outsourcing contract with a service provider in a third country will fall under this derogation where the subject of the contract is indirectly in the interests of the data subjects (for instance, where the service provider is administering the data controller's payroll functions). The argument advanced is that as the contract relates to the pay of the data subject (the employee) then it is in the interests of the data subject that this contract is performed. However, the Commissioner (in common with the Article 29 Working Party[42]) does not support this view on the basis that there is not a sufficiently close and substantial link between the contract and the data subject's interests. Instead the Commissioner would, as a general rule, expect such arrangements to comply with, or be exempt from, the eighth principle through other means – such as the adducing of adequacy (as described in Step 2) or the implementation of adequate safeguards (as set out in Step 3 and 'Use of Modal clauses' above).

---

[40] See 'General adequacy criteria' and 'Legal adequacy criteria' above for all the adequacy criteria to be taken into account when adducing adequacy.
[41] Paragraph 3 of Schedule 4 to the DPA.
[42] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, pages 13 – 14.

## Subprocessors

101. Many transfers to a third country are made where a data processor based in the UK then subcontracts the processing to another processor outside the EEA. As the data controller will remain liable for compliance with the DPA, it will be for the data controller to satisfy itself that such subcontracting will not materially increase the risks to the data being processed. In this situation, the data controller must expressly permit the subcontracting and it is likely that this will be best achieved by means of a clause in the controller to processor contract. The controller to processor contract should also contain an obligation on the part of the processor to contract in equivalent terms with the subprocessor and to enforce the terms of the subprocessor contract. Any contract between the processor and the subprocessor should therefore mirror the main controller to processor contract and also address any adequacy issues not covered by the main controller-processor contract (in the event that the main contract was drafted in the context of a processing within the UK).

102. As the data controller in the UK always remains liable to enforcement action by the Commissioner and to a civil action by a data subject for breaches taking place outside the UK as a result of the acts of a data processor, it is particularly important that a data controller is satisfied as to the identity and propriety of both the processor and any subprocessor engaged and, in particular, that the requirements of the seventh principle are satisfied.

## General points

103. Data controllers should take into account the legislation in place in the country or territory where the chosen processor is located and any obligations this may impose, for example, the US PATRIOT Act. As part of the assessment as to the adequacy of the protection available for the information being transferred, the data controller will need to consider other legislation, any risks this may pose, the likelihood of the controller or the processor being subject to that legislation and how the controller will respond if necessary. The data controller should have procedures and measures in place to deal with any requests for information they or their processor may receive under legislation in the country in which the processor is located.

104. If either the data controller or the data processor receives a request for information from another jurisdiction, the data controller will need to decide whether or not they are able to comply with the request. If they do decide to comply, then it is good practice to ask for more information if necessary, to make sure the request is specific enough to allow them to be able to identify, retrieve and transfer only that information that is relevant and necessary to comply with the request.

# Model Contract Clauses

## International transfers of personal data

## Data Protection Act

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of DPA can be found in The Guide to Data Protection .

This is part of a series of guidance, which goes into more detail than the Guide to DPA, to help you to fully understand your obligations, as well as promoting good practice.

This guidance explains one of the methods of transferring personal data outside the EEA in compliance with the DPA – using Model Contract clauses.

## Overview

A data controller may only transfer personal data outside the EEA to a country whose data protection laws have not been approved by the European Commission as providing adequate protection for data subjects' rights if there is an adequate level of protection for the rights of data subjects.

The adequacy of the level of protection associated with a particular transfer may be ensured in a number of ways. The data controller may:

- carry out his own assessment of the adequacy of the protection;
- use contracts to ensure adequacy;
- obtain Commission approval for a set of Binding Corporate Rules governing intra-group data transfers; or
- rely on one of the exceptions to the prohibitions on transfers of personal data outside the EEA.

This guidance considers how a data controller may carry use

contracts, in particular model contracts approved by the European Commission, to transfer personal data outside the EEA.

## What the DPA says

The eighth data protection principle provides that:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data"
>
> (Part 1 of Schedule 1 to the DPA).

If you decide you need to transfer personal data outside the EEA, and the recipient is not in a country subject to a positive finding of adequacy by the Commission, nor signed up to the Safe Harbor Scheme, you will need to:

- conduct a risk assessment into whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects; or
- if you do not find there is an adequate level of protection, put in place adequate safeguards to protect the rights of the data subjects, possibly using Model Contract Clauses or Binding Corporate Rules; or
- consider using one of the other statutory exceptions to the Eighth Principle restriction on international transfers of personal data.

This page provides advice on the use of Model Contract Clauses as referred to in the second of these options – putting in place adequate safeguards. The use of 'adequate safeguards' is recognised in Article 26(2) of the EU Directive on Data Protection and paragraphs 8 & 9, Schedule 4, DPA.

Adequate safeguards may be put in place in a variety of ways including using model contract clauses, binding corporate rules or other contractual arrangements. This page looks at adequate safeguards in the form of 'model contract clauses'.

## Model Contract Clauses as a basis for transferring personal data outside the EEA

The European Commission is empowered to recognise standard contractual clauses (known as model contract clauses) as offering adequate safeguards for the purposes of Article 26(2)[1]. The Commission has approved four sets of model contract clauses listed below.

The Information Commissioner is empowered to authorise transfers of personal data in such a manner 'as to ensure adequate safeguards for the rights and freedoms of data subjects' under paragraph 9, Schedule 4, DPA. Following approval by the Commission, the Information Commissioner has in turn also approved the following sets of model contract clauses.

- **Set I controller-controller** 2001 controller to controller

  Commission Decision 2001/497/EC, dated 15 June 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data controllers outside the EEA.

  Authorised by the Information Commissioner on 21st December 2001.

- **Set I controller-processor**

  Commission Decision 2002/16/EC, dated 27 December 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data processors outside the EEA.

  Authorised by the Information Commissioner on 18th March 2003. Model contract clauses authorisation - controllers to processors authorisation 2003.pdf

  (Note – this set is no longer available for new users but continues to have effect in relation to arrangements put in place prior to 15th May 2010).

- **Set II controller – controller** 2004 controller to controller.

[1] Article 26(4) of the Directive

Commission Decision 2004/915/EC, dated 27 December 2004 – in which the Commission approved an alternative set of model clauses for transfers from data controllers in the EEA to data controllers outside the EEA.

Authorised by the Information Commissioner on 27th May 2005.

- **Set II controller – processor** 2010 controller to processor

  Commission Decision 2010/87/EU, dated 5th February 2010 – in which the Commission approved a new set of model clauses for transfers from data controllers in the EEA to data processors outside the EEA to replace the Set I controller to processor clauses.

  Authorised by the Information Commissioner on 17th May 2010 Model Contract Clauses - Controller to Processor Authorisation 2010

If you use these model clauses in their entirety in your contract, you will not have to make your own assessment of the adequacy of protection afforded to the rights of data subject in connection with your transfer of their personal data.

## Controller to controller clauses

The model clauses impose obligations on both the exporter and the importer of the data to ensure that the transfer arrangements protect the rights and freedoms of the data subjects. Two of the sets of model clauses (the controller to controller clauses) relate to transferring personal data from one company to another company, which will then use it for its own purposes. You may choose to use either set of clauses, depending on which better suits your business arrangements.

The Set I controller-controller model clauses provide that you, the data exporter, and the data importer are jointly and severally liable to the data subject for any damage he may suffer as a result of a breach by either party of the model clauses. The data subject has a direct right of action under these model clauses by virtue of a third party beneficiary clause. This differs from the Set II controller-controller model clauses under which the data subject can only enforce his rights against the party who is responsible for the relevant breach. Where the data importer is at fault, if the data subject is having trouble taking action against the data importer he may be able to take action against you as data exporter for failing

to use reasonable efforts to ensure that the importer is able to satisfy its obligations under the clauses[2].

## Controller to processor clauses

The other sets of model clauses relate to the transfer of personal data to a processor acting under your instructions, such as a company that provides you with IT services or runs a call centre for you.

The Set I controller-processor model clauses (no longer available for new transfers) provided that the data exporter was primarily liable to the data subject for damage arising from a breach by either party of the clauses. In certain circumstances the data importer would be required to indemnify the data exporter in relation to the breach.

The Set II controller to processor clauses (like the Set II controller to controller clauses) allow for liability to follow fault – that is to say, the party causing the breach will be held liable for the breach rather than liability always lying with the data controller. In addition, the Set II controller to processor clauses envisage circumstances involving the onward transfer of personal data by the processor outside the EEA to a sub-processor. Any such sub-processing arrangements must contractually extend the protection for the rights of data subjects to the sub-processing and any sub-processing must be authorised by the data controller. The data subject may, by virtue of the third party beneficiary clause, take action in relation to any breach of the clauses primarily against the party at fault, be that the controller, the processor or the sub-processor. However, the controller will always retain responsibility for any harm arising from its initial transfer of the data.

## Amending the clauses, incorporating the clauses in other contracts and inserting additional clauses

If you are relying on any of the European Commission sets of model contract clauses as 'stand-alone contracts' you cannot change the

[2] The Set II controller-controller model clauses are intended to provide greater flexibility for contracting parties. The clauses also give the data importer greater discretion in deciding how to comply with data protection laws and how to respond to subject access requests. However, to prevent abuses arising from this additional flexibility, data protection authorities can more easily prohibit or suspend data transfers based on the Set II controller-controller model clauses in those cases where the data exporter refuses to take appropriate steps to enforce contractual obligations against the data importer or the latter refuses to cooperate in good faith with competent supervisory data protection authorities (Paragraph 7 of the Commission Decision 2004/915/EC dated 27 December 2004)

clauses in any way (save to add an additional party, such as an additional data importer).

The model contract clauses may however be incorporated into other contracts (such as data processing service agreements) or additional provisions may be added[3] provided nothing in the other contract or additional clauses alters the effect of any of the model clauses. The addition of an extra data importer into the model contract clauses (so that you may use the clauses to, for example, export personal data to a processor in New Zealand and a processor in Australia) will not change the status of the clauses provided obligations of all the parties remain clear and legally binding.

### Impact of amending the model contract clauses – use of 'Other Contracts'

Use of any version of the model clauses, whether as a stand-alone contract or incorporated into another contract, where the wording is changed (even if the meaning or effect of the changed clause remain unaltered), will **not** amount to use of clauses that are authorised by the Information Commissioner as providing adequate safeguards under one of the Information Commissioner authorisations set out above.

If you choose to amend the model contract clauses, you may take the view that your amended clauses are sufficient to provide adequate safeguards for the protection of the rights of the data subjects whose personal data you propose to transfer. Your amended clauses will not be 'model contract clauses' (attracting the Commission 'guarantee' that they provide adequate safeguards for data subjects rights) but may operate as contractual arrangements which in the reasonable view of the data controller provide adequate safeguards for data subjects' rights. Providing adequate safeguards by using your own clauses is an equally valid basis on which to proceed with a transfer as is the use of model contract clauses. The only difference is that you need to be prepared to offer evidence in support of your view (that your clauses provide adequate safeguards) if it is challenged. If you use model contract clauses, given that the Commission has determined that such clauses offer adequate safeguards, there can be no challenge as to the effectiveness of the safeguards the model contract clauses offer.

---

[3] Indeed, the Set II controller-controller model clauses include some suggested commercial clauses to be incorporated (e.g. an indemnity provision, dispute resolution clause and extra termination right). The Set II controller-controller clauses also allow the parties to update the description of the transfer that the parties will have originally set out in Annex B, to reflect changes as the relationship develops.

## Other considerations

Using model contract clauses is only one method of ensuring a transfer of personal data outside the EEA complies with the Directive.

Guidance on other transfer arrangements is available:

- Making your own assessment of the adequacy of the level of protection for the rights of data subjects
- Binding Corporate Rules
- International outsourcing arrangements

## More information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please Contact us: see our website www.ico.org.uk.

ARTICLE 29 DATA PROTECTION WORKING PARTY

3284/16/EN
WP 241

# Opinion 04/2016 on European Commission amendments proposals related to the powers of Data Protection Authorities in Standard Contractual Clauses and adequacy decisions

**Adopted on 31 October 2016**

## I. Introduction

On 14 October 2016, the Article 29 Working party was consulted as a matter of urgency by the European Commission on two draft implementing Decisions as it intends to submit those Decisions to the Article 31 Committee in the very near future. The WP29 has been asked to consider:

1 Draft Commission Decision amending Commission Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council (hereinafter: "draft decision on standard contractual clauses").

2 Draft Commission Decision amending Commission Decisions 2000/518/EC,

2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU, 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council (hereinafter: "draft decision on adequacy");

**As a general remark, the Working Party regrets the very short deadline given by the European Commission to analyse these draft decisions** especially as the proposed amendments directly concern the powers of Data Protection Authorities ("DPAs") under Adequacy decisions and Standard Contractual Clauses approved by the European Commission.

According to the Article 30.1.c of EC Directive 95/46/EC, the Article 29 Working party is competent to advise the Commission on any proposed Community measures affecting rights and freedoms of natural persons. As the proposed modifications directly address the powers of DPAs as referred to in article 28.3 of EC Directive 95/46/EC, it may affect rights and freedoms of natural persons and the Article 29 Working party welcomes this consultation.

**According to Recital 7 of the draft Commission Decisions, the purpose of the proposed modifications is to ensure the "*full implementation*" of the European Court of Justice ("CJEU") judgement in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (hereunder, "Case C-362/14 CJEU judgement")** for the listed existing Commission implementing decisions based on articles 25.6 and 26.4 of EC Directive 95/46/EC.

In Case C-362/14 CJEU judgement, the Court annulled article 3 of the Safe Harbor decision 2000/520/EC because the Commission lacked competence to restrict the national supervisory authorities' powers derived from Article 28 of Directive 95/46. The article 3.1.b of Safe Harbor decision imposed four cumulative conditions for the DPAs' intervention. The Court considered such conditions as "*restrictive conditions establishing a high threshold for intervention*" which was understood by the Court as denying the

powers of the national supervisory authorities which derive from Article 28 of Directive 95/46 to ensure compliance with article 25 of EC Directive 95/46/EC[1].

The opinion of the General advocate was more detailed: "*As the Belgian and Austrian Governments submitted, in essence, at the hearing, the emergency exit that Article 3(1)(b) of Decision 2000/520 represents is so narrow that it is difficult to put into practice. It imposes cumulative criteria and sets the bar too high. In the light of Article 8(3) of the Charter, it is not possible for the national supervisory authorities' scope for manoeuvre in relation to the powers resulting from Article 28(3) of Directive 95/46 to be limited in such a way that they can no longer be exercised.*"

The cumulative aspect of the conditions was in any case creating a particular burden, but this was particularly true in relation to one of the conditions where it was difficult (almost impossible) to assess whether "*the continuing transfer would create an imminent risk of grave harm to data subjects*"[2], especially in the framework of secret surveillance activities.

The Court of Justice also annulled article 1 of the Safe Harbor Decision 2000/520/EC as that the Commission did not state that the "*United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments*"[3]. In particular, the Decision 2000/520/EC did not contain "*any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security. Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind*"[4].

## II. Scope of the opinion

As the Working Party 29 understands that the European Commission intends to submit the draft Decisions to the Article 31 Committee imminently, this analysis focuses on the current proposal to amend article 3 of the Adequacy Decisions and article 4 of the Decisions on standard contractual clauses.

The Working Party 29 however notes that the Court of Justice stated that: "*in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must*

[1] See §§ 101-104 of Case C-362/14 CJEU judgement. Reference to article 25 here depends on the subject matter of the Case C-362/14 CJEU judgement and of course, it could not be understood as limiting the scope of application of article 28.

[2] See article 3.1.b of the annulled decision 2000/5220/EC on Safe Harbor.

[3] See paragraph 97 of Case C-362/14 CJEU judgement.

[4] See paragraphs 88 and 89 of Case C-362/14 CJEU judgement.

*find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order*[5]". In this particular regard, it is incumbent to the European Commission to provide for such findings in its adequacy decisions[6]. **The WP29 regrets that the Commission, in its draft decisions which are subject to the present consultation, only partially addresses the Court decision** by focusing on the implementation of the reasoning related to the annulment of article 3 of the Decision 2000/520/EC and by not addressing the arguments in relation to the annulment of its article 1.

In particular, the Working Party 29 regrets that the Commission has not carried out an in-depth assessment of the conditions under which public authorities in the third countries concerned access personal data transferred on the basis of the relevant decisions on adequacy. In this context, the WP29 notes that the current decisions on adequacy concern, in particular, the level of protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, as well as countries including Switzerland, Argentina, the State of Israel, the Eastern Republic of Uruguay and New Zealand. **In order to ensure their compliance with the fundamental rights to respect for private life and protection of personal data, the Working Party 29 insists that the draft decisions on adequacy must assess whether public authorities of these third countries responsible for national security, law enforcement or other public interests do not interfere with the rights of individuals to privacy and to protection of their personal data beyond what is strictly necessary, and that there is effective legal protection against such interferences.** The assessment made by the Commission as to the compliance with this requirement does not seem sufficient to meet the requirements stated by the CJEU in the Case C-362/14[7] and could jeopardize their legal validity possibly leading to a referral to a competent Court. **The Working Party 29**

[5] Paragraph 96 of Case C-362/14 CJEU judgement.

[6] In this regard, the Working Party 29 underlines that assessments of the level of adequacy were made, until recently, on the basis of detailed reports established by external experts appointed by the European Commission. The Working Party consequently strongly recommends that the European Commission provides extensive adequacy reports as basis of its decisions and resumes its previous practice to appoint external experts in charge of conducting such extensive and in-depth assessment work.

[7] For instance, in Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539) (2002/2/EC), the only reference made to access by public authorities to data originally processed for commercial purposes appears in recital 9 which states that: "*The Canadian Act covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests and to recognise certain information which exists in the public domain. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities, such as the Federal Privacy Commissioner invested with powers of investigation and intervention. Furthermore, the provisions of Canadian law regarding civil liability apply in the event of unlawful processing which is prejudicial to the persons concerned."*

**recommends that the Commission make this assessment as soon as possible to ensure a fully-fledged revision of those Decisions. As noted above, recital 7 of both draft decisions indicates that the proposed modifications is to ensure a "*full implementation of the Schrems judgement*" but instead only appear to address the conclusions of the CJEU on the powers of the national supervisory authorities and this should be made clearer in the draft decisions.**

**In addition, the present analysis does not cover the modifications needed to those Commission decisions in the light of the future entry into application of the General Data Protection Regulation.**

## III. Draft decision on standard contractual clauses

The European Commission is proposing to replace the content of Article 4 of Commission Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses (hereinafter: "SCC")[8].

The Working Party 29 would like to underline the fact that current Article 4 of Commission Decisions 2001/497/EC and 2010/87/EU on SCC is different from the article 3 of Safe Harbor decision. Article 4 of SCC is listing alternative situations for which DPA may exercise their existing powers to prohibit or suspend data flows to third countries while Article 3.1.b of Safe Harbor adequacy decision was imposing cumulative criteria.

However, the Working Party 29 welcomes the intention of the European Commission to avoid any additional conditions which might limit the DPAs' power of intervention.

As the Court confirmed: "*neither Article 8(3) of the Charter nor Article 28 of Directive 95/46/EC excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46*[9]". Recital 3 of the draft decision on standard contractual clauses adequately takes this into consideration.

However, recital 5 of the draft decision on standard contractual clauses is interpreting Case C-362/14 CJEU judgement and may be read as creating a duty for the supervisory authorities to always authorize transfers based on SCC. It is key to underline that the binding character does not prevent national supervisory authorities suspending or prohibiting personal data flows in order to protect rights and liberties of individuals. Therefore, **the Working party 29 suggests amending recital 5 to ensure its consistency with proposed recital 3 of the draft decision. A solution is to add the**

[8] To delete the content of current paragraphs 1 and 2 of Article 4 of Commission Decision 2010/87/EU and paragraphs 1 to 3 of Article 4 of Decision 2001/497/EC and to modify the last paragraph of Article 4 of both Decisions.

[9] Paragraph 54 of Case C-362/14 CJEU judgement.

**following recital: "*However, neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission Decision pursuant to Article 26.4 of Directive 95/46*"**[10].

**The Working Party 29 recommends adding in the recitals examples under which DPAs may exercise their powers to prohibit or suspend data flows to third countries.** According to the Working Party 29, the Case C-362/14 CJEU judgement requires the deletion of any condition which purports to restrict the power of DPAs but it does not prevent the European Commission from giving non exhaustive examples under which DPAs may exercise their powers. Those examples would be used by DPAs when exercising their competence and facilitate their work by **bringing more legal certainty**. **The European Commission gave similar clarifications in recital 60 of the Privacy Shield adequacy decision**, stating that the conditions under which a data importer handles data may also lead to violation of EU data protection law. Clarification is also needed for Decisions relating to Standard contractual clauses.

Therefore, **the Working party recommends complementing recital 3 by adding the following** : "*For instance, where a national supervisory authority, upon complaint or on its own initiative, considers that the transfer of personal data is carried out in violation of EU or national data protection law, such as when the data importer has not respected the standard contractual clauses or when the legislation applicable to the data importer imposes upon him requirements which go beyond the restrictions strictly necessary in a democratic society, it can exercise its powers vis-a-vis the data exporter and order the suspension or the ban of the data transfer."*

## IV. Draft decision on adequacy

As regards the DPAs powers, the Working Party 29 welcomes the article 1.1 of the draft decision, which acknowledges the powers of data protection authorities to suspend or ban the data flows[11].

Recitals 1 to 5 of the Draft decision directly refer to the Case C-362/14 CJEU judgement. Recitals 1 to 3 explain the prohibition on the European Commission restricting the DPAs powers and the fact that DPAs remain competent to oversee the transfers of personal data to a third country which has been the subject of a Commission adequacy decision. The two following recitals address the binding character of the Commission decisions and the prohibition for DPAs to adopt measures contrary to the Commission adequacy decision. There is however no further explanation on the manner those two purposes could be

[10] Application *Mutatis mutandis* of the Paragraph 54 of Case C-362/14 CJEU judgement.

[11] Note that this comment is made on the basis of Article 1 of the draft decision on adequacy, which refers to Commission Decision 2000/518/EC on the adequacy of Switzerland, but it also applies to all other corresponding decisions under amendment.

reconciled which would assist in ensuring that the adequacy decisions are applied uniformly.

**The Working Party 29 considers that there is a need to further explain how the European Court balanced the need to consider the European Commission decision as being legally binding against the necessity of preserving the powers of the DPAs**[12]. **The Court stated that the binding character of the Commission adequacy decision is notwithstanding the right of the national supervisory authorities to engage in legal proceedings** before the national courts, if they have doubts as to the validity of the Commission decision. This may then lead to a reference to the CJEU for a preliminary ruling for the purpose of examination of the decision's validity[13]. **This part is a core element** of the judgement of the Court **and should be explicitly incorporated** in the recital of the draft decisions.

Moreover, **the Working Party recommends clarifying that the exercise of this right to engage in legal proceedings includes the situation where the national supervisory authority considers that the data importer or any further recipient is subject to legal requirements which may interfere with the applicable data protection law in a manner which goes beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC.**

Furthermore, **in the same manner recital 60 of the Privacy Shield adequacy decision gave explanations** about the powers of DPAs to suspend or prohibit data flows based on article 28.3 of the EC Directive 95/46/EC (see also above Section III), **the Working Party 29 recommends stating, as an example, that this right may be exercised where the DPA considers that the transfer of personal data is carried out in violation of EU data protection law, including when the data importer or any further recipient is not complying with the applicable standard of protection subject to the relevant adequacy decision**. The absence of a similar recital may indicate a lack of consistency across all of the relevant Commission Decisions.

As regards the duty to monitor the adequacy decisions, the Working Party 29 welcomes the recitals 8 and 9 which further explain this duty of the European Commission to monitor the findings relating to adequacy decisions and in particular the developments concerning access to personal data by public authorities. In the same manner, the Working Party 29 welcomes article 1.2 relating to this monitoring duty.

[12] Such further explanation is in particular required as to whether and, if so, to what extent DPAs are entitled at least as interim measure to order suspension or prohibition of data flows if they are of the opinion that legislation applicable to the data importer imposes upon him requirements which go beyond the restrictions strictly necessary in a democratic society (see C465/93; C143/88 and joint cases C411/10 and C493/10).

[13] See § 65 of Case C-362/14 CJEU judgement.

Finally, **the Working Party 29 would like to propose the following additional drafting recommendations:**

- Under the first paragraph of article 1.2[14], reference should not only be made to the legal order but also to the *"practices in the third country"*[15]*;*

- The 3rd paragraph of article 1.2[16] should be modified in the following manner: "*The Member States and the Commission shall inform each other of any indications that interferences by Swiss public authorities responsible for national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is strictly necessary* **in a democratic society**, *or that there is no effective legal protection against such interferences*".

[14] Note that this comment is made on the basis of Article 1 of the draft decision on adequacy, which refers to Commission Decision 2000/518/EC on the adequacy of Switzerland, but it also applies to all other corresponding decisions under amendment.

[15] Case C-362/14 CJEU judgement, para. 34, 37, 59, 66, 67.

[16] Note that this comment is made on the basis of Article 1 of the draft decision on adequacy, which refers to Commission Decision 2000/518/EC on the adequacy of Switzerland, but it also applies to all other corresponding decisions under amendment.

05/EN
WP108

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

**Adopted on April 14th, 2005**

The participation of data protection authorities in the approval of binding corporate rules is entirely voluntary. 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 74[1] ("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] 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 WP74[2].

3. **<u>Which data protection authority should you apply to?</u>**

   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 responsibilities[3];

      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.

---

[2] WP74 sets out the requirements for binding corporate rules.

[3] 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

ARTICLE 29 Data Protection Working Party

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

## 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[1]" 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[2].

## 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[3]; 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.
- 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

---

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

[2] 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

[3] 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

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?<br>☐ Yes<br>☐ 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:<br>(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[4]

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

### INTERNAL BINDING NATURE[5]

***Binding within the entities of the Group[6]***

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[7]
- ☐ 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.)

[4] 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.

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

[6] See Section 5.3 WP108

[7] See also footnote 11

| ***Binding upon the employees***[8] |
|---|

| 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.<br><br>- Work employment contract<br><br>- Collective agreements (approved by workers committee/another body)<br><br>- Employees must sign or attest to have read the BCRs or related ethics guidelines in which the BCRs are incorporated<br><br>- BCRs have been incorporated in relevant company policies<br><br>- Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation<br><br>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***[9] |
|---|

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: |

[8] See Section 5.8 WP108

[9] See Section 5.10 WP108

## EXTERNALLY BINDING NATURE[10]

| 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[11]. |
|---|

| ***Legal claim or actions*** |
|---|
| Explain how you meet the obligations according to the requirement of paragraph 5.14. of WP 108[12]. |

| 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. |

[10] See Section 3.3.2 WP74 and Section 5.12 WP108

[11] 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.

[12] 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[13]

It is important to show how the BCRs in place within your organisation 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.)

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:

***Internal complaint handling[14]***

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

Please describe the system for handling complaints:

[13] See Section 5.2 WP74 and Section 6 WP108

[14] 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[15]

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?

[15] See Section 5.4 WP 74

## 7. DESCRIPTION OF PROCESSING AND DATA FLOWS[16]

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:

[16] See Section 7 WP108

## 8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[17]

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[18]

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.)

[17] See Section 9 WP108

[18] 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).

ARTICLE 29 DATA PROTECTION WORKING PARTY

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**

## 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 74[1] & WP 108[2],

- 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 133[3]),

- giving per principle the corresponding text references in documents WP 74[4] and WP 108[5] 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 Corpate 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) | The Group will have to explain in its application form how the rules are made binding :<br><br>i) Between the companies/entities in the group by one or more of:<br>Intra-group agreement,<br>Unilateral undertakings,<br>Internal regulatory measures,<br>Policies of the group, or<br>Other means<br><br>ii) On employees by one or more of:<br>Individual and separate agreement/undertaking with sanctions ,<br>Clause in employment contract with sanctions,<br>Internal policies with sanctions, or<br>Collective agreements with sanctions |
| **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 |
|---|---|---|---|---|
| **1.4 The company accepts liability for paying compensation and to remedy breaches of the BCR.** | YES | YES | 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) | 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.<br><br>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.<br><br>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. |
| **1.5 The company has sufficient assets.** | NO | YES | WP 74 point 5.5.2. §2 (page 18) + WP108 point 5.17. (page 6) | 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. |

| 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) | 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.<br><br>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. |
| **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) | The BCRs must contain the right for every data subject to have an easy access to the BCRs.<br><br>All data subjects beneficiating from the third party beneficiary right should also have easy access to this clause.<br><br>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). |
| **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) | 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.<br><br>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. |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments |
|---|---|---|---|---|
| **2.2 The existence of a complaint handling process for the BCR** | YES | YES | WP 74 point 5.3. (page 17) + WP 108 point 5.15 and 5.18 (page 6) | 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.<br><br>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.<br><br>The application form must explain how data subject will be informed about the practical steps of the complaint system, for instance:<br>- where to complain,<br>- in which form,<br>- delays for the reply on the complaint,<br>- consequences in case of rejection of the complaint<br>- consequences in case the complaint is considered as justified<br>- 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 |
|---|---|---|---|---|
| **2.3 The existence of an audit programme covering the BCRs** | YES | YES | WP 74 point 5.2. (page 16) + WP 108 point 6 (page 7) | 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).<br><br>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.<br><br>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.<br><br>The application form will contain a description of the audit system. For instance :<br>- which entity (department within the group) decides on the audit plan/programme,<br>- which entity will make the audit,<br>- time of the audit (regularly or on specific request from the appropriate Privacy function.)<br>- 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, …)<br>- 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 |
|---|---|---|---|---|
| **2.4 The creation of a network of privacy officers or appropriate staff for handling complaints and overseeing and ensuring compliance with the rules.** | YES | NO | WP 74, point 5.1 (page 16) and 5.3 (page 17) | 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.<br><br>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. |
| **3 - COOPERATION DUTY** | | | | |
| **3.1 A duty to cooperate with Data Protection Authorities** | 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** | | | | |
| **4.1 A description of the transfers covered by the BCRs** | YES | YES | WP 74 point 4.1 § 4 (page 14) + WP 108 point 7 (pages 7-8) | 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:<br>i) the nature of the data transferred<br>ii) the purposes of the transfer/processing<br>iii) the data importers/exporters in the EU and outside of the EU<br><br>Some Data Protection Authorities may require more detailed description of the transfers. |

| 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) | The BCRs should indicate if they apply to:<br>i) all personal data transferred from the European Union within the group OR,<br>ii) all processing of personal data made within the company group<br><br>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. |
| **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) | The BCRs can be modified (*for instance to take into account modifications of the regulatory environment or the company structure*) but they should impose a duty to report changes to all group members and to the Data Protection Authorities.<br><br>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 :<br>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.<br>ii) No transfer is made to a new member until the new member is effectively bound by the BCRs and can deliver compliance.<br>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:<br>i) Transparency, fairness<br>ii) Purpose limitation<br>iii) Data quality<br>iv) Security including the obligation to enter into contracts with all subcontractors/processors specifying the use of the data and the necessary security measures<br>v) Rights of access, rectification, objection to processing<br>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 | Even though it is not required by the WP 74 and 108, it is very useful to specifiy the relationship between the BCRs and the relevant applicable law.<br><br>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.<br><br>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. |

Done at Brussels, on 24/06/2008

*For the Working Party*
*The Chairman*
*Alex TÜRK*

ARTICLE 29 DATA PROTECTION WORKING PARTY

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**

## 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 of elements of those rules are in documents WP74[1] and WP108[2].

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 74[3] and WP 108[4].

[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 Corpate 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 EU[5].

[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 group[6], 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 proportionnality

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 effects 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 beneficiating 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 responsibilities[7] 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*

ARTICLE 29 DATA PROTECTION WORKING PARTY

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**

## 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 74[2] and WP 108[3]. 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 Corpate 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*

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 254

# Adequacy Referential (updated)

**Adopted on 28 November 2017**

## Introduction

The Working Party of EU Data Protection Authorities[1] (the WP29) has previously published a Working Document on transfers of personal data to third countries (WP12)[2]. With the replacement of the Directive by the EU General Data Protection Regulation (GDPR)[3], WP29 is revisiting WP12, its earlier guidance, to update it in the context of the new legislation and recent case law of the European Court of Justice (CJEU)[4].

This working document seeks to update Chapter One of WP12 relating to the central question of adequate level of data protection in a third country, a territory or one or more specified sectors within that third country or in an international organization (hereafter: "third countries or international organizations"). This document will be continuously reviewed and if necessary updated in the coming years, based on the practical experience gained through the application of the GDPR. Chapters 2 (*Applying the approach to countries that have ratified Convention 108*) and 3 (*Applying the approach to industry self-regulation*) of the WP12 document should be updated at a later stage.

This working paper is focused solely on adequacy decisions, which are implementing acts[5] of the European Commission, according to article 45 of the GDPR. Other aspects of transfers of personal data to third countries and international organizations will be examined in following working papers that will be published separately (BCRs, derogations).

This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations by establishing the core data protection principles that have to be present in a third country legal framework or an international organization in order to ensure essential equivalence with the EU framework. In addition, it may guide third countries and international organizations interested in obtaining adequacy. However, the principles set out in this working document are not addressed directly to data controllers or data processors.

The present document consists of 4 Chapters:

**Chapter 1:** Some broad information in relation to the concept on adequacy

**Chapter 2:** Procedural aspects for adequacy findings under the GDPR

**Chapter 3**: General Data Protection Principles. This chapter includes the core general data protection principles to ensure that the level of data protection in a third country or international organization is essentially equivalent to the one established by the EU legislation.

**Chapter 4:** Essential guarantees for law enforcement and national security access to limit the interferences to fundamental rights. This Chapter includes the essential guarantees for law enforcement and national security access following the CJEU Schrems judgment in 2015 and based on the Essential Guarantees WP29 working document adopted in 2016.

---

[1] As established under Article 29 of the EU Data Protection Directive 95/46/EC

2 WP12 , 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' adopted by the Working Part on 24 July 1998.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

4 Including Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015

[5] See relevant articles 45(3) and 93(2) of the GDPR for further information on the implementing acts

## Chapter 1: Some broad information in relation to the concept of adequacy

Article 45, paragraph (1) of the GDPR sets out the principle that data transfers to a third country or international organization shall only take place if the third country, territory or one or more specified sectors within that third country or the international organization in question, ensures an adequate level of protection.

This concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. At this point it is important to recall the standard set by the CJEU in Schrems, namely that while the "*level of protection*" in the third country must be "*essentially equivalent*" to that guaranteed in the EU, "*the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]*"[6]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States[7] that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union[8]. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules.

Article 45, paragraph (2) of the GDPR, establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organization.

For example, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into.

It is therefore clear that any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. It is upon the European Commission to verify – on a regular basis - that the rules in place are effective in practice.

The 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the EU Charter of Fundamental Rights and the GDPR. In addition, consideration should also be given to other international agreements on data protection, e.g. Convention 108.[9]

---

[6] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74);

[7] Article 288 (2) TFEU

[8] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 52);

9 Recital 105 of the GDPR

Attention must also be paid to the legal framework for the access of public authorities to personal data. Further guidance on this is provided in Working paper 237 (i.e. the Essential Guarantees document)[10] on safeguards in the context of surveillance.

General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable.

## Chapter 2: Procedural aspects for adequacy findings under the GDPR

For the EDPB to fulfil its task in advising the European Commission according to Article 70(1) (s) of the GDPR the EDPB should be provided with relevant documentation, including relevant correspondence and the findings made by the European Commission. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organization. In any case, the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country. The EDPB will provide an opinion on the European Commission's findings in due time and, identify insufficiencies in the adequacy framework, if any. The EDPB will also endeavor to propose alterations or amendments to address possible insufficiencies.

According to Article 45 (4) of the GDPR it is upon the European Commission to monitor – on an ongoing basis - developments that could affect the functioning of an adequacy decision.

Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

Given the mandate to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organization by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization. The EDPB would appreciate to be invited to participate in these review processes and missions.

It should also be noted that according to article 45 (5) of the GDPR the European Commission has the right to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend should consequently involve the EDPB by requesting its opinion pursuant art. 70(1) (s).

[10] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237, 13 April 2016

Furthermore, as now recognized in article 58 (5) of the GDPR and according to the CJEU's Schrems ruling, data protection authorities must be able to engage in legal proceedings if they find a claim by a person against an adequacy decision well founded: *"It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity"*[11].

**Chapter 3: General Data Protection Principles to ensure that the level of protection in a third country, territory or one or more specified sectors within that third country or international organization is essentially equivalent to the one guaranteed by the EU legislation**

**A third country's or international organisation's system must contain the following basic content and procedural/enforcement data protection principles and mechanisms:**

**A. <u>Content Principles:</u>**

**1) Concepts**

Basic data protection concepts and/or principles should exist. These do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data".

**2) Grounds for lawful and fair processing for legitimate purposes**

Data must be processed in a lawful, fair and legitimate manner.

The legitimate bases, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

**3) The purpose limitation principle**

Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

**4) The data quality and proportionality principle**

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

[11] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§ 65)

### 5) Data Retention principle

Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed.

### 6) The security and confidentiality principle

Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

### 7) The transparency principle

Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise**,** transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

### 8) The right of access, rectification, erasure and objection[12]

The data subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed.

The data subject should have the right to obtain rectification of his/her data as appropriate, for example, where they are inaccurate or incomplete and erasure of his/her personal data when, for example, their processing is no longer necessary or unlawful.

The data subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. In the GDPR, for example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

The exercise of those rights should not be excessively cumbersome for the data subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

[12] The non-existence of the rights to data portability or the restriction of processing in the third country's or international organization's system, should not be an obstacle for it to be recognized as ensuring essential equivalence with the EU framework. However, the existence of these rights would be considered as a plus.

### 9) Restrictions on onward transfers

Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.

## B. Examples of additional content principles to be applied to specific types of processing:

### 1) Special categories of data

Specific safeguards should exist where 'special categories of data are involved[13]. These categories should reflect those enshrined in Article 9 and 10 of the GDPR. This protection should be put in place, through more demanding requirements for the data processing such as for example, that the data subject gives his/her explicit consent for the processing or through additional security measures.

### 2) Direct marketing

Where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time.

### 3) Automated decision making and profiling

Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. In the European framework, such conditions include, for example, the need to obtain the explicit consent of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. The law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis.

[13] Such special categories are also known as "sensitive data" in recital 10 of the GDPR.

## C. Procedural and Enforcement Mechanisms:

**Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union[14], a system consistent with the European one must be characterized by the existence of the following elements:**

### 1) Competent Independent Supervisory Authority

One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.

### 2) The data protection system must ensure a good level of compliance

A third country system should ensure a high degree of accountability and of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials**.**

### 3) Accountability

A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.

### 4) The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.

Where rules are not complied with, the data subject should be provided as well with effective administrative and judicial redress, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

[14] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, para. 74.

**Chapter 4: Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights**

When assessing the adequacy of the level of protection, under Art 45(2)(a) the Commission is required to take into account "*relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation…*".

The CJEU in Schrems, noted that the "*term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*". Even though the means to which that third country has recourse, in this connection, may differ from those employed within the European Union, those means must nevertheless prove, in practice, effective[15].

In this context, the court also noted critically that the previous Safe Harbor decision did "*not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security.*"

The WP29 has identified in the opinion WP237, adopted on 13 April 2016, essential guarantees reflecting the jurisprudence of the CJEU and the ECHR in the field of surveillance. While the recommendations detailed in WP237 remain valid and should be taken into account when assessing the adequacy of a third country in the field of surveillance, the application of these guarantees may differ in the fields of law enforcement and national security access to data. Still those four guarantees need to be respected for access to data, whether for national security purposes or for law enforcement purposes, by all third countries in order to be considered adequate:

1) **Processing should be based on clear, precise and accessible rules (legal basis)**

2) **Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated**

3) **The processing has to be subject to independent oversight**

4) **Effective remedies need to be available to the individuals**

[15] See recital 74 of Case C-360/14 "Schrems"

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP 256

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

**(updated)**

**Adopted on 29 November 2017**

## INTRODUCTION

In order to facilitate the use of Binding Corporate Rules for Controllers (BCR-C) by a corporate group or a group of enterprises engaged in a joint economic activity for international transfers from organisations established in the EU to organisations within the same group established outside the EU, the Article 29 Working Party (WP29) has amended the Working Document 153 (which was adopted in 2008) setting up a table with the elements and principles to be found in Binding Corporate Rules in order to reflect the requirements referring to BCRs now expressly set out by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR)[1].

It should be recalled that BCR-Controllers are suitable for framing transfers of personal data from Controllers established in the EU to other Controllers or to Processors (established outside the EU) within the same group, whereas BCR-Processors (BCR-P) apply to data received from a Controller (established in the EU) which is not a member of the group and then processed by the concerned group members as Processors and/or Sub-processors. Hence the obligations set out in the BCR-C apply in relation to entities within the same group acting as controllers and to entities acting as 'internal' processors. As for this very last case, it is worth recalling that a contract or other legal act under Union or Member State law, binding on the processor with regard to the controller and which comprise all requirements as set out in Art. 28.3 GDPR, should be signed with all internal and external subcontractors/processors (i.e. Service Agreement). Indeed, the obligations set forth in the BCR-C apply to entities acting as 'internal' processor to the extent that this does not lead to a contradiction with the Service Agreement (i.e. the Processors members of the group processing on behalf of Controllers members of the group shall primarily abide by this contract).

Taking into account that Article 47.2 GDPR sets forth a minimum set of elements to be inserted within Binding Corporate Rules, this amended table is meant to:

- Adjust the wording of the previous referential so as to keep it in line with Article 47 GDPR,
- Clarify the necessary content of BCRs as stated in Article 47 (taking into account documents WP 74[2] & WP 108[3] adopted by the WP29 within the framework of the directive 95/46/EC),
- Make the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority (competent SA) in the BCRs application (document WP 133[4]),

[1] Text with EEA relevance.
[2] 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
[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
[4] Working Document WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, adopted on January 10, 2007, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc

- Give the principles the corresponding text references in Article 47 GDPR, and
- Provide explanations/comments on the principles one by one.

Article 47 GDPR is clearly modelled on the Working documents relating to BCRs adopted by the WP29. However, it specifies some new elements that need to be taken into account when updating already existing BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

### 1.1 New elements

In this perspective, the WP29 would like to draw attention in particular to the following elements:

- ***right to lodge a complaint***: Data subjects should be given the choice to bring their claim either before the Supervisory Authority ('SA') in the Member State of his habitual residence, place of work or place of the alleged infringement (pursuant to Art. 77 GDPR) or before the competent court of the EU Member States (choice for the data subject to act before the courts where the data exporter has an establishment or where the data subject has his or her habitual residence (Article 79 GDPR);
- ***Transparency***: All data subjects benefitting from the third party beneficiary rights should in particular be provided with information as stipulated in Articles 13 and 14 GDPR and information on their rights in regard to processing and the means to exercise those rights, the clause relating to liability and the clauses relating to the data protection principles;
- ***Scope of application***: The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members (GDPR Art. 47.2.a). The BCRs must also specify its material scope, for instance the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the types of data subjects affected and the identification of the recipients in the third country or countries (GDPR Art. 47.2.b);
- ***Data Protection principles***: Along with the principles of transparency, fairness, purpose limitation, data quality, security, the BCRs should also explain the other principles referred to in Article 47.2.d – such as, in particular, the principles of lawfulness, data minimisation, limited storage periods, guarantees when processing special categories of personal data, the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- ***Accountability***: Every entity acting as data controller shall be responsible for and able to demonstrate compliance with the BCRs (GDPR Art. 5.2);

- ***Third country legislation***: The BCRs should contain a commitment that where any legal requirement a member of the group of undertakings or group of enterprises engaged in a joint economic activity is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, the problem will be reported to the competent supervisory authority (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). This includes any legally binding request for disclosure of personal data by a law enforcement authority or state security body.

**1.2 Amendments of already adopted BCRs**

While in accordance with article 46-5 of the GDPR, authorisations by a Member State or supervisory authority made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority, groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements.

This document aims to assist those groups with approved BCRs in implementing the relevant changes to bring them in line with the GDPR. In addition, these groups are invited to notify the relevant changes to their BCRs as part of their obligation (under 5.1 of WP153) to all group members and to the DPAs via the Lead DPA under their annual update as of 25 May 2018.

Taking into account the above, the DPAs reserve their right to exercise their powers under article 46-5 of the GDPR.

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **1 - BINDING NATURE** | | | | | |
| **INTERNALLY** | | | | | |
| **1.1 The duty to respect the BCRs** | YES | YES | GDPR Art. 47.1.a and 47.2.c | The BCRs must be legally binding and shall contain a clear duty for each participating member of the Group of undertakings or group of enterprises engaged in a joint economic activity ('BCR member') including their employees to respect the BCRs. | |
| **1.2 An explanation of how the rules are made binding on the BCR members of the group and also the employees** | NO | YES | GDPR Art. 47.1.a and 47.2.c | The Group will have to explain in its application form how the rules are made binding :<br><br>i) For each participating company/entity in the group by one or more of:<br><br>- Intra-group agreement,<br>- Unilateral undertakings (this is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs),<br>- Other means (only if the group demonstrates how the binding character of the BCRs is achieved) | |

[5] To be completed by applicant.

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | ii) On employees by one or more of:<br><br>- Individual and separate agreement(s)/undertaking with sanctions,<br>- Clause in employment contract with a description of applicable sanctions,<br>- Internal policies with sanctions, or<br>- Collective agreements with sanctions | |
| **EXTERNALLY** | | | | | |
| **1.3 The creation of third-party beneficiary rights for data subjects. Including the possibility to lodge a complaint before the competent DPA and before the courts** | YES | YES | GDPR Art. 47.1.b, e and 47.2.c | The BCRs must expressly confer rights on data subjects to enforce the rules as third-party beneficiaries.<br><br>Data subjects must at least be able to enforce the following elements of the BCRs:<br><br>- Data protection principles (Art. 47.2.d and Section 6.1 of this referential),<br>- Transparency and easy access to BCRs (Art. 47.2.g and Section 6.1, Section 1.7 of this referential),<br>- Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (GDPR Art. 47.2.e and Art. 15, 16, 17,18, 21, 22),<br>- National legislation preventing respect of BCRs (Art. 47.2.m and Section 6.3 of this referential),<br>- Right to complain through the internal complaint mechanism of the companies (Art. 47.1.j and Section 2.2 of this referential), | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | - Cooperation duties with Data Protection Authority (Art. 47.2.k and l, Section 3.1 of this referential),<br>- Liability and jurisdiction provisions (Art. 47.2.e and f, Section 1.3, 1.4 of this referential). In particular, the BCRs must confer the right to lodge a complaint with the competent supervisory authority (choice before the SA in the Member State of his habitual residence, place of work or place of the alleged infringement, pursuant to art. 77 GDPR) and before the competent court of the EU Member States (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to Article 79 GDPR).<br><br>The BCRs should expressly confer to the data subjects the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCRs as enumerated above (see Articles 77 – 82 GDPR).<br>Companies should ensure that all those rights are covered by the third party beneficiary clause of their BCRs by, for example, making a reference to the clauses/sections/parts of their BCRs where these rights are regulated or by listing them all in the said third party beneficiary clause.<br>These rights do not extend to those elements of the BCRs pertaining to internal mechanisms implemented within entities such as detail of training, audit programmes, compliance network, | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | and mechanism for updating of the rules. | |
| **1.4 The EU headquarters, EU member with delegated data protection responsibilities or the data exporter accepts liability for paying compensation and to remedy breaches of the BCRs.** | YES | YES | GDPR Art. 47.2.f | The BCRs must contain a duty for the EU headquarters, or the EU BCR member with delegated responsibilities to accept responsibility for and to agree to take the necessary action to remedy the acts of other members outside of the EU bound by the BCRs and to pay compensation for any material or non-material damages resulting from the violation of the BCRs by BCR members.<br><br>The BCRs must also state that, if a BCR member 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 BCR member that has accepted responsibility and liability as if the violation had been caused by them in the Member State in which they are based instead of the BCR member outside the EU.<br><br>Another option, in particular if it is not possible for a group with particular corporate structures to impose on a specific entity to take all the responsibility for any breach of BCRs outside of the EU, it may provide that every BCR member exporting data out of the EU on the basis of the BCR will be liable for any breaches of the BCRs by the BCR member established outside the EU which received the data from this EU BCR member. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **1.5 The company has sufficient assets.** | NO | YES | [WP 74 point 5.5.2. §2 (page 18) + WP108 point 5.17. (page 6)] | The application form must contain a confirmation that any BCR member that has accepted liability for the acts of other members bound by the BCRs outside of the EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs. | |
| **1.6 The burden of proof lies with the company not the individual.** | YES | YES | GDPR Art. 47.2.f | BCRs must state that the BCR member that has accepted liability will also have the burden of proof to demonstrate that the BCR member outside the EU is not liable for any violation of the rules which has resulted in the data subject claiming damages.<br><br>If the BCR member that has accepted liability can prove that the BCR member outside the EU is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **1.7 Transparency and easy access to BCRs for data subjects** | YES | NO | GDPR Art. 47.2.g | All data subjects benefitting from the third party beneficiary rights should in particular be provided with the information as required by Articles 13 and 14 GDPR, information on their third party beneficiary rights with regard to the processing of their personal data and on the means to exercise those rights, the clause relating to the liability and the clauses relating to the data protection principles.<br><br>The information must be complete and not only summarized.<br><br>The BCRs must contain the right for every data subject to have an easy access to them. For instance, the BCRs may state that at least the parts of the BCRs on which information to the data subjects is mandatory (as described in the previous paragraph) will be published on the internet or on the intranet (when data subjects are only the company staff having access to the intranet). | |
| **2 - EFFECTIVENESS** | | | | | |
| **2.1 The existence of a suitable training programme** | YES | YES | GDPR 47.2.n | The BCRs must state that appropriate training on the BCRs will be provided to personnel that have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data.<br><br>The Supervisory Authorities evaluating the BCRs may ask for examples and explanations of the training programme during the application procedure. The training programme should be specified in the application. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **2.2 The existence of a complaint handling process for the BCRs** | YES | YES | GDPR 47.2.i and 12.3 | An internal complaints handling process must be set up in the BCRs to ensure that any data subject should be able to exercise his/her rights and complain about any BCR member.<br><br>- The complaints must be dealt with, without undue delay and in any event within one month, by a clearly identified department or person with an appropriate level of independence in the exercise of his/her functions. Taking into account the complexity and number of the requests, that one month period may be extended at maximum by two further months,, in which case the data subject should be informed accordingly.The application form must explain how data subjects will be informed about the practical steps of the complaint system, in particular:<br>- Where to complain,<br>- In what form,<br>- Delays for the reply on the complaint,<br>- Consequences in case of rejection of the complaint,<br>- Consequences in case the complaint is considered as justified,<br>- Consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court and a complaint before the Supervisory Authority) . | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **2.3 The existence of an audit programme covering the BCRs** | YES | YES | GDPR Art. 47.2.j and l and Art. 38.3, | 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) to ensure verification of compliance with the BCRs.<br><br>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 relevant board of the controlling undertaking of a group or of the group of enterprises engaged in a joint economic activity. Where appropriate, the result may be communicated to the ultimate parent's board.<br><br>The BCRs must state that Supervisory Authorities can have access to the results of the audit upon request and give the SAs the authority/power to carry out a data protection audit of any BCR member if required.<br><br>The application form will contain a description of the audit system. For instance :<br><br>- Which entity (department within the group) decides on the audit plan/programme,<br>- Which entity will conduct the audit,<br>- Time of the audit (regularly or on specific request from the appropriate Privacy function.)<br>- Coverage of the audit (for instance, applications, IT systems, databases that | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | 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, …)<br>- Which entity will receive the results of the audits | |
| **2.4 The creation of a network of data protection officers (DPO) or appropriate staff for monitoring compliance with the rules.** | YES | NO | GDPR Art. 47.2.h and Art. 38.3 | A commitment to designate a DPO where required in line with article 37 of the GDPR or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs enjoying the highest management support for the fulfilling of this task.<br><br>The DPO or the other privacy professionals can be assisted by a team, a network of local DPOs or local contacts as appropriate. The DPO shall directly report to the highest management level (GDPR Art. 38-3). The BCRs should include a brief description of the internal structure, role, position and tasks of the DPO or similar function and the network created to ensure compliance with the rules. For example, that the DPO or chief privacy officer informs and advises the highest | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | management, deals with Supervisory Authorities' investigations, monitors and annually reports on compliance at a global level, and that local DPOs or local contacts can be in charge of handling local complaints from data subjects, reporting major privacy issues to the DPO, monitoring training and compliance at a local level. | |
| **3 - COOPERATION DUTY** | | | | | |
| **3.1 A duty to cooperate with SAs** | YES | YES | GDPR Art. 47. 2.l | The BCRs should contain a clear duty for all BCR members to co-operate with, to accept to be audited by the Supervisory Authorities and to comply with the advice of these Supervisory Authorities on any issue related to those rules. | |
| **4 - DESCRIPTION OF PROCESSING AND DATA FLOWS** | | | | | |
| **4.1 A description of the material scope of the BCRs (nature of data transferred, type of data subjects, countries)** | YES | YES | GDPR Art. 47.2.b | The BCRs must specify their material scope and therefore contain a general description of the transfers so as to allow the Supervisory Authorities to assess that the processing carried out in third countries is compliant. The BCRs must in particular, specify the data transfers or set of transfers, including the nature and categories of personal data, the type of processing and its purposes, the types of data subjects affected (data related to employees, customers, suppliers and other third parties as part of its respective regular business activities) and the identification of the recipients in the third country or countries. | |
| **4.2 A statement of the geographical scope of the BCRs** | YES | YES | GDPR art 47.2.a | The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its Members. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | The BCRs should indicate if they apply to:<br>i) All personal data transferred from the European Union within the group OR,<br>ii) All processing of personal data within the group | |
| **5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES** | | | | | |
| **5.1 A process for updating the BCRs** | YES | YES | GDPR Art. 47.2.k | The BCRs can be modified (*for instance to take into account modifications of the regulatory environment or the company structure*) but they should impose a duty to report changes without undue delay to all BCR members and to the relevant Supervisory Authorities, via the competent Supervisory Authority.<br><br>Updates to the BCRs or to the list of the Members of the BCRs are possible without having to re-apply for an approval providing that :<br><br>i) An identified person keeps a fully updated list of the BCR members and keeps track of and record any updates to the rules and provide the necessary information to the data subjects or Supervisory Authorities upon request.<br>ii) No transfer is made to a new BCR member until the new BCR member is effectively bound by the BCRs and can deliver compliance.<br><br>Any changes to the BCRs or to the list of BCR members should be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update. Where a modification would possibly affect the level of the protection offered by the BCRs or | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | significantly affect the BCRs (i.e. changes to the binding character), it must be promptly communicated to the competent Supervisory Authority. | |
| **6 - DATA PROTECTION SAFEGUARDS** | | | | | |
| **6.1.1 A description of the data protection principles including the rules on transfers or onward transfers out of the EU.** | YES | YES | GDPR art. 47.2.d | The BCRs should explicitly include the following principles to be observed by the company:<br><br>i. Transparency, fairness and lawfulness (GDPR Art. 5.1.a, 6, 9, 10, 13 and 14)<br>ii. Purpose limitation (GDPR Art.5.1.b)<br>iii. Data minimisation and accuracy (GDPR Art. 5.1.c and d)<br>iv. Limited storage periods (GDPR Art. 5.1.e)<br>v. Processing of special categories of personal data<br>vi. Security (GDPR Art. 5.f and 32) including the obligation to enter into contracts with all internal and external subcontractors/processors which comprise all requirements as set out in Art. 28.3 GDPR and as well the duty to notify without undue delay any personal data breaches to the EU headquarters or the EU BCR member with delegated data protection responsibilities and the other relevant Privacy Officer/Function and data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms . Furthermore, any personal data breaches should be documented (comprising the facts relating to the personal data breach, its effects and the remedial action taken) and the documentation should be made available to the supervisory authority on request (GDPR Art. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | 33 and 34).<br>ii. Restriction on transfers and onward transfers to processors and controllers which are not part of the group (BCR members that are controllers can transfer data to processors/controllers out of the group that are located outside of the EU provided that adequate protection is provided according to Articles 45, 46, 47 48 GDPR, or that a derogation according to 49 GDPR applies)<br><br>The wording and definitions of the BCRs key principles should be consistent with the wording and definitions of the GDPR. | |
| **6.1.2 Accountability and other tools** | YES | YES | GDPR Art. 47.2.d and Art. 30 | Every entity acting as data controller shall be responsible for and able to demonstrate compliance with the BCRs (GDPR Art. 5.2 and 24).<br><br>In order to demonstrate compliance, BCR members need to maintain a record of all categories of processing activities carried out in line with the requirements as set out in Art. 30.1 GDPR. This record should be maintained in writing, including in electronic form, and should be made available to the supervisory authority on request.<br><br>In order to enhance compliance and when required, data protection impact assessments should be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (GDPR Art. 35). Where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | taken by the controller to mitigate the risk, the competent supervisory authority, prior to processing, should be consulted (GDPR Art. 36).<br><br>Appropriate technical and organisational measures should be implemented which are designed to implement data protection principles and to facilitate compliance with the requirements set up by the BCRs in practice (data protection by design and by default (GDPR Art. 25) | |
| **6.2 The list of entities bound by BCRs** | NO | YES | GDPR 47.2.a | 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 (including contact details) bound by the BCRs and the need to inform the Supervisory Authorities and the data subjects 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 | GDPR Art. 47.2.m | A clear commitment that where a BCR member has reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCRs or has substantial effect on the guarantees provided by the rules, he will promptly inform the EU headquarters or the EU BCR member with delegated data protection responsibilities and 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).<br><br>In addition, the BCRs should contain a commitment that where any legal requirement a BCR member is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, the problem | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| | | | | should be reported to the competent SA. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. In such a case, the competent SA should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).<br><br>If in specific cases the suspension and/or notification are prohibited, the BCRs shall provide that the requested BCR member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.<br><br>If, in the above cases, despite having used its best efforts, the requested BCR member is not in a position to notify the competent SAs, it must commit in the BCRs to annually providing general information on the requests it received to the competent SAs (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).<br><br>In any case, the BCRs must state that transfers of personal data by a BCR member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Texts of reference | Comments | References to application/BCRs[5] |
|---|---|---|---|---|---|
| **6.4 A statement about the relationship between national laws and BCRs** | NO (not required, but welcomed) | NO (not required, but welcomed) | N/A | 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.<br><br>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 BCRs.<br><br>In any event personal data shall be processed in accordance to the applicable law as provided by the Article 5 of the GDPR and the relevant local legislation. | |

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP 257

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

**(updated)**

**Adopted on 29 November 2017**

## INTRODUCTION

In order to facilitate the use of Binding Corporate Rules for Processors (BCR-P) by a corporate group or a group of enterprises engaged in a joint economic activity for international transfers from organisations established in the EU to organisations within the same group established outside the EU, the Article 29 Working Party (WP29) has amended the Working Document 195 (which was adopted in 2012) setting up a table with the elements and principles to be found in Binding Corporate Rules in order to reflect the requirements referring to BCRs now expressly set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR).

It should be recalled that BCR-P apply to data received from a controller established in the EU which is not a member of the group and then processed by the group members as processors and/or sub processors; whereas BCRs for Controllers (BCR-C) are suitable for framing transfers of personal data from controllers established in the EU to other controllers or to processors established outside the EU within the same group. Hence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller.

According to Article 28.3 of the GDPR, a contract or another legal act under Union or Member State law that is binding on the processor with regard to the controller must be implemented between the controller and the processor. Such a contract or other legal act will be referred here as the "service agreement".

Taking into account that Article 47.2 of the GDPR lists a minimum set of elements to be contained within a BCR, this amended table is meant to:

- Adjust the wording of the previous referential so as to bring it in line with Article 47 GDPR,
- Clarify the necessary content of a BCR as stated in Article 47 and in document WP 204[1] adopted by the WP29 within the framework of the Directive 95/46/EC,
- Make the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority in the BCRs application (document WP 195a[2]), and
- Provide explanations/comments on each of the requirements.

Article 47 of the GDPR is clearly modelled on the Working documents relating to BCRs adopted by the WP29. However, it specifies some new elements that need to be taken into account when updating already existing approved BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

[1] Working Document WP204: Explanatory Document on the Processor Binding Corporate Rules, as last revised and adopted on 22 May 2015

[2] Working Document WP 195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, adopted on 17 September 2012

## 1. New elements

In this perspective, the WP29 would like to draw attention in particular to the following elements:

- ***Scope of application***: The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members (Art. 47.2.a GDPR). The BCRs must also specify its material scope, for instance the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the types of data subjects affected and the identification of the recipients in the third country or countries (Art. 47.2.b GDPR);

- ***Third party beneficiary rights***: Data subjects should be able to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR (Art. 28, 29, 79 GDPR).

- ***Right to lodge a complaint***: Data subjects should be given the choice to bring their claim either before the Supervisory Authority ('SA') in the Member State of his habitual residence, place of work or place of the alleged infringement (Art.77 GDPR) or before the competent court of the EU Member States (choice for the data subject to act before the courts where the data exporter has an establishment or where the data subject has his or her habitual residence (Article 79 GDPR)

- ***Data Protection principles***: Along with the obligations arising from principles of transparency, fairness, lawfulness, purpose limitation, data quality, security, the BCRs should also explain how other requirements, such as, in particular, in relation to data subjects rights, sub-processing and onward transfers to entities not bound by the BCRs will be observed by the processor;

- ***Accountability***: Processors will have an obligation to make available to the controller all information necessary to demonstrate compliance with their obligations including through audits and inspections conducted by the Controller or an auditor mandated by the Controller (Art. 28-3-h GDPR);

- ***Service Agreement***: The Service Agreement between the Controller and the Processor must contain all required elements as provided by Article 28 of the GDPR.

## 2. Amendments of already adopted BCRs

While in accordance with article 46-5 of the GDPR, authorisations by a Member State or supervisory authority made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority, groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements.

This document aims to assist those groups with approved BCRs in implementing the relevant changes to bring them in line with the GDPR. In addition, these groups are invited to notify the relevant changes to their BCRs as part of their obligation (under 5.1 of WP195) to all group members and to the DPAs via the Lead DPA under their annual update as of 25 May 2018.

Taking into account the above, the DPAs reserve their right to exercise their powers under article 46-5 of the GDPR.

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| **1 - BINDING NATURE** | | | | |
| **INTERNALLY** | | | | |
| **1.1 The duty to respect the BCRs** | YES | YES | The BCRs must be legally binding and shall contain a clear duty for each participating member of the Group of undertakings or group of enterprises engaged in a joint economic activity ("BCR member") including their employees to respect the BCRs.<br><br>The BCRs shall also expressly state that each Member including their employees shall respect the instructions from the controller regarding the data processing and the security and confidentiality measures as provided in the Service Agreement (Art. 28, 29 and 32 of the GDPR). | |
| **1.2 An explanation of how the rules are made binding on the members of the group and also the employees** | NO | YES | The Group will have to explain in its application form how the rules are made binding :<br><br>i) For each BCR member by one or more of:<br><br>- Intra-group agreement,<br>- Unilateral undertakings (this is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other BCR members ), or<br>- Other means (only if the group demonstrates how bindingness is achieved)<br><br>ii) On employees by one or more of:<br><br>- Individual and separate agreement/undertaking with sanctions, or Clause in employment contract with sanctions, or<br>- Internal policies with sanctions, or<br>- Collective agreements with sanctions. | |
| **EXTERNALLY** | | | | |
| **1.3 The creation of third-party beneficiary rights for data** | YES | YES | i) Rights which are directly enforceable against the processor | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| **subjects, including the possibility to lodge a complaint before the competent Supervisory Authorities and before the courts** | | | The BCRs must grant rights to data subjects to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR. In this regard, data subjects shall at least be able to enforce the following elements of the BCRs directly against the processor:<br><br>- Duty to respect the instructions from the controller regarding the data processing including for data transfers to third countries (Art. 28.3.a, 28.3.g., 29 GDPR and section 1.1, 6.1.ii and 6.1.iv of this referential),<br><br>- Duty to implement appropriate technical and organizational security measures (Art. 28.3.c and 32 GDPR and section 6.1.iv of this referential) and duty to notify any personal data breach to the controller (Art. 33.2 GDPR and section 6.1.iv of this referential),<br><br>- Duty to respect the conditions when engaging a sub-processor either within or outside the Group (Art. 28.2, 28.3.d . 28.4, 45, 46, 47 GDPR, section 6.1.vi and 6.1.vii of this referential),<br><br>Duty to cooperate with and assist the controller in complying and demonstrating compliance with the law such as for answering requests from data subjects in relation to their rights (Art. 28.3.e, 28.3.f, 28.3.h and sections 3.2, 6.1.i, 6.1.iii, 6.1.iv, 6.1. v and 6.1. 2 of this referential)<br><br>- Easy access to BCRs (Art.47.2.g GDPR and section 1.8 of this referential)<br><br>- Right to complain through internal complaint mechanisms ( Art.47.2.i and section 2.2 of this referential)<br><br>- Duty to cooperate with the supervisory authority (Art. 31, 47.2.l of GDPR and section 3.1 of this referential) | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | - Liability, compensation and jurisdiction provisions (Art.47.2.e, 79, 82 GDPR and sections 1.3, 1.5 and 1.7 of this referential).<br><br>- National legislation preventing respect of BCRs (Art.47.2.m and section 6.3 of this referential)<br><br>ii) Rights which are enforceable against the processor in case the data subject is not able to bring a claim against the controller :<br><br>The BCRs must expressly confer rights to data subjects to enforce the BCRs as third-party beneficiaries in case the data subject is not able to bring a claim against the data controller; because the data controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity.<br><br>In such a case, data subjects shall at least be able to enforce against the processor the following sections set out in this referential: 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3<br><br>The data subjects' rights as mentioned under i) and ii) shall cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress).<br><br>In particular, data subjects shall be entitled to lodge a complaint before the competent supervisory authority (choice between the supervisory authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to Article 79 of the GDPR).<br><br>Where the processor and the controller involved in the same processing | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | are found responsible for any damage caused by such processing, the data subject shall be entitled to receive compensation for the entire damage directly from the processor (Art. 82.4 GDPR) | |
| **1.4. Responsibility towards the Controller** | YES | YES | The BCRs shall be made binding towards the Controller through a specific reference to it in the Service Agreement which shall comply with art 28 of the GDPR.<br><br>Moreover, the BCR must state that the Controller shall have the right to enforce the BCR against any BCR member for breaches they caused, and, moreover, against the BCR member referred under point 1.5 in case of a breach of the BCRs or of the Service Agreement by BCR members established outside of EU or of a breach of the written agreement referred under 6.1.vii, by any external sub-processor established outside of the EU. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| **1.5 The company accepts liability for paying compensation and to remedy breaches of the BCRs.** | YES | YES | The BCRs must contain a duty for the EU headquarters of the Processor or the EU BCR member of the Processor with delegated responsibilities or the EU exporter processor (e.g. the EU party contracting with the controller) to accept responsibility for and to agree to take the necessary action to remedy the acts of other BCR members established outside of EU or breaches caused by external sub-processor established outside of EU and to pay compensation for any damages resulting from a violation of the BCRs.<br><br>This BCR member will accept liability as if the violation had taken place by him in the Member State in which he is based instead of the BCR member outside the EU or the external sub-processor established outside of EU. This BCR member may not rely on a breach by a sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities.<br><br>If it is not possible for some groups with particular corporate structures to impose all the responsibility for any type of breach of the BCRs outside of the EU on a specific entity, another option may consist of stating that each and every BCR member exporting data out of the EU will be liable for any breaches of the BCR by the sub-processors (internal or external of the group) established outside the EU which received the data from this EU BCR member. | |
| **1.6 The company has sufficient assets.** | NO | YES | The application form must contain a confirmation that any BCR member that has accepted liability for the acts of other BCR members outside of EU and/or for any external sub-processor established outside of EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs. | |
| **1.7 The burden of proof lies with the company not the individual.** | YES | YES | The BCRs must state that the BCR member that has accepted liability will have the burden of proof to demonstrate that the BCR member outside the EU or the external sub-processor is not liable for any violation of the rules which has resulted in the data subject claiming damages<br><br>The BCRs must also state that where the Controller can demonstrate that | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs, it will be for the BCR member of the group that accepted liability to prove that the BCR member outside of the EU or the external sub-processor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place<br><br>If the entity that has accepted liability can prove that the BCR member outside the EU is not responsible for the act, it may discharge itself from any responsibility/liability. | |
| **1.8 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 | Access for the Controller: The Service Agreement will ensure that the BCRs are part of the contract. BCRs will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access.<br><br>Access for Data Subjects: All data subjects benefiting from the third party beneficiary rights should, in particular, be provided with the information on their third party beneficiary rights with regard to the processing of their personal data and on the means to exercise those rights. The BCRs must stipulate the right for every data subject to have easy access to them. Relevant parts of the BCRs shall be published on the website of the Processor Group or other appropriate means in a way easily accessible to data subjects or at least a document including **all** (and not a summary of) the information relating to points 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2, 6.3 of this referential. | |
| **2 – EFFECTIVENESS** | | | | |
| **2.1 The existence of a suitable training programme** | YES | YES | The BCRs must state that appropriate training on the BCRs will be provided to personnel that have permanent or regular access to personal data who are involved in the collection of personal data or in the development of tools used to process personal data.<br><br>The Supervisory Authorities evaluating the BCRs may ask for some examples and explanation of the training programme during the application procedure and the training programme shall be specified in the application. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| **2.2 The existence of a complaint handling process for the BCRs** | YES | YES | The BCRs shall contain a commitment from the Processor Group to create a specific contact point for data subjects.<br><br>All BCR members shall have the duty to communicate a claim or request without delay to the Controller without obligation to handle it, (except if it has been agreed otherwise with the Controller).<br><br>The BCRs shall contain a commitment for the Processor to handle complaints from data subjects where the Controller has disappeared factually or has ceased to exist in law or became insolvent.<br><br>In all cases where the processor handles complaints, these shall be dealt without undue delay and in any event within one month by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions. Taking into account the complexity and number of the requests, that period may be extended by two further months at the utmost, in which case the data subject should be informed accordingly.<br><br>The application form must explain how data subjects will be informed about the practical steps of the complaint system, in particular :<br>- where to complain,<br>- in what form,<br>- delays for the reply on the complaint,<br>- consequences in case of rejection of the complaint<br>- consequences in case the complaint is considered as justified<br>- consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court/Supervisory Authority) | |
| **2.3 The existence of an audit programme covering the BCRs** | YES | YES | 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) to ensure the verification of compliance with the BCRs.<br><br>The BCRs must state that the audit programme covers all aspects of the | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | 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 relevant board of the controlling undertaking of a group or of the group of enterprises engaged in a joint economic activity but also will be made accessible to the Controller. Where appropriate, the result may be communicated to the ultimate parent's board.<br><br>The BCRs must state that the Supervisory Authorities competent for the Controller can have access to the results of the audit upon request and give the Supervisory Authorities the authority/power to carry out a data protection audit of any BCR member if required.<br><br>Any processor or sub-processor processing the personal data on behalf of a particular controller will accept, at the request of that controller, to submit their data processing facilities for audit of the processing activities relating to that controller which shall be carried out by the controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the Supervisory Authority.<br><br>The application form will contain a description of the audit system. For instance:<br>- Which entity (department within the group) decides on the audit plan/programme,<br>- Which entity will conduct the audit,<br>- Time of the audit (regularly or on specific request from the appropriate Privacy function.)<br>- 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, …)<br>- Which entity will receive the results of the audits. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | | |
| **2.4 The creation of a network of data protection officers (DPO) or appropriate staff for monitoring compliance with the rules** | YES | NO | A commitment to appoint a DPO where required in line with article 37 of the GDPR or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs. This person/entity shall enjoy the highest management support in exercising this function.<br><br>The DPO or other person/entity as mentioned, respectively, can be assisted, in exercising this function, by a team/a network of local DPOs or local contacts as appropriate. The DPO shall directly report to the highest management level (GDPR Art. 38.3).<br><br>A brief description of the internal structure, role, position and tasks of the DPO or similar function, as mentioned, and the team/network created to ensure compliance with the rules. For example, that the DPO or chief Privacy Officer informs and advises the highest management, deals with Supervisory Authorities' investigations, monitors and annually reports on BCRs compliance at a global level, and that local DPOs or local contacts are in charge of reporting major privacy issues to the DPO or chief privacy officer, monitoring training and compliance at a local level. | |
| **3 – COOPERATION DUTY** | | | | |
| **3.1 A duty to cooperate with Supervisory Authorities** | YES | YES | The BCRs shall contain a clear duty for all BCR members to cooperate with and to accept to be audited by the Supervisory Authorities competent for the relevant controller and to comply with the advice of these Supervisory Authorities on any issue related to those rules. | |
| **3.2 A duty to cooperate with the Controller** | YES | YES | The BCRs shall contain a clear duty for any processor or sub-processor to co-operate and assist the Controller to comply with data protection law (such as its duty to respect the data subject rights or to handle their complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities). This shall be done in a reasonable time and to the extent reasonably possible. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| **4 – DESCRIPTION OF PROCESSING AND DATA FLOWS** | | | | |
| **4.1 A description of the transfers and material scope covered by the BCRs** | YES | YES | The BCRs shall contain a list of BCR members, i.e. entities that are bound by the BCRs (see also point 6.2)<br><br>The Processor submitting a BCR shall give a general description to the Supervisory Authority of the material scope of the BCRs (expected nature of the data transferred, categories of personal data, types of data subjects concerned by the transfers, anticipated types of processing and its purposes and data importers/exporters in the EU and outside of the EU). | |
| **4.2 A statement of the geographical scope of the BCRs (nature of data, type of data subjects, countries)** | YES | YES | The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of the BCR members.<br><br>The BCRs shall indicate that it is up to the Controller to apply the BCRs to:<br>i) All personal data processed for processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), OR;<br>ii) All processing of data processed for processor activities within the group whatever the origin of the data. | |
| **5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES** | | | | |
| **5.1 A process for updating the BCRs** | YES | YES | The BCRs can be modified (for instance to take into account modifications of the regulatory environment or the company structure) but they shall impose a duty to report changes to all BCR members, to the competent Supervisory Authorities and to the controller.<br><br>Where a change affects the processing conditions, the information should be given to the controller in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the modification is made (for instance, on any intended changes concerning the addition or replacement of subcontractors, before the data are communicated to the new sub-processor). | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | Updates to the BCRs or to the list of the BCR members are possible without having to re-apply for an authorization providing that:<br><br>i) An identified person keeps a fully updated list of the BCR members and of the sub-processors involved in the data processing activities for the controller which shall be made accessible to the data controller, data subject and Supervisory Authorities.<br><br>ii) This person will keep track of and record any updates to the rules and provide the necessary information systematically to the data controller and upon request to Supervisory Authorities upon request.<br><br>iii) No transfer is made to a new BCR member until the new BCR member is effectively bound by the BCR and can deliver compliance.<br><br>iv) Any substantial changes to the BCRs or to the list of BCR members shall be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update. Where a modification would affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes in the bindingness), it must be promptly communicated to the competent Supervisory Authority. | |
| **6 - DATA PROTECTION SAFEGUARDS** | | | | |
| **6.1 A description of the privacy principles including the rules on transfers or onward transfers outside of the EU** | YES | YES | The BCRs shall include the following principles to be observed by any BCR member:<br><br>i) Transparency, fairness, and lawfulness: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law (for instance, to be transparent about sub-processor activities in order to allow the controller to correctly inform the data subject); | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | ii) Purpose limitation: duty to process the personal data only on behalf of the controller and in compliance with its documented instructions including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest (Art. 28-3-a of the GDPR). In other cases, if the processor cannot provide such compliance for whatever reasons, it agrees to inform promptly the data controller of its inability to comply, in which case the controller is entitled to suspend the transfer of data and/or terminate the contract.<br><br>On the termination of the provision of services related to the data processing, the processors and sub-processors shall, at the choice of the controller, delete or return all the personal data transferred to the controller and delete the copies thereof and certify to the controller that it has done so, unless legislation imposed upon them requires storage of the personal data transferred. In that case, the processors and the sub-processors will inform the controller and warrant that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.<br><br>iii) Data quality: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law, in particular:<br><br>- Processors and sub-processors will execute any necessary measures when asked by the Controller, in order to have the data updated, corrected or deleted. Processors and sub-processors will inform each BCR member to whom the data have been disclosed of any rectification, or deletion of data.<br>- Processors and sub-processors will execute any necessary measures, when asked by the Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | anymore. Processor and sub-processors will communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data.<br><br>iv) Security: Processors and sub-processors will have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of the GDPR. Processors and sub-processors will also have a duty to assist the Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of processing and information available to the processor (Art.28-3-f of the GDPR). Processors and sub-processors must implement technical and organisational measures which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement. Processors shall inform the Controller without undue delay after becoming aware of any personal data breach. In addition, sub-processors shall have the duty to inform the Processor and the Controller without undue delay after becoming aware of any personal data breach.<br><br>v) Data subject rights: Processors and sub-processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the controller, for the fulfilment of the controller's obligations to respond to requests for exercising the data subjects rights as set out in Chapter III of the GDPR (Art. 28-3-e of the GDPR) including by communicating any useful information in order to help the controller to comply with the duty to respect the rights of the data subjects. Processor and sub-processors will transmit to the controller any data subject request without answering it unless he is authorised to do so. | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | vi) Sub-processing within the Group: data may be sub-processed by other BCR members bound by the BCRs only with the prior informed specific or general written authorization of the controller[3]. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new sub-processor. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of a sub-processor in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new sub-processor.<br><br>vii) Onward transfers to external sub-processors: Data may sub processed by non-members of the BCRs only with the prior informed specific or general written authorization of the controller[4]. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of sub-processors in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new sub-processor.<br><br>Where the BCR member bound by the BCRs subcontracts its obligations under the Service Agreement, with the authorization of the controller, it shall do so only by way of a contract or other legal act under Union or Member State law with the sub-processor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the same data protection obligations as set out in the Service Agreement between the controller and the processor and sections 1.3, 1.4, 3 and 6 of this referential are imposed on the sub- | |

[3] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.
[4] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | processor, in particular providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that the processing will meet the requirements of the GDPR (Art. 28-4 of the GDPR). | |
| **6.1.2 Accountability *and other tools*** | YES | YES | Processors will have a duty to make available to the controller all information necessary to demonstrate compliance with their obligations as provided by Article 28-3-h of the GDPR and allow for and contribute to audits, including inspections conducted by the controller or another auditor mandated by the controller. In addition, the processor shall immediately inform the controller if in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.<br><br>In order to demonstrate compliance with the BCRs, BCR members need to maintain a record of all categories of processing activities carried out on behalf of each controller in line with the requirements as set out in Art. 30.2 GDPR. This record should be maintained in writing, including in electronic form and should be made available to the supervisory authority on request (Art.30.3 and 30.4 GDPR)<br><br>The BCR members shall also assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice such as data protection by design and by default (Art. 25 and 47.2.d GDPR) | |
| **6.2 The list of entities bound by BCRs** | YES | YES | BCR shall contain a list of the entities bound by the BCRs including contact details. | |
| **6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs** | YES | NO | A clear commitment that where a BCR member has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the controller or its obligations under the BCRs or Service Agreement, it will promptly notify this to the controller which is entitled to suspend the transfer of data and/or terminate the contract, to the EU headquarter processor or EU member with delegated data protection responsibilities or the other relevant Privacy Officer/function, but also to the Supervisory Authority | |

| Criteria for approval of BCRs | In the BCRs | In the application form | Comments | References to Application/BCRs |
|---|---|---|---|---|
| | | | competent for the controller and the Supervisory authority competent for the processor.<br><br>Any legally binding request for disclosure of the personal data by a law enforcement authority or state security body shall be communicated to the controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the controller and the competent Supervisory Authority for the processor should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited). | |
| **6.4 A statement about the relationship between national laws and BCRs** | YES | NO | BCRs shall specify the relationship between the BCRs and the relevant applicable law.<br><br>The BCRs shall 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 BCRs.<br><br>In any event data shall be processed in accordance with the applicable law. | |

## II. COMMITMENTS TO BE TAKEN IN THE SERVICE LEVEL AGREEMENT

The BCRs for Processors shall unambiguously be linked to the Service Level Agreement signed with each Client. To that extent, it is important to make sure in the Service Level Agreement which must contain all required elements provided by Article 28 of the GDPR that:

- BCRs will be made binding through a specific reference to it in the SLA (as an annex).
- The Controller shall commit that if the transfer involves special categories of data the Data Subject has been informed or will be informed before the transfer that his data could be transmitted to a third country not providing adequate protection;
- The Controller shall also commit to inform the data subject about the existence of processors based outside of EU and of the BCRs. The Controller shall make available to the Data Subjects upon request a copy of the BCRs and of the service agreement (without any sensitive and confidential commercial information);
- Clear confidentiality and security measures are described or referred with an electronic link;
- A clear description of the instructions and the data processing;
- The service agreement will precise if data may be sub-processed inside of the Group or outside of the group and will precise if the prior authorization to it expressed by the controller is general or needs to be given specifically for each new sub-processing activities.

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP263 rev.01

# Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR

**Adopted on 11 April 2018**

## Introduction

The procedure for approving binding corporate rules (BCRs) for controllers and processors is laid out by provisions contained in Articles 47.1, 63, 64 and (only if necessary) 65 of the Regulation (EU) 2016/679 (GDPR).

As a result, binding corporate rules are to be approved by the competent supervisory authority[1] in the relevant jurisdiction in accordance with the consistency mechanism set out in Article 63, under which the European Data Protection Board (EDPB) will issue a non-binding opinion on the draft decision submitted by the competent Supervisory Authority (Article 64 GDPR).

As the group applying for approval of its BCRs may have entities in more than one Member State, this procedure may involve a number of concerned Supervisory Authorities (SAs)[2], e.g. in those countries from where the transfers are to take place. However, the GDPR does not lay down specific rules for the cooperation phase which should take place among the concerned SAs in advance of referral to the EDPB. It also does not set out specific rules for identifying the competent SA – which will act as Lead Authority for the BCRs ('BCR Lead')[3]. The role of such BCR Lead includes acting as a single point of contact with the applicant organization or group during the approval process and managing the application procedure in its cooperation phase.

The aim of this document is to update the WP 107 and identify smooth and effective cooperation procedures in line with the GDPR whilst taking full advantage of the previous fruitful experience of the Data Protection Authorities in dealing with the approval of BCRs.

This document will be reviewed and if necessary updated, based on the practical experience gained through the application of the GDPR.

---

[1] Article 57.1.s GDPR states that "without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory […] approve binding corporate rules pursuant to Article 47" and Article 58.3.j GDPR according to which each supervisory authority shall have the "authorisation and advisory powers […] to approve binding corporate rules pursuant to Article 47".

[2] Pursuant to Article 4(22) (a) and (b), a 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing". As for the BCRs approval procedure, the concerned SAs are the SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a Member State may provide services to controllers in several – potentially all – Member States).

[3] The "BCR Lead" is generally distinct from the "OSS Lead" considering that BCR transfers will not as a rule meet the definition/criteria of a cross-border processing operation. However, there could be cases in which the same SA could be the BCR Lead and the OSS Lead. This might e.g. be the case if a transfer performed by one establishment substantially affects data subjects in more than one MS (i.e. if personal data are first sent from member states A, B and C to the controller's establishment in member state A, and subsequently transferred by this establishment in A to a third country or, in case of BCR-P, where the processor carries out the same transfers for all their clients in the different member states). In any case, the BCR approval procedure would be the specific one settled by Article 64 GDPR.

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 (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

## 1. Identification of the BCR Lead Supervisory Authority

1.1 A group of undertakings, or group of enterprises engaged in a joint economic activity ('Group'), interested in submitting draft binding corporate rules (BCRs) for the approval of the competent Authority according to Articles 47, 63 and 64 GDPR should propose a SA as the BCR Lead. The decision as to which SA should act as BCR Lead is based upon the criteria contained in this document (see next paragraph). It is for the organisation to justify the reasons why a given SA should be considered as the BCR Lead.

1.2 An applicant Group should justify the proposal of the BCR Lead on the basis of relevant criteria such as:

a. the location(s) of the Group's European headquarters;

b. the location of the company within the Group with delegated data protection responsibilities[4];

c. 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;

d. the place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) are taken; and

e. the member state within the EU from which most or all transfers outside the EEA will take place.

1.3 Particular attention will be given to factor described under 1.2 (a) above.

1.4 These are not formal criteria. The SA to which the application is sent (as prospective BCR Lead SA) will exercise its discretion in deciding whether it is in fact the most appropriate lead SA and, in any event, the SAs among themselves may decide to allocate the application to a SA other than the one to which the Group applied (see next paragraph), in particular if it would be possible and worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

[4] According to Article 47.2.f GDPR, there should always be an EU based member of the group established on the territory of a Member State accepting liability for any breaches of the binding corporate rules by any member concerned not established in the Union. If the headquarters of the group were somewhere else, the headquarters should delegate these responsibilities to a member based in the EU.

1.5 The applicant should also provide the proposed BCR Lead (the entry point) with all appropriate information (both on paper and electronically to facilitate further distribution) which justifies its proposal, *inter alia*, the nature and general structure of the processing activities in the EU with particular attention to the place/s where decisions are made, the location and nature of affiliates in the EU, the number of employees or persons concerned, the means and purposes of the processing, the places from where the transfers to third countries do take place and the third countries to which those data are transferred.

## 2. **Cooperation procedure for the approval of BCRs**

2.1 The proposed BCR Lead will forward the information received as to why that SA has been selected by the company to be the lead authority for the BCRs to all SAs concerned[5] with an indication of whether or not it agrees to be the BCR Lead. If the entry point agrees to be the lead authority, the other concerned SAs will be asked, under Article 57.1.g GDPR, to raise any objections within two weeks (period extendable to two additional weeks if requested by any SA concerned). Silence is deemed as consent. In the event that the entry point is of the view that it should not act as the BCR Lead, it should explain the reasons for its decision as well as its recommendations (if any) as to which other SA would be the appropriate lead authority. The SAs concerned will endeavor to reach a decision within one month from the date that the papers were first circulated.

2.2 Once a decision on the BCR Lead has been made, the latter will start the discussions with the applicant and review the draft BCR documents. In order to foster a more consistent approach, it will send, under Article 57.1.g GDPR, a first revised draft of the BCRs and the related documents to one or two SAs (depending on the number of Member States from whose territories the transfers will take place)[6] which will act as co-reviewers and will help the BCR Lead in the assessment. In case there is no response from a SA acting as co-reviewer within one month from the date the draft and the related documents were sent to it (deadline extendable under justified circumstances), that SA will be deemed to have agreed with them. There may need to be several different drafts or exchanges between the applicant and the relevant SAs before a satisfactory draft is produced.

2.3 The result of these discussions should be a "consolidated draft" sent by the applicant to the BCR Lead which will circulate it among all concerned SAs[7] under Article 57.1.g GDPR for comments. According to this procedure, the period for comments on the consolidated draft will not exceed one month. A concerned SA which has not presented a

[5] See above footnote n. 2.

[6] As a rule, the BCR Lead will consult 2 co-reviewers whenever 14 Member States or more are concerned by transfers. Under this threshold it is possible to have one or two co-reviewers depending on the specific case and the availability of SAs.

[7] See above footnote n. 2.

reasoned objection within this period shall be deemed to be in agreement with the consolidated draft.

2.4 The BCR Lead will send any further comments on the "consolidated draft" to the applicant and may resume discussions, if necessary. If the lead authority is of the view that the applicant is in a position to address satisfactorily all comments received, it will invite the applicant to send a "final draft" to it.

2.5 Pursuant to Article 64.1 and 64.4 GDPR, the BCR Lead will submit the draft decision to the EDPB on the 'final draft' of the BCRs along with all relevant information, documentation and the views of the concerned SAs. The EDPB will adopt an opinion on the matter in accordance with Article 64.3 GDPR and its Rules of Procedure.

2.6 Where the opinion handed down by the EDPB under Article 64.3 endorses the draft decision on the draft BCRs in the form submitted, the BCR Lead will adopt its decision approving the draft BCRs.

2.7 Where the opinion handed down by the EDPB according to Article 64.3 requires any amendment to the draft BCRs, the BCR Lead will communicate to the Chair of the Board within the two-week period set out in Article 64.7 whether it intends to maintain its draft decision (i.e. not to follow the opinion of the EDPB) or whether it intends to amend it in accordance with the EDPB opinion[8]. In the first case, pursuant to Article 64.8 GDPR, Article 65.1 GDPR shall apply[9]. If the BCR Lead communicates to the Chair of the Board that it intends to amend its draft decision in accordance with the EDPB opinion, the BCR Lead will contact the applicant immediately in order to request the amendments to the draft BCRs to be made in accordance with the EDPB opinion so that the draft BCRs can be finalized. When the draft BCRs have been finalized in accordance with the EDPB opinion, the BCR Lead will amend its initial draft decision accordingly, notify the EDPB pursuant Article 64.7 of its amended decision and approve the BCR.

2.8 Once the BCR Lead approves the BCRs, it will inform and send a copy of them to all the concerned SAs. In accordance with Article 46.2.b GDPR, the approved 'binding corporate rules' will provide for the appropriate safeguards referred to in paragraph 46.1 without requiring any specific authorisation from the other concerned supervisory authorities.

2.9 Translations: as a general rule and without prejudice to other translations where necessary or

[8] According to Article 64.5, the Chair of the Board will, without undue delay, inform by electronic means the members of the Board and the Commission of this information.

[9] In particular, in accordance with Article 65.1.c., "in order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases: [...] (c) where a competent supervisory authority [...] does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board".

required by law, all documents including the consolidated draft of the BCRs should be provided by the applicant in the language of the BCR Lead and also in English when possible in accordance with national law. The final draft and the approved BCRs must be translated by the applicant into the languages of those SAs concerned[10].

2.10 Once the BCRs have been approved, the BCR Lead, according to WP 256 and 257, points 5.1, will inform the concerned SAs of any updates to the BCRs or to the list of BCR members as provided by the applicant. In case the group extended the scope of the BCRs to an additional EU member state (because of the establishment of a new BCR member in this EU member state), the SA of this member state will then be deemed to be a new concerned SA as for point 2.8.

[10] See also on this WP 256 and 257, Sections 1.7 according to which "The BCRs must contain the right for every data subject to have an easy access to them".

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP263 rev.01

# Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR

**Adopted on 11 April 2018**

## Introduction

The procedure for approving binding corporate rules (BCRs) for controllers and processors is laid out by provisions contained in Articles 47.1, 63, 64 and (only if necessary) 65 of the Regulation (EU) 2016/679 (GDPR).

As a result, binding corporate rules are to be approved by the competent supervisory authority[1] in the relevant jurisdiction in accordance with the consistency mechanism set out in Article 63, under which the European Data Protection Board (EDPB) will issue a non-binding opinion on the draft decision submitted by the competent Supervisory Authority (Article 64 GDPR).

As the group applying for approval of its BCRs may have entities in more than one Member State, this procedure may involve a number of concerned Supervisory Authorities (SAs)[2], e.g. in those countries from where the transfers are to take place. However, the GDPR does not lay down specific rules for the cooperation phase which should take place among the concerned SAs in advance of referral to the EDPB. It also does not set out specific rules for identifying the competent SA – which will act as Lead Authority for the BCRs ('BCR Lead')[3]. The role of such BCR Lead includes acting as a single point of contact with the applicant organization or group during the approval process and managing the application procedure in its cooperation phase.

The aim of this document is to update the WP 107 and identify smooth and effective cooperation procedures in line with the GDPR whilst taking full advantage of the previous fruitful experience of the Data Protection Authorities in dealing with the approval of BCRs.

This document will be reviewed and if necessary updated, based on the practical experience gained through the application of the GDPR.

---

[1] Article 57.1.s GDPR states that "without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory […] approve binding corporate rules pursuant to Article 47" and Article 58.3.j GDPR according to which each supervisory authority shall have the "authorisation and advisory powers […] to approve binding corporate rules pursuant to Article 47".

[2] Pursuant to Article 4(22) (a) and (b), a 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing". As for the BCRs approval procedure, the concerned SAs are the SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a Member State may provide services to controllers in several – potentially all – Member States).

[3] The "BCR Lead" is generally distinct from the "OSS Lead" considering that BCR transfers will not as a rule meet the definition/criteria of a cross-border processing operation. However, there could be cases in which the same SA could be the BCR Lead and the OSS Lead. This might e.g. be the case if a transfer performed by one establishment substantially affects data subjects in more than one MS (i.e. if personal data are first sent from member states A, B and C to the controller's establishment in member state A, and subsequently transferred by this establishment in A to a third country or, in case of BCR-P, where the processor carries out the same transfers for all their clients in the different member states). In any case, the BCR approval procedure would be the specific one settled by Article 64 GDPR.

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 (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

## 1. Identification of the BCR Lead Supervisory Authority

1.1 A group of undertakings, or group of enterprises engaged in a joint economic activity ('Group'), interested in submitting draft binding corporate rules (BCRs) for the approval of the competent Authority according to Articles 47, 63 and 64 GDPR should propose a SA as the BCR Lead. The decision as to which SA should act as BCR Lead is based upon the criteria contained in this document (see next paragraph). It is for the organisation to justify the reasons why a given SA should be considered as the BCR Lead.

1.2 An applicant Group should justify the proposal of the BCR Lead on the basis of relevant criteria such as:

a. the location(s) of the Group's European headquarters;

b. the location of the company within the Group with delegated data protection responsibilities[4];

c. 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;

d. the place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) are taken; and

e. the member state within the EU from which most or all transfers outside the EEA will take place.

1.3 Particular attention will be given to factor described under 1.2 (a) above.

1.4 These are not formal criteria. The SA to which the application is sent (as prospective BCR Lead SA) will exercise its discretion in deciding whether it is in fact the most appropriate lead SA and, in any event, the SAs among themselves may decide to allocate the application to a SA other than the one to which the Group applied (see next paragraph), in particular if it would be possible and worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

[4] According to Article 47.2.f GDPR, there should always be an EU based member of the group established on the territory of a Member State accepting liability for any breaches of the binding corporate rules by any member concerned not established in the Union. If the headquarters of the group were somewhere else, the headquarters should delegate these responsibilities to a member based in the EU.

1.5 The applicant should also provide the proposed BCR Lead (the entry point) with all appropriate information (both on paper and electronically to facilitate further distribution) which justifies its proposal, *inter alia*, the nature and general structure of the processing activities in the EU with particular attention to the place/s where decisions are made, the location and nature of affiliates in the EU, the number of employees or persons concerned, the means and purposes of the processing, the places from where the transfers to third countries do take place and the third countries to which those data are transferred.

## 2. **Cooperation procedure for the approval of BCRs**

2.1 The proposed BCR Lead will forward the information received as to why that SA has been selected by the company to be the lead authority for the BCRs to all SAs concerned[5] with an indication of whether or not it agrees to be the BCR Lead. If the entry point agrees to be the lead authority, the other concerned SAs will be asked, under Article 57.1.g GDPR, to raise any objections within two weeks (period extendable to two additional weeks if requested by any SA concerned). Silence is deemed as consent. In the event that the entry point is of the view that it should not act as the BCR Lead, it should explain the reasons for its decision as well as its recommendations (if any) as to which other SA would be the appropriate lead authority. The SAs concerned will endeavor to reach a decision within one month from the date that the papers were first circulated.

2.2 Once a decision on the BCR Lead has been made, the latter will start the discussions with the applicant and review the draft BCR documents. In order to foster a more consistent approach, it will send, under Article 57.1.g GDPR, a first revised draft of the BCRs and the related documents to one or two SAs (depending on the number of Member States from whose territories the transfers will take place)[6] which will act as co-reviewers and will help the BCR Lead in the assessment. In case there is no response from a SA acting as co-reviewer within one month from the date the draft and the related documents were sent to it (deadline extendable under justified circumstances), that SA will be deemed to have agreed with them. There may need to be several different drafts or exchanges between the applicant and the relevant SAs before a satisfactory draft is produced.

2.3 The result of these discussions should be a "consolidated draft" sent by the applicant to the BCR Lead which will circulate it among all concerned SAs[7] under Article 57.1.g GDPR for comments. According to this procedure, the period for comments on the consolidated draft will not exceed one month. A concerned SA which has not presented a

[5] See above footnote n. 2.

[6] As a rule, the BCR Lead will consult 2 co-reviewers whenever 14 Member States or more are concerned by transfers. Under this threshold it is possible to have one or two co-reviewers depending on the specific case and the availability of SAs.

[7] See above footnote n. 2.

reasoned objection within this period shall be deemed to be in agreement with the consolidated draft.

2.4 The BCR Lead will send any further comments on the "consolidated draft" to the applicant and may resume discussions, if necessary. If the lead authority is of the view that the applicant is in a position to address satisfactorily all comments received, it will invite the applicant to send a "final draft" to it.

2.5 Pursuant to Article 64.1 and 64.4 GDPR, the BCR Lead will submit the draft decision to the EDPB on the 'final draft' of the BCRs along with all relevant information, documentation and the views of the concerned SAs. The EDPB will adopt an opinion on the matter in accordance with Article 64.3 GDPR and its Rules of Procedure.

2.6 Where the opinion handed down by the EDPB under Article 64.3 endorses the draft decision on the draft BCRs in the form submitted, the BCR Lead will adopt its decision approving the draft BCRs.

2.7 Where the opinion handed down by the EDPB according to Article 64.3 requires any amendment to the draft BCRs, the BCR Lead will communicate to the Chair of the Board within the two-week period set out in Article 64.7 whether it intends to maintain its draft decision (i.e. not to follow the opinion of the EDPB) or whether it intends to amend it in accordance with the EDPB opinion[8]. In the first case, pursuant to Article 64.8 GDPR, Article 65.1 GDPR shall apply[9]. If the BCR Lead communicates to the Chair of the Board that it intends to amend its draft decision in accordance with the EDPB opinion, the BCR Lead will contact the applicant immediately in order to request the amendments to the draft BCRs to be made in accordance with the EDPB opinion so that the draft BCRs can be finalized. When the draft BCRs have been finalized in accordance with the EDPB opinion, the BCR Lead will amend its initial draft decision accordingly, notify the EDPB pursuant Article 64.7 of its amended decision and approve the BCR.

2.8 Once the BCR Lead approves the BCRs, it will inform and send a copy of them to all the concerned SAs. In accordance with Article 46.2.b GDPR, the approved 'binding corporate rules' will provide for the appropriate safeguards referred to in paragraph 46.1 without requiring any specific authorisation from the other concerned supervisory authorities.

2.9 Translations: as a general rule and without prejudice to other translations where necessary or

[8] According to Article 64.5, the Chair of the Board will, without undue delay, inform by electronic means the members of the Board and the Commission of this information.

[9] In particular, in accordance with Article 65.1.c., "in order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases: [...] (c) where a competent supervisory authority [...] does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board".

required by law, all documents including the consolidated draft of the BCRs should be provided by the applicant in the language of the BCR Lead and also in English when possible in accordance with national law. The final draft and the approved BCRs must be translated by the applicant into the languages of those SAs concerned[10].

2.10 Once the BCRs have been approved, the BCR Lead, according to WP 256 and 257, points 5.1, will inform the concerned SAs of any updates to the BCRs or to the list of BCR members as provided by the applicant. In case the group extended the scope of the BCRs to an additional EU member state (because of the establishment of a new BCR member in this EU member state), the SA of this member state will then be deemed to be a new concerned SA as for point 2.8.

[10] See also on this WP 256 and 257, Sections 1.7 according to which "The BCRs must contain the right for every data subject to have an easy access to them".

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP265

# Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data

**Adopted on 11 April 2018**

# Standard Application for Approval of Binding Corporate Rules for Processors

## PART 1: APPLICANT INFORMATION

| 1. STRUCTURE AND CONTACT DETAILS OF THE GROUP OF UNDERTAKINGS OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (THE GROUP) |
|---|

| |
|---|
| Name of the Group and location of its headquarters (ultimate parent company): |
| Does the Group have its headquarters in the EEA?<br>☐ Yes<br>☐ 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:<br>(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 from which BCRs for Processors will be used: |

## 2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS

Please, indicate the following:

- Expected nature of the data covered by BCR, and in particular, if they apply to one category of data or to more than one category, types of data subjects concerned, (for instance human resources, customers,…), anticipated types of processing and its purposes

- Anticipated purposes of data transfers for processing activities

- Do the BCR only apply to transfers from the EEA, or do they apply to all transfers for processing activities between members of the Group?

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

- Extent of the transfers within the Group that are covered by the BCR; including a description and contact details of any Group members in the EEA or outside EEA to which personal data may be transferred for processing activities

## 3. DETERMINATION OF THE LEAD SUPERVISORY AUTHORITY (BCR LEAD)

Please explain which should be the BCR Lead, 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

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

# PART 2: BACKGROUND PAPER[1]

## 4. BINDING NATURE OF THE BINDING CORPORATE RULES (BCR) FOR PROCESSORS

### INTERNAL BINDING NATURE[2]

***Binding within the entities of the Group acting as internal subprocessors[3]***

How are the BCR for processors made binding upon the members of the Group?

- ☐ Measures or rules that are legally binding on all members of the Group
- ☐ Contracts or intra-group agreements between the members of the Group
- ☐ Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group (that is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral declarations or undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs);
- ☐ Other means (only if the Group demonstrates how the binding character of the BCRs is achieved), 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 BCR for Processors extend to the whole Group? (If some Group members should be exempted, specify how and why)

Please confirm that any use of subprocessors (internal) is only done after prior information to data controllers and with their prior written consent

[1] Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP257, adopted on 6 February 2018.

[2] See Section 1.1 and 1.2 WP 257

[3] See Section 1.2 (i) WP 257

| ***Binding upon the employees***[4] |
|---|
| Your Group may take some or all of the following steps to ensure that the BCR for Processors are binding on employees, but there may be other steps. Please, give details below.<br><br>-Individual and separate agreement/undertaking with sanctions<br><br>- Work employment contract with sanctions<br><br>- Collective agreements (approved by workers committee/another body) with sanctions<br><br>- Employees must sign or attest to have read the BCR for Processors or related ethics guidelines in which the BCR for Processors are incorporated<br><br>- BCR for Processors have been incorporated in relevant company policies with sanctions<br><br>- Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation<br><br>- Other means (but the group must properly explain how the BCRs are made binding on employees)<br><br>Please provide a summary supported by extracts from policies and procedures or confidentiality agreements as appropriate to explain how the BCR for Processors are binding upon employees. |

[4] See Section 1.2 (ii) WP257

| *EXTERNALLY BINDING NATURE* |
|---|

| *Binding upon external subprocessors processing the data* |
|---|

| |
|---|
| Please confirm that a written contract or other legal act under Union or Member State law is put in place with external subprocessors which states that adequate protection is provided according to Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the external subprocessors will have to respect the same data protection obligations as are imposed on the Group members according to the Service Agreements concluded with data controllers and Sections 1.3, 1.4, 3 and 6 of WP257[5]. |
| How do such contracts or other legal acts under Union or Member State law address the consequences of non compliance? Please specify the sanctions imposed on subprocessors for failure to comply |
| Please confirm that any use of subprocessors (external) is only done after prior informed specific or general written authorization of the data controller[6] |
| Please confirm that subprocessors accept to submit their data processing facilities for audit, at the request of a data controller, of the processing activities relating to that controller[7]. Please describe the system. |

| |
|---|
| 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[8]. |
| Please provide a summary supported by extracts from the agreement signed with data controllers as appropriate to explain how the BCR for Processors are made binding towards data controllers[9]<br><br>Please confirm that data controllers' rights shall cover the judicial remedies and the right to receive compensation |

[5] See Section 6.1 (vii) WP257

[6] See Section 6.1 (vii) WP257

[7] See Section 2.3 WP 257

[8] 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 absence 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.

[9] See Section 1.4 WP 257

| ***Legal claim or actions*** |
|---|
| Explain how you meet the obligations according to the requirements of Article 47.2.e, 77, 79, 82, as further specified in paragraph 1.3 of WP257[10] |

| |
|---|
| Please confirm that the controller established on the territory of a Member State (e.g. EEA headquarters of the Group, the Group member of the Processor with delegated data protection responsibilities in the EEA or the EEA exporter processor (e.g., the EEA contracting party with the controller), has made appropriate arrangements to enable itself to remedy the acts and to pay compensation, for any damages suffered either by a data subject or a data controller, resulting from the breach, by any member of the Group or by any external subprocessor, of the BCR for Processors and explain how this is ensured. |
| Please confirm that the burden of proof with regard to an alleged breach of the rules caused either by a Group member or by an external subprocessor will rest with the member of the Group in the EU that have accepted to endorse liability for breaches caused by non EEA members of the group or by subprocessors, regardless of where the claim originates. |

| ***Easy access to BCR for Processors[11]*** |
|---|

| |
|---|
| Please confirm that your BCR for Processors are annexed to the Service Agreements signed with data controllers, or that reference to it is made with a possibility of electronic access: |
| Please confirm that your BCR for Processors are published on the website of the Group of processor in a way easily accessible to data subjects, or at least that a document is published and contains all the information as required in Section 1.8 of WP257: |

[10] 1.3 WP 257 provides that the BCRs must grant rights to data subjects to enforce BCRs as third party beneficiaries against the processor either when the requirements at stake are specifically directed to processors in accordance with the GDPR or in case the data subject is not able to bring a claim against the data controller because the data controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

[11] See Section 1.8 WP257

## 5. EFFECTIVENESS[12]

It is important to show how the BCR for Processors in place within your Group are brought to life in practice, in particular in non EEA countries where data will be transferred for processing activities on the basis of the BCR for Processors, as this will be significant in assessing the adequacy of the safeguards.

***Training and awareness raising (employees)[13]***

- Special training programs

- Employees are tested on BCR for Processors and data protection

- BCR for Processors 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[14]***

Do the BCR for Processors contain an internal complaint handling system to (i) communicate claims or requests without delay to data controllers, and to (ii) handle complaints instead of a data controller when the latter has disappeared factually, has ceased to exist in law or became insolvent, or when it has been agreed with a data controller that the Group will handle claims and requests from data subjects?

Please describe the system for handling complaints:

[12] See Section 2 WP257

13 See Section 2.1 WP257

[14] See Section 2.2 WP257

***Verification of compliance***[15]

What verification mechanisms do your Group have in place to audit each Group members' compliance with your BCR for Processors? (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 BCR for Processors 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 BCR for Processors 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

***Network of data protection officers (DPO) or appropriate staff*** [16]

Please confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with top management support to oversee and ensure compliance with the BCR for Processors:

Please explain how your network of DPOs or privacy officers functions:

- Internal structure:

- Role and responsibilities:

[15] See Section 2.3 WP 257
[16] See Section 2.4 WP 257

## 6. COOPERATION WITH SAs[17]

| |
|---|
| Please, specify how your BCR for Processors deal with the issues of cooperation with SAs: |

| |
|---|
| Do you confirm that you will permit the relevant SAs to audit your compliance?<br><br>Do you confirm that the Group as a whole and each members of the Group will abide by the advice of the relevant Supervisory authorities relating to the interpretation and the application of your BCR for Processors? |

## 7. COOPERATION WITH DATA CONTROLLERS[18]

| |
|---|
| Please specify how your BCR for Processors deal with the duty of cooperation with data controllers? |

| |
|---|
| Do you confirm that you will submit your data processing facilities to data controller (or to an inspection body composed of independent members, selected by the data controller) which requested it for audits of the processing activities relating to them? |

[17] See Section 3.1 WP257
[18] See Section 3.2 WP 257

## 8. DESCRIPTION OF PROCESSING AND DATA FLOWS[19]

Please indicate the following:

- Expected nature of the data covered by the BCR for Processors, 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 for processing activities?

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

- Purposes for which the data covered by the BCR for Processors are transferred to third countries and type of processing

- Extent of the transfers within the Group that are covered by the BCR for Processors, including a description and contact details of any Group members in the EEA or outside the EEA to which personal data may be transferred for processing activities

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

## 8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[20]

[19] See Section 4.1 WP257

[20] See Section 5.1 WP257

Please confirm and explain how your BCR for Processors allow for informing other parts of the Group, the concerned Supervisory Authorities via the competent SA under Article 64 (i.e. the BCR Lead) and data controllers of any changes to the BCR for Processors and/or the list of BCR members (summary):

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

Please confirm that where a change affects the processing conditions, data controllers are informed in a timely fashion that data controllers have the possibility to object to the changes or terminate the contract before the modification is made

## 9. DATA PROTECTION SAFEGUARDS[21]

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

- Transparency, fairness and lawfulness (e.g., general duty to help and assist the controller)

- Purpose limitation (e.g., duty to process personal data only on behalf of data controllers and in compliance with their instructions and to return the data to the data controller at the end of the contract)

- Data quality (e.g., general duty to help and assist the controller)

- Security

- Data subjects' rights (e.g., general duty to help and assist the controller)

- Subprocessing within the Group

- Restrictions on onward transfers to external subprocessors

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

[21] See Section 6 of WP257

## 10. ACCOUNTABILITY AND OTHER TOOLS[22]

-Please confirm and specify how BCR members will make available to the controller all information necessary to demonstrate compliance with their obligations as provided by Article 28-3-h (including through audits, and information of the controller if an instruction infringes the GDPR or other Union or Member State data protection provisions)

-Please confirm that the BCR members will maintain a record of all categories of processing activities carried out on behalf of each controller as provided by Article 30-2 GDPR

-Please specify how BCR members will assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with requirements set out by BCRs in practice (e.g. data protection by design, data protection by default)

Please provide supporting documents where appropriate with respect to the information requested above

[22] See Section 6.1.2 WP257

# ANNEX 1:
# COPY OF THE FORMAL BINDING CORPORATE RULES FOR PROCESSORS

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

**11639/02/EN**
**WP 74**

# 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 3 June 2003**

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

**has adopted the present Working Document:**

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

# INDEX

**Working Document on Binding Corporate Rules for International Data Transfers**

## 1. INTRODUCTION

Data Protection Authorities receive requests for authorisations for the transfer of personal data to third countries within the meaning of Article 26 (2) of the Directive[2]. Traditionally most of these requests have required contractual solutions which national authorities have considered in the light of the principles outlined in WP 12[3], other documents issued by this group and particularly the Commission decisions on standard contractual clauses.

Contractual solutions have been already used by multinational companies and the possibility of broadening their use is now under discussion in some Member States. These experiences must be taken into account seriously for evaluating the possible developments of the regulation in these matters.

At the same time, some multinational companies due to their complex architectural structures worldwide would like to benefit from the possibility to adopt "codes of conduct for international transfers"[4] dealing with the international transfer of personal data within the same corporate group at a multinational level subject to the authorisation of the relevant data protection authorities, under Art. 26 (2) of the Directive,. These multinational companies are also of the view that the possibility of unilateral undertakings surrounded by solid guarantees should also be exploited.

In so far as a unilateral undertaking is able to deploy real and ensured legal effects, in particular as regards the effective protection of data subjects after the transfer and as regards the possible intervention of national supervisory authorities or other authorities, as further clarified under chapters 3 and 5 below, there should not be any reason to exclude such a possibility: Article 26 (2) of Directive 95/46/EC offers the Member States a broad margin of manoeuvre in this regard.

---

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

3 Working document: Transfer of personal data to third countries: applying Articles 25 and 26 of the EU Data Protection Directive, approved on 24 July 1998.

4 The adoption of codes of conduct by corporate groups is relatively frequent. Typical subjects of codes of conduct adopted by multinationals would be the following: (a) maintenance and retention of accurate books and records; (b) truthfulness and accuracy in communications with the public and the government; (c) procedures such as Chinese walls to assure that advice to clients and business decisions are not affected by conflicts of interest; (d) protection of confidential information; (e) prohibition of misuse of corporate assets; (f) elimination of improper discrimination and harassment; (g) prohibition of bribery and kickbacks; (h) implementation of ethical business practices and compliance with laws that foster competition in the marketplace; and (i) prohibition of securities trading based on inside information

However, it is important to recognise that under the national law of some Member States, unilateral undertakings do not create obligations and rights with legal effects. In consideration of that, the Working Party intends to stress the general nature of the present document on the subject matter in order to avoid the risk to interfere with the applicable national legislations and reserves the right to provide further solutions that may harmonise further the use of binding corporate rules in all Member States.

Binding corporate rules should not be considered as the only or the best tool but for carrying out international transfers but only as an additional one where the use of existing instruments (i.e. Commission decisions on standard contractual clauses or the Safe Harbor Principles where applicable) seem to be particularly problematic. This working document may not be used as forcing or even simply as inciting the Member States to use a given tool in responding to the requests of multinational companies. National supervisory authorities or any other competent bodies are entirely free to analyse and answer the proposals submitted to them in the way that fits best with their national laws and the given elements of the submission

The Working Party is of the view nevertheless that it is useful to extend these reflections to the Community level and agree on a series of principles and procedures which will both facilitate the work for companies and authorities in the Member States and guarantee consistency within the EU. In any case this working document aims at contributing to a more harmonised application and interpretation of Article 26 (2) of the Directive in the Member States and facilitating data flows in cases where adequate protection is provided. [5]

Finally, the Article 29 Working Party would like to reiterate that adducing sufficient safeguards within the meaning of Article 26 (2) is a broad concept that certainly includes contractual solutions and binding corporate rules but may also cover other situations not dealt with by this paper which data protection authorities can also consider suitable for the granting of authorisations. This working document, nevertheless, has reviewed the application of Article 26 (2) of the Directive in the particular case of the binding corporate rules.

The Article 29 Working Party also shares the concern expressed by some national data protection authorities in the sense that they may lack sufficient resources to deal with numerous requests for authorisations in a lengthy and negotiable manner. It is confident that corporations will bear these limitations in mind and will endeavour to submit applications as close as possible to the recommendations contained in this working document.

## 2. THE POTENTIALITIES OF CONTRACTUAL SOLUTIONS

The Article 29 Working Party would like to stress that the fact that this working document focus on binding corporate rules (or codes of conduct in more traditional terminology) should not be interpreted as indicating that contractual solutions have been superseded. On the contrary, after the Commission decisions on standard contractual

clauses and the considerable guidance provided by this Working Party and national data protection authorities, companies are making broad use of these instruments in a very positive and encouraging way (e.g. the standard contractual clauses with many parties to the contract).

The Article 29 Working Party believes that the potential of standard contractual clauses has only begun being exploited by operators. Two issues must be pointed out in this regard.

First, the Commission decisions on standard contractual clauses prevent a Member State from determining that a data exporter ready to enter into a contract in line with the standard contractual clauses does not offer sufficient safeguards for the transfer to take place, except in the particular circumstances specified by the Commission decisions. In other words, the standard contractual clauses are a useful, practical tool – at the moment already available for operators – legally recognised and adopted at both EU and national level, which provides an equal, sufficient level of harmonised guarantees for operators and data subjects. At the same time, Member States are entitled to consider other contractual arrangements as long as they undoubtedly assure a sufficient level of protection for the personal data concerned.

Secondly, it seems also possible, on the basis of the use of standard contractual clauses, to envisage the use of the binding corporate rules to allow, under certain conditions[6], onward transfers to other recipients different from the data importer without other contracts being necessary with these further recipients. There appears to be an interesting combination to consider between the contractual solutions and the use of the binding corporate rules that may overcome the obstacles posed by the lack of legal effects of unilateral undertakings in some Member States. Thus, the circulation of personal data within the members of the corporate group might be allowed under this solution, provided the necessary guarantees are put into place.

## 3. DEFINITION AND LEGAL ISSUES AT STAKE

### 3.1. Scope of this instrument and definitions

When dealing with requests under Article 26 (2) of the Directive, the assessment for granting an authorisation consists of an analysis of the safeguards put in place by the controller in order to guarantee an adequate protection of the personal data with regard to its transfer to a third country.

This exercise is therefore different from the approval of codes of conduct provided for in Article 27 of the Directive, that is, professional rules aimed at the practical application of national data protection legislation in a specific sector. In either case, the internal rules of a corporate group cannot replace the data protection obligations by which the members of the corporate group are bound by law. Compliance with national law is of course a condition *sine qua non* for any authorisation to be granted.

[6] For example by identifying in the contract the further recipients and attaching the binding corporate rules as an annex to the contract, but at the same time as an integral part of it, with all legal consequences.

A transfer to a third country consists of the communication of data to another data controller or data processor in a third country, the legitimacy of which should be assessed by reference to the general circumstances of the case with regards to the principles set up by the Directive (Articles 6, 7, 8, 17, etc.). Where the processing is carried out in the context of the activities of an establishment of a member of a corporate group on Community territory or the processing is carried out by a member of the corporate group who is not established on Community territory but makes use of equipment situated on Community territory, the Directive and national laws of implementation apply.

The principles of protection contained in the binding corporate rules must comply to a large extent with the principles of protection of Directive 95/46/EC. From this perspective, as a general principle, the implementation of binding corporate rules within the Community does not pose any problem provided that the rules comply with the national data protection legislation. If these conditions were met, this would allow corporate groups to have a truly global privacy policy.

In the same line of thought and by definition, binding corporate rules are global and therefore no distinction should be made in their application. The rules must apply generally throughout the corporate group irrespective of the place of establishment of the members or the nationality of the data subjects whose personal data is being processed or any other criteria or consideration. However, whilst the rules would always remain the same and the corporate group would endeavour to respect them accordingly, their enforceability vis-à-vis the corporate group may legitimately differentiate between data originating in the EU, in other words, personal data that were once subject to EU law and subsequently transferred abroad, and other categories of data.

For this latter category of data, the corporate group is not obliged to entitle data subjects to claim or enforce any rights on Community territory. Although such an inclusion cannot be regarded as a *condition sine qua non* for the granting of an authorisation, it would always be very welcomed and regarded as a serious commitment of the corporate group to data protection requirements.

Consequently, as the purpose of these instruments is different from the codes of conduct foreseen in Article 27 of the Directive, rather than referring to them as "codes of conduct" (which could be misunderstood) it seems more appropriate to find a terminology which fits with the real nature of these instruments, that is, the provision of sufficient safeguards for the protection of personal data transferred outside the Community.

A possible terminology for these instruments could be **"binding corporate rules for international data transfers" or "legally enforceable corporate rules for international data transfers"**

a) **binding or legally enforceable** because only with such a character may any clauses be regarded as "sufficient safeguards" within the meaning of Article 26 (2)

b) **corporate** in the sense that they consist of the rules in place in multinational companies, usually set up under the responsibility of the headquarters. For the purposes of this document, a corporate group is any group of companies which are effectively bound by the rules as provided for in chapter 3.3.

c) **for international data transfers** as the main reason for their existence.

The notion of "corporate group" may vary from one country to another and may correspond to very different business realities: from closely-knit, highly hierarchically structured multinational companies to groups of loose conglomerates; from groups of companies sharing very similar economical activities and therefore processing operations to broad partnerships of companies with very different economical activities and different processing operations. Obviously, these differences in structure and activity impacts upon the applicability, design and scope of the binding corporate rules and corporate groups must bear this in mind when submitting their proposals.

For loose conglomerates, binding corporate rules are very unlikely to be a suitable tool. The diversity between their members and the broad scope of the processing activities involved would make it very difficult (if not impossible) to meet the requirements outlined in this working document. For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules. In other words, should a final product end up being acceptable under Article 26 (2) of the Directive, it would certainly look like very different from the binding corporate rules discussed in this working document.

In practice, it is expected that multinational companies will be the most frequent users of these mechanisms, as they will want to regulate intra-group transfers world-wide in this way. The Article 29 Working Party would like to stress again the fact that the scope of any authorisation granted on the basis of this instrument would only concern transfers or categories of transfers within the corporate group, in other words, exchanges of personal data between companies bound by these corporate rules. Transfers of personal data to companies outside the corporate group would remain possible but not on the basis of the arrangements put in place by legally enforceable corporate rules but on the basis of any other legitimate grounds under Article 26 of the Directive (e.g. under standard contractual clauses- model contracts or ad hoc ones- concluded with the recipients of the information).

### 3.2. Onward transfers

Onward transfers, that is, transfers from members of the corporate group outside of the Community to companies outside the corporate group would be possible by subscribing the standard contractual clauses adopted by the European Commission in its decision 2001/497/EC (transfers to data controllers) and 2002/16/EC (transfers to data processors) or on the conditions set up therein.

In accordance with this decision, further transfers of personal data to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25 (6) of the Directive may take place if the data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer, or, in other cases, have been given the opportunity to object.

The minimum information to be provided to data subjects should contain, in a language understandable to them:

- the purposes of the onward transfer
- the identification of the data exporter established in the Community from where the personal data originates

- the categories of the further recipients of the personal data and the countries of destination

- an explanation that, after the onward transfer, data may be processed by a controller who is not bound by the binding corporate rules and is established in a country where there is not an adequate level of protection of the privacy of individuals.

The regular audits foreseen in Chapter 4.4. of the binding corporate rules should contain a specific chapter on onward transfers which will review the use of the model contracts by the corporate group. The corporate group should make these contracts available to the data protection authorities upon request and to the data subjects on the conditions contained in the Commission decisions mentioned above.

### 3.3. Considerations about the binding nature of the corporate rules

Organisations respond to their data processing needs on the basis of different legal and cultural backgrounds and different business philosophies and practices. From the limited experience with these instruments, it is clear that nearly every multinational company approaches this matter in a different way. There is, however, an element that must be present in all systems if they are to be used to adduce safeguards for the data transfers to third countries: the binding nature of the corporate rules both internally and towards the outside world (legal enforceability of the rules).

#### 3.3.1. Binding nature of the corporate rules within the corporate group[7]

A distinction can be made between the problem of compliance with the rules and the problem of their legal enforceability.

Indeed, the assessment of the "binding nature" of such corporate rules implies a common assessment of their binding nature *in law (legal enforceability)*, and of their binding nature *in practice (compliance)*. Even if the legal enforceability of unilateral commitments or contracts creating the same effects can be demonstrated from the conceptual perspective, the reality is that the enforcement of rights in transfrontier scenarios is always very complex and may involve disproportionate effort for the data subjects. Therefore, it is worth seeking not only that the internal rules are legally enforceable but also binding in practice[8].

The binding nature of the rules *in practice*, in this respect, would imply that the members of the corporate group, as well as each employee within it, will feel compelled to comply with the internal rules. In that respect, relevant elements could include the existence of disciplinary sanctions in case of contravention of the rules, individual and effective information of employees, setting up special education programmes for employees and subcontractors, etc. All these elements, which are also considered at section 5, could establish why individuals within the corporate group will feel obliged to comply with these rules.

---

[7] The adoption of a conduct is a step that corporations do not take lightly because its adoption poses significant risks and even legal consequences for those companies that breach their own code.

[8] WP 12 emphasises a functional approach and argues that the determining factor in relation to the adequacy is that the protection afforded is delivered in practice.

From the internal perspective, it is not for the Working Party to stipulate the way in which corporate groups should guarantee that all the members are effectively bound or feel compelled by the rules although some examples are well known such as internal policies whose application is of the responsibility of the headquarters or internal codes of conduct backed by intra company agreements[9]. But corporate groups must bear in mind that those applying for an authorisation will have to demonstrate to the grantor of the authorisation that this is effectively the case throughout the group.

The internal binding nature of the rules must be clear and good enough to be able to guarantee compliance with the rules outside the Community, normally under the responsibility of the European headquarters or the European member with delegated data protection responsibilities which must take any necessary measures to guarantee that any foreign member adjust their processing activities to the undertakings contained in the binding corporate rules.[10]

As a matter of fact, there is always an EU based member of the corporate group adducing sufficient safeguards and dealing with the application before the data protection authority. If the headquarters of the corporate group were somewhere else, the headquarters should delegate these responsibilities to a member based in the EU. It makes sense that the effective adducer of the safeguards remains responsible for the effective compliance with the rules and guarantees enforcement. See in this regard sections 5.5. and 5.6. on liability and jurisdiction.

3.3.2. Legal enforceability of the corporate rules by the data subjects (third party beneficiary rights) and by the data protection authorities

Data subjects covered by the scope of the binding corporate rules must become third party beneficiaries either by the legal effects of unilateral undertakings (where possible under national law) or by contractual arrangements between the members of the corporate group making this possible. As third party beneficiaries, data subjects should be entitled to enforce compliance with the rules both by lodging a complaint before the competent data protection authority and before the competent court on Community territory as explained later in section5.6.

The Article 29 Working Party attaches great importance to the existence of both possibilities. Although it seems much easier in principle for the data subject to lodge a complaint before the competent data protection authority and indeed the duty of co-operation of the corporate group with the authority is likely to solve most of the problems, there are two reasons that justify that, even in the assumption of a well-functioning system, the right to seek a judicial remedy is still necessary (see section 5.6):

a) because the duty of co-operation could never guarantee 100% compliance with the rules and data subjects may not necessarily always agree with the views of the data protection authority, and

---

[9] Ideally, the binding corporate rules should be adopted by the board of directors of the ultimate parent of the group.

[10] Under international corporate law affiliates may be able to enforce codes of conduct against each other based on claims of quasi-contractual breach, misrepresentation and negligence.

b) because the competence of data protection authorities in the Community can slightly vary from one country to the other (e.g. some authorities may not impose sanctions or block transfers directly) and none of them can award compensation for damages; only courts could do that.

Although the possibility for data subjects to enforce the rules before the courts is a necessary element for the reasons just mentioned, the Article 29 Working Party attaches more importance to the fact that the rules are complied with in practice by the corporate group as is the aim of any self-regulatory approach.

Regarding another aspect, differences in civil and administrative law raise the question of whether or not unilateral declarations can be regarded as the origin of third party beneficiary rights for individuals.

Where in some cases the legal enforceability of such unilateral declarations do not raise any doubts, in other Member States the situation is not that clear and unilateral declarations might not be sufficient as such. Where unilateral declarations cannot be considered as granting legally enforceable third party beneficiary rights, the corporate groups would have to put in place the necessary contractual arrangements allowing for that. These undertakings can be legally enforced under private law in all Member States. [11]

The scope of the third party beneficiary rights should match at least the one granted by the Commission Decision 2001/947/EC on standard contractual clauses in respect of both the Data Exporter and the Data Importer (see clause 3 "third-party beneficiary"[12]): this

---

[11] Nowadays it is possible to grant third party beneficiary rights in a contract in all Member States. See at this point previous experiences with standard contractual clauses and third party beneficiaries.

[12] Data subjects should be entitled to enforce the following rights (for ease of reference, corresponding clauses of the Commission Decision on Standard Contractual Clauses are indicated between brackets):

- that if the transfer involves special categories of data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a third country not providing adequate protection (clause 4b)
- to obtain a copy of the binding corporate rules upon request (clauses 4c and 5e)
- to be replied to in a reasonable time and to the extent reasonably possible about queries concerning the processing of this personal data outside the Community (clauses 4d and 5c),
- to declare that a member of the corporation bound by the rules is not co-operating with the competent data protection authorities and/or is not abiding by the advice given by the data protection authority with regard to the processing of the data transferred (clause 5c),
- to declare that the legislation applicable to any of the members of the corporations outside the Community prevents him from fulfilling his obligations under the binding corporate rules (clause 5a)
- to declare that the processing of personal data of any member of the corporation bound by the rules is not in accordance with the binding corporate rules (clause 5b)
- to claim liability and, where appropriate, compensation in accordance with the terms set up in the binding corporate rules (clause 6),

clearly confirms the value and the importance of the existing standard contractual clauses.

Such contractual arrangements do not need to be complex or long. They are only instruments to trigger third party beneficiary rights for the individuals in those countries where there are doubts that unilateral declarations may achieve a similar result. In some cases, this could be achieved with the addition of a simple clause to other contracts in place between the members of the corporate group. For example, in those cases where there are contracts between the headquarters and the affiliates to guarantee internal compliance with the binding corporate rules -see previous section-, the addition of a "third party beneficiary clause" to them would be enough to meet this requirement.

As regards the legal enforceability of the binding corporate rules by the competent data protection authority, it is clear that by submitting an application for an authorisation for an international data transfer, the corporate group binds itself vis-à-vis the data protection authority to respect the safeguards adduced (in this case the binding corporate rules). This does not prejudice the question whether the responsibility to enforce these undertaking lies with the data protection authority herself or another authority (e.g. a court after the advice of the data protection authority).

On the top of that, data subjects would always be entitled to lodge a complaint before the national data protection authority or before judicial courts, as indicated under section 5.6 below. This might provide a more satisfactory course of action for data subjects and in any case a sort of "indirect" third party beneficiary rights for the data subjects.

3.3.3. Mandatory requirements of national legislation applicable to the members of the corporate group

The binding corporate rules should contain a clear provision indicating that where a member of the corporate group has reasons to believe that the legislation applicable to him may prevent him from fulfilling his obligations under the binding corporate rules and have a substantial adverse effect on the guarantees provided by them, he will promptly inform the headquarters in the EU or the EU member with delegated data protection responsibilities, unless otherwise prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

The headquarters in the EU or the EU member with delegated data protection responsibilities should take a responsible decision and have to consult the competent data protection authorities. Any incidences under this chapter of the rules will be detailed and reviewed by the regular audits foreseen under Chapter 5.2.

---

- to be able to use European jurisdiction in accordance with the terms set up in the binding corporate rules (clause 7),

- to declare that the rules have been varied contrary to the binding corporate rules or without respecting the procedural obligations set up thereof, or that any member of the corporation does not honour its obligations once he is no longer bound by the rules (clauses 9 and 11)

The scope of third party beneficiary rights must be clear in the contractual arrangements allowing for them.

Mandatory requirements of national legislation applicable to the members of the corporate group which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13 (1) of Directive 95/46/EC[13], are in principle not in contradiction with the binding corporate rules. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax reporting requirements or anti money-laundering reporting requirements. In case of doubt, corporate groups should promptly consult the competent data protection authority.

## 4. SUBSTANTIAL CONTENT OF THE BINDING CORPORATE RULES

### 4.1. Substantial content and level of detail

The Working Party reaffirms the principles contained in working document number 12[14], with special reference to chapters 3 (*applying the approach to Industry self-regulation*) and to a lesser extent chapter 6 (*procedural issues*). Having said that, it must be clear that these principles *per se* might mean very little for companies and employees processing personal data outside the Community, in particular in those countries where there is no data protection legislation in place and most probably no data protection culture whatsoever.

These principles need to be developed and detailed in the binding corporate rules so that they practically and realistically fit with the processing activities carried out by the organisation in the third countries and can be understood and effectively applied by those having data protection responsibilities within the organisation.

From this perspective, the binding corporate rules may have something in common with the codes of conducts foreseen in Article 27 of the Directive in the sense that they are supposed to overcome the level of abstraction of the legislation (in this case the principles of Working Document number12). The corporate rules should contain tailor-made provisions as well as a reasonable level of detail in the description of the data flows, purposes of the processing, etc.

As indicated in Article 26 (2) of the Directive, the authorisation may concern a transfer or a set of transfers but in any case there must be an explanation of the transfers being authorised. The level of detail must be sufficient so as to allow the data protection authorities to assess that the processing carried out in third countries is adequate (e.g. a detailed description of the economical activities pursued by the different entities of the corporate group).

---

[13] that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others

[14] Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf

By way of example and in so far as the national applicable legislation provides for a notification regime, a practical suggestion could be that in those countries where the notification system contains a high level of detail, this section of the binding corporate rules should mirror the rules on the way that data controllers must notify to data protection authorities: in the same way that the notification allows the data protection authority to understand the processing operations carried out by the controller[15] the same level of information should in principle suffice for the data protection authority to understand the processing operations covered by the binding corporate rules within the corporate group. Where the level of detail in the notification system is not sufficiently detailed (Article 18.2 of the Directive gives Member States a great margin of manoeuvre in this regard), it would be necessary to add further information in order to provide an adequate description of the personal data being transferred to third countries. Binding corporate rules do not replace in any way notification requirements under EU law.

### 4.2. Particularisation and updates to the rules

Binding corporate rules may particularise further the relevant rules for different countries or regions outside the Community if this is the wish of the corporate group putting them in place. However, this particularisation would obviously add complexity to the system that is in principle meant to develop global policies.

As regards updates of the transfers taking place and, as matter of course, update of the rules, the Article 29 Working Party acknowledges that corporate groups are mutating entities whose members and practices may change from time to time and therefore they could not 100% correspond to the reality at the time the authorisation was granted. Updates are possible (without having to re-apply for an authorisation) providing that the following conditions are met:

a) no transfer of personal data is made to a new member until the exporter of the data has made sure that the new member is effectively bound by the rules and can deliver compliance,

b) an identified person or department of the corporate group should keep a fully updated list of the members and keep track of and record of any updates to the rules and provide the necessary information to the data subjects or data protection authorities upon request,

c) any updates to the rules or changes to the list of members should be reported once a year to the data protection authorities granting the authorisations with a brief explanation of the reasons justifying the update.

Updating the rules should be understood in the sense that working procedures may change and the rules would need to be adapted to such changing environments. Significant changes not only related to the principles of protection but also to the purposes of the processing, the categories of data processed or the categories of data subjects, would in principle have an effect on the authorisation.

[15] See Article 19 of the Directive

## 5. DELIVERING COMPLIANCE AND GUARANTEEING ENFORCEMENT

In addition to those rules dealing with substantial data protection principles, any binding corporate rules for international data transfers must also contain:

### 5.1. Provisions guaranteeing a good level of compliance

The rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The issuing by the headquarters of internal privacy policies must be regarded only as a first step in the process of adducing sufficient safeguards within the meaning of Article 26 (2) of the Directive. The applicant corporate group must also be able to demonstrate that such a policy is known, understood and effectively applied throughout the group by the employees which received the appropriate training and have the relevant information available at any moment, for example via the intranet. The corporate group should appoint the appropriate staff, with top-management support, to oversee and ensure compliance.

### 5.2. Audits

The rules must provide for self-audits and/or external supervision by accredited auditors on a regular basis with direct reporting to the ultimate parent's board[16]. Data Protection Authorities will receive a copy of these audits where updates to the rules are notified and upon request where necessary in the framework of the co-operation with the data protection authority.

The rules must also indicate that the duty of co-operation with the data protection authorities (see chapter 5.4.) may also require the acceptance of audits to be carried out by inspectors of the supervisory authority themselves or independent auditors on behalf of the supervisory authority. This is most likely to be the case where the audits foreseen in the previous paragraph were not available for whatever reasons, they failed to contain relevant information necessary for a normal follow-up of the authorisation granted or the urgency of the situation would advocate in favour of a direct participation of the competent data protection authority or independent auditors on his behalf.

Such audits would take place in accordance with the relevant laws and regulations governing the data protection authorities' investigatory powers, without any prejudice to the inspection powers of each data protection authority, of which the corporate group will be duly informed by the competent data protection authority. In any case, they will take place with full respect to confidentiality and trade secrets and would be narrowly limited to ascertaining compliance with the binding corporate rules.

---

[16] The content of these audits must be comprehensive and elaborate in any case about some particulars already identified in this working document, such as the existence of onward transfers on the basis of standard contractual clauses (see section 3.2.) or the decisions taken as regards mandatory requirements under national law which may create conflicts with the binding corporate rules (see section 3.3.3.).

### 5.3. Complaint handling

The rules must set up a system by which individuals' complaints are dealt with by a clearly identified complaint handling department. Data protection officers or any person handling these complaints must benefit from an appropriate level of independence in the exercise of their functions. The use of alternative dispute resolution mechanisms, with the possible involvement of data protection authorities where appropriate, should also be promoted, in compliance with the applicable national laws and regulations.

### 5.4. The duty of co-operation with data protection authorities

As outlined in WP 12, one of the most important elements for assessing the adequacy of a self-regulatory system is the level of support and help available to individual data subjects:

*"A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed"*

This is indeed one of the most important elements of the binding corporate rules for international data transfers: the rules must contain clear duties of co-operation with data protection authorities so individuals can benefit from the institutional support mentioned in WP 12.

There must be an unambiguous undertaking that the corporate group as a whole and any of its members separately will accept the audit requirements indicated in chapter 5.2. There must also be an unambiguous undertaking that the corporate group as a whole and any of its members separately will abide by the advice of the competent data protection authority on any issues related to the interpretation and application of these binding corporate rules. The advice of the competent data protection authority will consist of recommendations addressed to the corporate group either in response to a questionnaire, as a result of a complaint lodged by a data subject or at the own initiative of the data protection authority.

Before issuing any advice the competent data protection authority may seek the views of the corporate group, the data subjects concerned and those data protection authorities which may be associated as a result of the co-ordinated procedure foreseen in this working document[17]. The advice of the authority may be made public.

In addition to any relevant provision at national level, a serious and/or persistent refusal by the corporate group to co-operate or to comply with the advice of the competent data protection authority may entail the suspension or the withdrawal of the authorisation granted either by the data protection authority itself or the competent authority under national law empowered to do so. This decision will have the form of an administrative act which the addressee may challenge before the competent court as provided for by national law. It will be notified to the European Commission and the other data protection authorities involved and it could also be made public.

---

[17] See chapter 6.

## 5.5. Liability

5.5.1. General right to obtain redress and where appropriate compensation

The rules should indicate that the data subjects would benefit from the remedies and liability provided for in Articles 22 and 23 of the Directive (or similar provisions transposing these articles of the Directive in the Member States legislations) in the same way and with the same scope from which they would benefit if the processing operation carried out by the corporate group would fall under the scope of the Data Protection Directive or any national laws transposing it.

The purpose of these rules therefore is limited to guaranteeing that authorisations granted by data protection authorities (which will make possible or lawful a transfer of personal data abroad which would otherwise be unlawful) would not end up depriving data subjects of their right to remedies or compensations from which they would have benefited had the data never left EU territory.[18]

As a complement to this general right, the rules must also contain provisions on liability and jurisdiction aimed at facilitating its practical exercise.

5.5.2. Rules on liability

First of all, the headquarters (if EU based) or the European member with delegated data protection responsibilities should accept responsibility for, and agree to take the necessary action to remedy the acts of other members of the corporate group outside the Community and, where appropriate, to pay compensation (within the scope indicated in the previous chapter) for any damages resulting from the violation of the binding corporate rules by any member bound by the rules.

The corporate group will attach to his request for an authorisation evidence that the EU headquarters or the European member with delegated data protection responsibilities has sufficient assets in the Community to cover the payment of compensation for breaches of the binding corporate rules in normal circumstances or that it has taken measures to ensure that it would be able to meet such claims to that extent (for example: insurance coverage for liability).

The headquarters (if EU based) or the European member with delegated data protection responsibilities must also accept that it will be sued in the EU and, where appropriate pay compensation:

a) in those cases where damages resulting from the breach of the binding corporate rules were claimed, or

---

[18] Some multinationals have been reluctant in the past to adopt global privacy policies on the argument that although they could agree to provide adequate protection to those covered by European legislation, they did not want to extend the same level of protection to other countries or regions where the level was not so high or there was no data protection at all. They have traditionally shown concern about the inclusion of any provisions on redress or compensation for data subjects. This formulation addresses these concerns, because as explained in Chapter 3.1.. the enforceability of the binding corporate rules (therefore including compensation for damages) may be limited to data originating from the EU.

b) damages were not claimed but the data subject was not satisfied with the remedies resulting from the recourse to the internal complaint handling procedures (see section 5.3.) or the lodging of a complaint before the competent data protection authority

Where the European headquarters or the European member with delegated data protection responsibilities can prove that the member of the corporate group in the third country is not responsible for the act resulting in the damage claimed by the data subject, it may discharge itself from any responsibility.

The rules should say that it would always be for the European headquarters or the European member with delegated data protection responsibilities to demonstrate that the member of the corporate group outside the Community is not liable for the violation resulting in the damage claimed by the data subject, rather than for the data subject to demonstrate that a company in a third country is engaged in processing contrary to the corporate rules (an evidence which most of the time would be impossible to get and in any case it would involve disproportionate effort, time and money for the data subject).

### 5.6. Rule on jurisdiction

As explained above in chapter 5.5.2., the corporate group must also accept that data subjects would be entitled to take action against the corporate group, as well as to choose the jurisdiction :

a) either in the jurisdiction of the member that is at the origin of the transfer, or

b) in the jurisdiction of the European headquarters or the jurisdiction of the European member with delegated data protection responsibilities.

Assuming the proper functioning of the system which implies a good level of compliance throughout the group, regular audits, efficient complaint handling, co-operation with data protection authorities, etc. the involvement of the courts seems unlikely, but in any case cannot be excluded. Having said that, only experience with these instruments will tell us if such forecast is right.

The relevant principles and rules on jurisdiction contained both in the Directive and in national laws will duly apply.

### 5.7. Transparency

In addition to the provision of information contained in Articles 10 and 11 of the Directive and national laws transposing them, corporate groups adducing sufficient safeguards must be in a position to demonstrate that data subjects are made aware that personal data are being communicated to other members of the corporate group outside the Community on the basis of authorisations by data protection authorities based on legally enforceable corporate rules, the existence and the content of which must be readily accessible for individuals.

This particularised duty to provide information means that without prejudice to the access to the corporate rules as a whole, corporate groups must be in a position to demonstrate that individuals have readily accessible information on the main data protection obligations undertaken by the corporate group, updated information as regards the members bound by the rules and the means available to data subjects in order to ascertain compliance with the rules.

## 6. PROCEDURE FOR CO-OPERATION BETWEEN NATIONAL AUTHORITIES WHEN DEALING WITH NATIONAL REQUESTS UNDER ARTICLE 26 (2) OF THE DIRECTIVE

The Working Party is aware of the importance of the notification of any authorisations granted to other Member States and to the European Commission as provided for in Article 26 (3) of the Directive. These notifications, nevertheless, may be complemented with additional co-operation activities between national data protection authorities before granting the relevant authorisations. Such a co-operation is indeed foreseen under Article 28 of the Directive in those cases where a national decision may have effects on the processing activities of the same corporate group in another Member State.

Corporate groups interested in a license for similar types of data export from several Member States may make use of a co-ordinated procedure[19]. Any coordinated activity applies only to those data protection authorities with powers under national law to authorise international data transfers and that are legally in the position to accept to be involved from time-by-time and on a case-by-case basis. .

The main idea behind this procedural arrangements is to allow companies to go through one process of application for a permit via a data protection authority of one Member State that will, through the co-ordination process between the involved data protection authorities, lead to the granting of permits by all the different DPAs of the Member States where this company operates. The details of the procedure will be promptly determined case-by-case by the data protection authorities involved.

This working document does not prejudice the rights and obligations that national supervisory authorities may have under national law to deal with complaints from individuals and, in general, to monitor the application of the Directive in those cases where they are competent. These arrangements, nevertheless, address the duty of co-operation provided for in Article 28 (6) of the Directive in those cases where they consider the legal pre-requisites at national level to co-operate with one another.

[19] The Article 29 Working Party may give further guidance on this issue as soon as possible and on the basis of the experience with this procedure. There is a co-operative working relationship between supervisory authorities in the Community therefore it is not necessary to provide for every eventuality. The applicant should indicate the entry point with an explanation of the grounds for its designation as well as the indication of other national supervisory authorities that should be involved in the procedure. The granting of the necessary authorisations under Article 26 (2) of the Directive and national laws pursuant to it and the notification to the European Commission would be the final steps of the co-ordinated procedure.

## 7. CONCLUSION

The Working Party believes that the guidance provided in this document may facilitate the application of Article 26 (2) of the Directive. It should also lead to a certain degree of simplification for multinational corporate groups routinely exchanging personal data on a world-wide basis.

The content of this working document should not be regarded as the final word of the Article 29 Working Party on this issue but as a solid first step to highlight the possibility to use national authorisations under Article 26 (2) on the basis of a self-regulatory approach and co-operation among the authorities, without prejudice to the possibility to use other tools for the transfer of personal data abroad such as the standard contractual clauses or the Safe Harbor principles where applicable.

Further input from interested circles and experts on the basis of the experience obtained with the use of this working document is welcomed. The Working Party might decide to revisit this issue in the light of experience.

Done at Brussels, 3 June 2003
For the Working Party
*The Chairman*
Stefano RODOTA