FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES

March 2009

Disclaimer: Answers to these FAQs may help to clarify understanding of the legal framework in force in the EU with regard to transfers to third countries of personal data processed in the EU/EEA.

They do not have any legal value and do not necessarily represent the position that the Commission may adopt in a particular case.

[NOTE FOR THE READER: The electronic form of these FAQs will contain hyperlinks enabling the reader to have direct access to the specific question of interest to him. This practice is also followed by similar documents published by some national data protection authorities in their websites]

Contents

I. Introduction

Answers to these FAQs have been prepared by the Data Protection Unit of the Directorate-General for Justice, Freedom and Security with a view to assisting EU/EEA entities, and more particularly SMEs, in understanding the EU legal framework applicable to transfers of personal data processed in the EU (and the EEA) to "third countries" (i.e. countries that are not members of the EU or the EEA).

Such transfers are regulated by Articles 25 and 26 of Directive 95/46/EC (hereinafter the "Data Protection Directive")[1].

According to Article 25(1), transfer of personal data "*may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection*". The essential concern of the Data Protection Directive on this point is to ensure that personal data lawfully processed in the EU (and the EEA) remain subject to safeguards when transferred to third countries.

The Data Protection Directive thus determines the situations where personal data may be transferred to third countries. The preferred solution under Article 25 of the Data Protection Directive is one where there is an adequate level of protection; this can be assessed by the Member States or by the European Commission (the Commission has the power to make determinations of adequacy that are binding on EU (and EEA) Member States (Article 25(6)[2]). But there also exist situations where the level of protection has not been assessed and determined but where personal data may nevertheless be transferred to the third country:

- the controller adduces additional safeguards with respect to the protection of privacy and fundamental rights (e.g. by using appropriate contractual clauses or binding corporate rules) (Article 26(2));
- the controller adopts the Commission's standard contractual clauses (Article 26(4));
- the controller can refer to one of the six derogations listed in Article 26(1).

The Data Protection Directive does not cover transfers of personal data in the course of judicial and police cooperation activities falling within Titles V and VI of the Treaty on European Union.

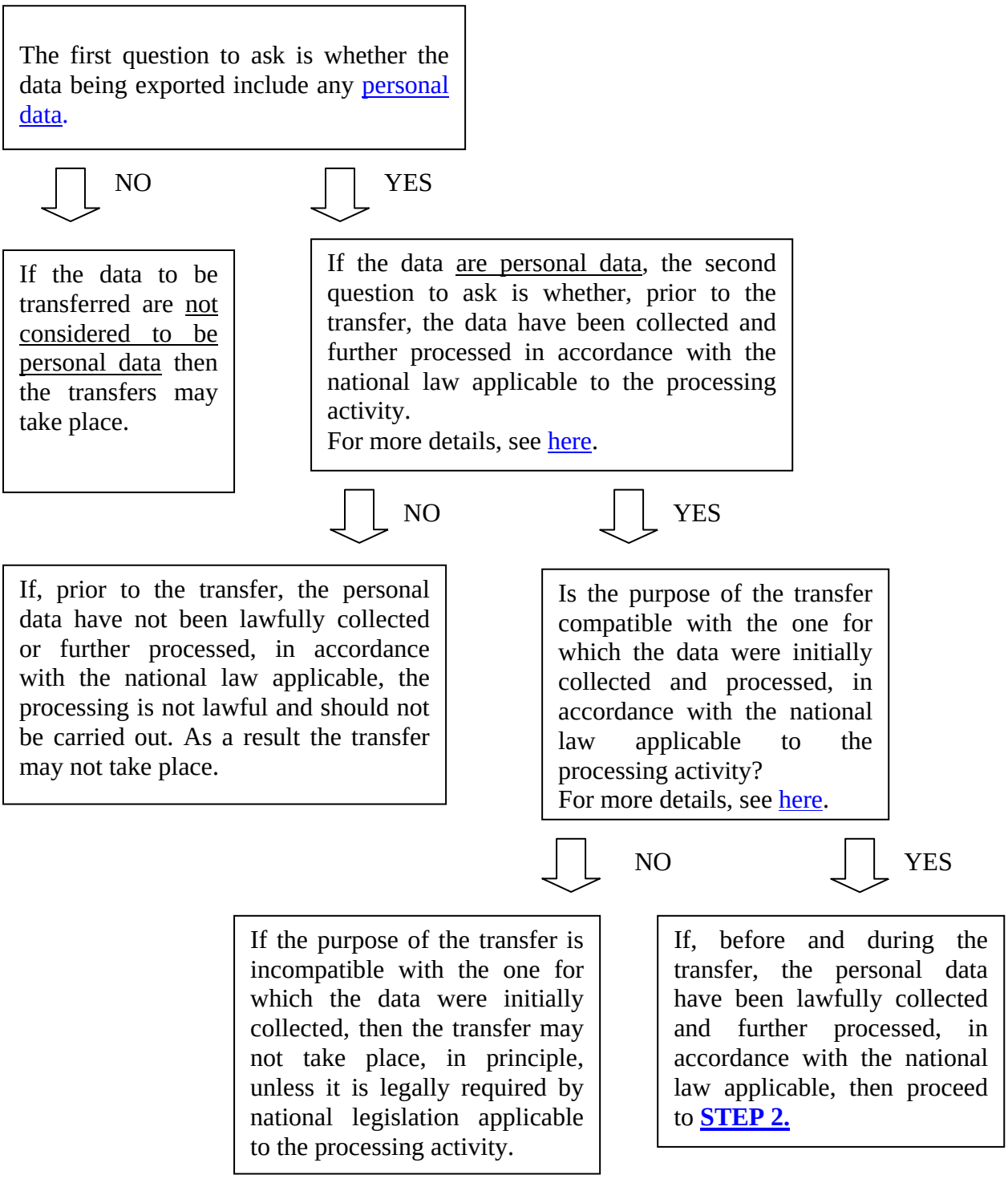
1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31 *et seq.*).

2 The Commission does not make such decisions on its own but with input from: (i) the Data Protection Working Party established pursuant to Article 29 of the Directive, which may deliver a non-binding opinion on the proposed decision (Article 30(1)(a) and (b)); (ii) the Committee of Member State representatives set up under Article 31 of the Directive, which must approve the proposed decision and may refer the matter to the Council for final determination (Article 31(2)); and (iii) the European Parliament, which is able to check whether the Commission has properly used its powers. The procedure follows the ground rules set out in Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ L 184, 17.7.1999, p. 23 *et seq.*).

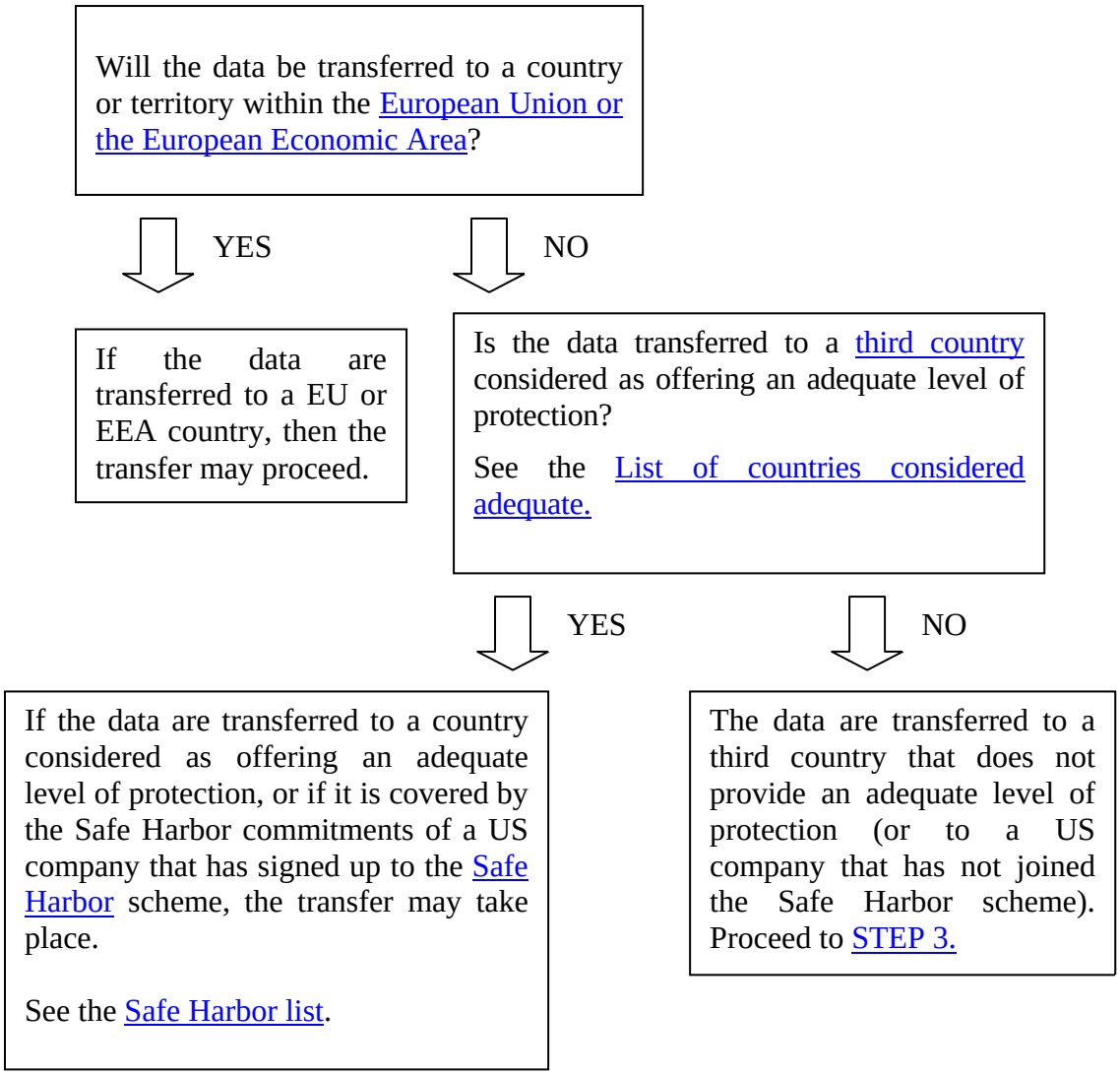
II. Step-by-step decision-making process

The following process should be undertaken before any transfer of personal data takes place:

STEP 1

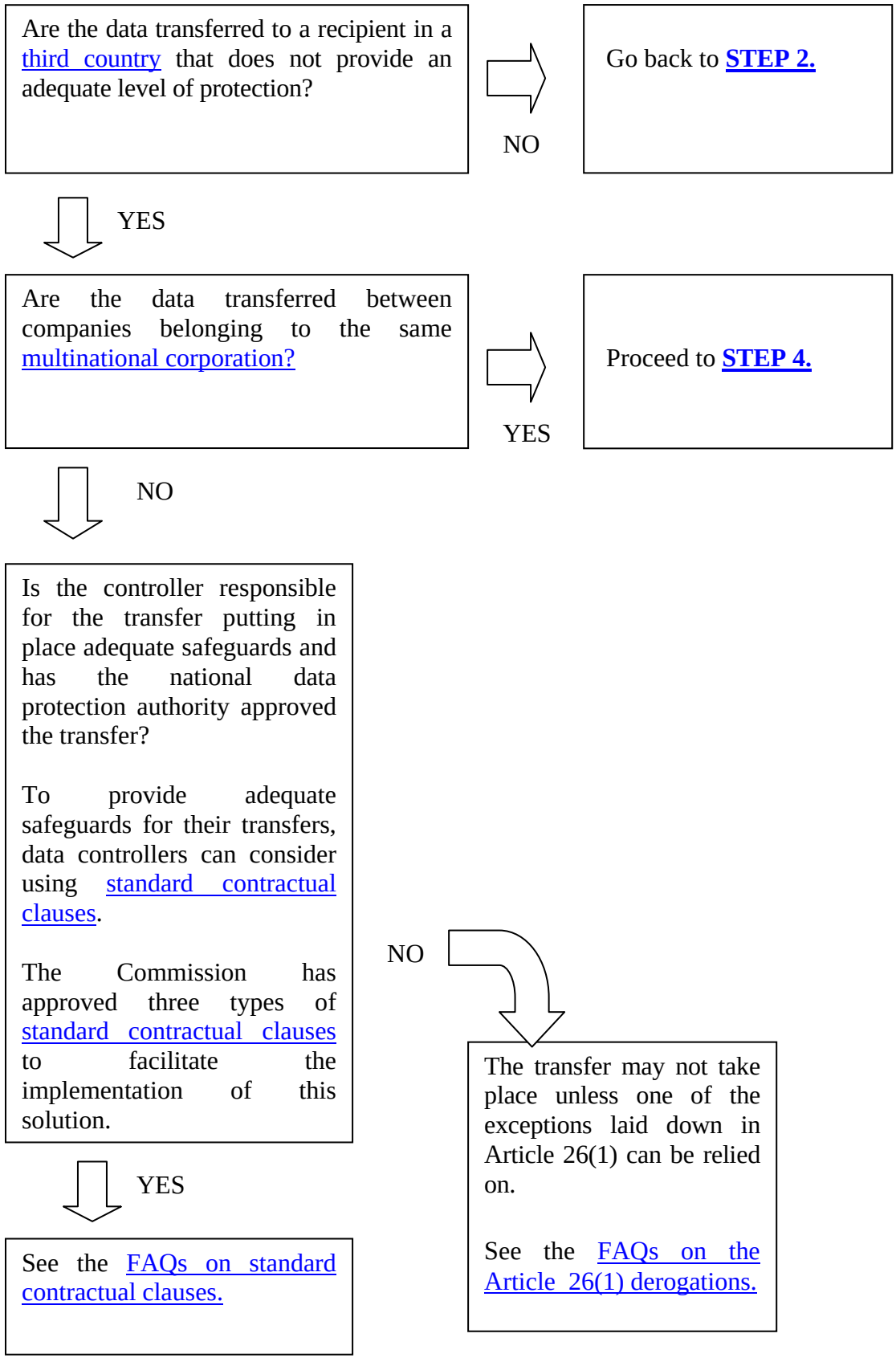


STEP 2



For more details on this step, please refer to the FAQs on general questions.

STEP 3


Are the data transferred to a recipient in a third country that does not provide an adequate level of protection?
NO
Go back to STEP 2.
YES
Are the data transferred between companies belonging to the same multinational corporation?
YES
Proceed to STEP 4.
NO
Is the controller responsible for the transfer putting in place adequate safeguards and has the national data protection authority approved the transfer?
To provide adequate safeguards for their transfers, data controllers can consider using standard contractual clauses.
The Commission has approved three types of standard contractual clauses to facilitate the implementation of this solution.
NO
The transfer may not take place unless one of the exceptions laid down in Article 26(1) can be relied on.
See the FAQs on the Article 26(1) derogations.
YES
See the FAQs on standard contractual clauses.

STEP 4

Are the data transferred between companies belonging to the same multinational corporation established in third countries that do not ensure an adequate level of protection?

NO → Go back to **STEP 2.**

YES

Has the multinational corporation adopted binding corporate rules that are approved by the national data protection authority?

YES → See the FAQs on binding corporate rules.

OR ALTERNATIVELY

Do the companies use standard contractual clauses for transfers of personal data between companies belonging to the same multinational corporation?

The Commission has approved three types of standard contractual clauses to ease the implementation of this solution.

YES → See the FAQs on standard contractual clauses.

NO

If the use of standard contractual clauses or binding corporate rules is not practical and/or feasible, the transfer may not proceed unless one of the exceptions laid down in Article 26(1) can be relied on.

See the FAQs on the Article 26(1) derogations.

III. Glossary

Personal data

Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Art. 2(a) of the Data Protection Directive.

This definition is meant to be broad. The principles of protection must apply to any information concerning an identified or identifiable person. In order to determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person. Some examples of "personal data" are a person's address, credit card number, bank statements. See Opinion No 4/2007 on the concept of personal data issued by the Article 29 Working Party (WP 136).

Processing of personal data

Processing of personal data means *any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.* Article 2(b) of the Data Protection Directive.

Personal data filing system ("filing system")

A personal data filing system (filing system) means *any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.* Article 2(c) of the Data Protection Directive.

Data subject

An identified or identifiable person to whom the personal data relate. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Article 2(a) of the Data Protection Directive See Opinion No 4/2007 on the concept of personal data issued by the Article 29 Working Party (WP 136).

European Union and European Economic Area countries

The area set up by the EEA agreement, comprising the 27 Member States of the European Union and the three countries of EFTA (the European Free Trade Association) which are bound by the Agreement on the European Economic Area (EEA). The 27 Member States are Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom. The three EFTA countries which are also bound by the Data Protection Directive, through being part of the EEA, are Iceland, Liechtenstein and Norway.

Switzerland is a member of EFTA but is not part of the EEA. It is therefore not bound by the Data Protection Directive but has "third country" status. Switzerland has been considered to be a third country offering an adequate level of protection in accordance with Article 25 of the Directive (see List of adequate countries).

Third country

Any country other than the EU and EEA Member States.

Article 29 Working Party

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data is one of the bodies competent for interpreting the provisions of the Data Protection Directive. It carries out this task by issuing recommendations, opinions and working documents on different aspects of the Data Protection Directive. The Article 29 Working Party is composed of representatives of the national data protection authorities of the EU Member States, representatives of the European Data Protection Supervisor and representatives of the European Commission.

Working Paper 12 (WP 12)

Working Paper 12 (WP 12) is a working document issued by the Article 29 Working Party on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive". This document covers all the central questions raised by flows of personal data to third countries in the context of the application of Directive 95/46/EC. Among other things, it sets out the core criteria that the Article 29 Working Party considers third countries should fulfil to provide an adequate level of protection for personal data.

Data protection authority

The national data protection authority is an independent public authority responsible for monitoring the application of data protection law within its territory.

Each national authority should be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;
- the power to engage in legal proceedings where the national provisions have been violated or to bring these violations to the attention of the judicial authorities;
- jurisdiction to hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms with regard to the processing of personal data.

For a list of the Member States' national data protection authorities and their contact details, please click here.

Controller

The controller is *the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.* Article 2(d) of the Data Protection Directive.

Being a controller carries with it serious legal responsibilities, so an organisation which processes personal data should be quite clear if these responsibilities apply to it.

In practice, to find out who controls the contents and use of personal information kept, an organisation should ask itself the following questions:

- who decides what personal information is going to be kept?
- who decides the use and purpose to which the information will be put?
- who decides on the means of processing of personal data?

If that organisation controls and is responsible for the personal data which it holds, then it is a controller. In some instances it is likely that these decisions are taken jointly with other organisations, in which case both organisations will be co-controllers. If, on the other hand, an organisation holds the personal data, but some other organisation decides on and is responsible for what happens to the data and the first organisation acts under the instruction of that other organisation, then that other organisation is the data controller, and the first one is a "processor".

Processor

The processor is the *natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.* Article 2(e) of the Data Protection Directive.

If an organisation holds or processes personal data, but does not exercise responsibility for or control over the personal data, then this organisation is a "processor".

Examples of processors include payroll companies, accountants and market research companies, call centres of telecom or financial companies, all of which could hold or process personal information on behalf of someone else.

It is possible for one company or person to be both a controller and a processor, in respect of distinct sets of personal data. For example, a payroll company would be the data controller in respect of the data about its own staff, but would be the processor in respect of the staff payroll data it is processing for its client companies.

A processor is distinct from the controller for whom he is processing the personal data. An employee of a controller, or a section or unit within a company which is processing personal data for the company as a whole, is not a "processor". However, someone who is not employed by the controller, but is contracted to provide a particular data processing service (such as a tax adviser, or a telemarketing company used to manage customer accounts) would

be a processor. A subsidiary company owned by a controller to process personal data on its behalf (for example to manage the payroll) is a distinct legal person and is a processor.

Third party

Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data. Article 2(f) of the Data Protection Directive.

Safe Harbor

In order to bridge the different privacy approaches between the EU and the US and provide a way for US organisations to reach an adequate level of protection of personal data as required by the Data Protection Directive, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework which the Commission considered as providing an adequate level of protection.
More information on the Safe Harbor principles can be found on the European Commission website and on the website of the US Department of Commerce. The list of US companies having signed up to the Safe Harbor scheme is available here.

Multinational corporation

For the purposes of these FAQs, a multinational corporation is a closely-knit, highly hierarchically structured multinational company.

Binding corporate rules

Binding corporate rules may be described as an international code of practice followed by a multinational corporation for transfers of personal data between the companies belonging to the same multinational corporation. Any multinational corporation wishing to transfer personal data between its own companies on an international basis can consider using binding corporate rules, which must be approved by the national data protection authority pursuant to its own national legal procedures. For more details, please refer to the FAQs on binding corporate rules.

Standard contractual clauses

The Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards as required by Article 26(2), that is, they provide 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.

The effect of such a decision is that by incorporating the standard contractual clauses into a contract, personal data can flow from a data controller established in any of the 27 EU Member States and three EEA member countries (Iceland, Liechtenstein and Norway) to a data controller established in a country not ensuring an adequate level of data protection. Except in very specific circumstances, national data protection authorities cannot block such transfer.

Two sets of standard contractual clauses have been adopted for transfers between data controllers, and one set exists for transfers between a data controller and a data processor.

See the FAQs on such standard contractual clauses for more information and information on the use of non-standard contractual clauses.

List of countries covered by a Commission Adequacy Finding Decision

List of countries considered as offering an adequate level of protection in accordance with Article 25 of the Data Protection Directive:

- On the one hand, the European Commission has the power to make determinations of adequacy which are binding on EU (and EEA) Member States. Positive determinations of adequacy have hitherto been made for **Switzerland**, **Canada**, with regard to transfers made to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act, **Argentina**, the Bailiwick of **Guernsey**, the **Isle of Man,** the Bailiwick of **Jersey** and the **Safe Harbor** Privacy Principles of the United States Department of Commerce. The Decisions can be found here.

- In addition, Member States may also assess the adequacy of third countries. This assessment will be made in the light of all the circumstances surrounding a data transfer. The law of the Member State may lay down rules for determining whether the protection afforded by a third country is adequate. Data controllers should therefore check with their national data protection authority whether additional third countries, specific data transfer operations or sets of data transfer operations to third countries are considered adequate according to their national data protection legislation. For a list of the Member States' national data protection authorities and their contact details, please click here.

Sensitive data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures. Article 8 of the Data Protection Directive

Law applicable to a processing of personal data activity

The data protection law of an EU/EEA country applies to the processing of personal data in the following circumstances:

- the processing is carried out in the context of the activities of an establishment of the controller on the territory of the EU/EEA country; when the same controller is established on the territory of several EU/EEA countries, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

- the controller is not established on the EU/EEA country's territory, but in a place where its national law applies by virtue of international public law;

- the controller is not established on EU/EEA territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the EU/EEA country, unless such equipment is used only for purposes of transit through the

territory of the EU/EEA. In this case, the controller must designate a representative established in the territory of that EU/EEA country. (Article 4 of the Data Protection Directive).

IV. Frequently Asked Questions: table

A. Frequently Asked Questions: general questions

B. Frequently Asked Questions: standard contractual clauses

B.1. General FAQs regarding the three sets of rules

B.2. FAQs regarding Sets I and II: transfer of personal data from controller to controller outside the EU/EEA

General questions — difference between the two sets

FAQs regarding Set I (Decision 2001/497/EC)

V. Frequently Asked Questions relating to the transfer of personal data from the EU/EEA to third countries

Introduction

Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* requires Member States to restrict transfers of personal data to countries outside the European Economic Area (EEA) to situations where the third country concerned ensures an adequate level of protection for such data. Where this is not the case, the transfer may not take place.

However, where the third country to which the personal data is to be exported does not ensure this adequate level of protection, the Data Protection Directive provides that a transfer may take place none the less:

- if the Member State authorises the transfer when the entity responsible for the processing offers appropriate guarantees regarding the protection of privacy and fundamental rights and freedoms, as well as with regard to the exercise of these rights. Such protection can be ensured by way of a contract binding the exporter and the importer of data ("contractual clauses"), or, with regard to flows among the different organisations of a multinational company, via the adoption of a binding code of conduct containing appropriate data protection guarantees (binding corporate rules) (Data Protection Directive , Article 26(2) and (4));

- under one of the limited derogations laid down explicitly in the Data Protection Directive (Article 26(1)).

The purpose of this framework is to ensure that the level of protection of the fundamental right to the protection of personal data established by the Data Protection Directive is not undermined, given the ease with which personal data can be moved around on international networks. This rule is also aimed at ensuring that data subjects (persons whose personal data are processed) will continue to be protected when their personal data leave EU/EEA territory.

A. Frequently Asked Questions: general questions

1. WHAT IS AN INTERNATIONAL TRANSFER OF PERSONAL DATA?

The term “transfer of personal data” is often associated with the act of sending or transmitting personal data from one country to another, for instance by sending paper or electronic documents containing personal data by post or e-mail. Other situations also fall under this definition: all the cases where a controller takes action in order to make personal data available to a third party located in a third country. However the Court of Justice has stated that that there is no "*transfer of personal data to a third country" where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country". (Case C-101-01, Bodil Lindqvist, ECR, 2003-Page I-12971)*

2. WHAT CONDITIONS HAVE TO BE FULFILLED FOR AN INTERNATIONAL TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY TO BE LAWFUL?

International transfers of personal data will be considered lawful only if, prior to the transfer, the personal data have been collected and further processed in accordance with the national data protection laws applicable to the data controller established in the EU.

Data protection laws generally demand good data management practices on the part of the entities that process data (“controllers”) and include a series of obligations and rights for data subjects. These include the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to collect only relevant and necessary data, the obligation to guarantee the security of the data against accidental or unauthorised access or manipulation and in specific cases the obligation to notify the competent independent supervisory body before carrying out all or certain types of data processing operations. These laws provide for a series of rights for individuals such as the right to receive certain information whenever data

are collected, the right of access to the data and, if necessary, the right to have the data corrected, and the right to object to certain types of data processing. These laws also provide for certain safeguards or special procedures to be applied in case of transfers of data abroad.

Each controller has to comply with the provisions of the Member State where he or she is established even if the personal data relate to data subjects established in other Member States. When the controller is not established in the Community (e.g. a foreign company) he or she has to comply with the law of the Member State(s) where the processing equipment (e.g. a computing centre) is located or where equipment is used. In this case these controllers are required to appoint a representative established in the Member State(s) where the processing equipment is situated.

3. MAY I TRANSFER PERSONAL DATA FOR A DIFFERENT PURPOSE THAN THE ONE FOR WHICH THE DATA WERE INITIALLY COLLECTED AND PROCESSED?

As previously explained, the Data Protection Directive requires that before any transfer is made, the processing of personal data must comply with the national data processing law. A fundamental principle of data protection laws is that data must be collected for a specific purpose and may not be re-used for further purposes incompatible with the initial one, unless this is required by national legislation. Therefore, in principle, re-using personal data for a different purpose which is incompatible with the initial one is unlawful, unless required by law. The transfer of the data for this second use is therefore unlawful, unless it is required by legislation of the Member State to which the controller is subject.

For example, collecting personal data for a specific commercial transaction with a customer, and later on deciding to export the data to another firm for the purposes of direct marketing is unlawful unless it has been initially notified to the data subject, who has been informed of his/her right to oppose such use.

4. WHAT IS A "THIRD COUNTRY"?

A "third country" is any country other than the 27 EU Member States (Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom) and the three Parties to the EEA (European Economic Area) countries which are not part of the EU but have agreed to be bound by the Data Protection Directive (Iceland, Liechtenstein and Norway).

5. WHAT ARE THE MAIN RULES I HAVE TO APPLY WHEN TRANSFERRING PERSONAL DATA TO A "THIRD COUNTRY" FROM THE EU/EEA?

When personal data are transferred from a Member State to a "third country" two conditions must be respected. First, the processing must comply with the applicable national requirements laid down in order to lawfully process personal data in that Member State or EEA member country (see question 2). Second, the level of data protection in this third

country should be assessed in accordance with the applicable national law in order to ensure that the third country in question ensures an adequate level of protection. The law of the Member State may lay down rules for determining whether the protection afforded by a third country is adequate. You should consult your national data protection authority.

In addition, mechanisms have been developed to provide for legal certainty: the Commission may determine — and EU Member States are bound by such decision — that a third country ensures an adequate level of protection (either as a whole or for specific areas). This decision is referred to as "Commission adequacy finding". Some call this list of countries the "list of adequate countries" (see question 6).

If the recipient third country is found not to ensure an adequate level of protection, the transfer may still be possible and allowed, but only in certain circumstances::

1. when the data controller offers "*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*" (Article 26(2)). These safeguards may result from appropriate contractual clauses, and more particularly from standard contractual clauses issued by the Commission according to Article 26(4) of the Directive (see the FAQs on standard contractual clauses). In the case of multinationals, the adoption of binding corporate rules could be an appropriate solution (see the FAQs on binding corporate rules); or

2. under the derogations laid down in Article 26(1) of the Data Protection Directive (for more details about these derogations, see the FAQs on the Article 26(1) derogations).

6. WHICH THIRD COUNTRIES DO ENSURE AN ADEQUATE LEVEL OF PROTECTION ACCORDING TO A COMMISSION DECISION UNDER ARTICLE 26(4)?

The Commission has recognised Switzerland (July 2000), Canada (December 2001), Argentina (June 2003), the Bailiwick of Guernsey (Nov. 2003), the Isle of Man (April 2004), the US Department of Commerce's Safe Harbor Privacy Principles of the US Department of Commerce (July 2000) and the Bailiwick of Jersey (2008). For a list of companies that have signed up the Safe Harbor scheme, please click here.

7. WHAT ARE THE CONDITIONS TO BE RESPECTED FOR TRANSFERRING PERSONAL DATA TO SUCH THIRD COUNTRIES ENSURING AN ADEQUATE LEVEL OF PROTECTION ACCORDING TO A COMMISSION DECISION?

Any transfer of personal data to third countries recognised as ensuring an adequate level of protection or to companies that have signed up to the Safe Harbor principles may take place without any additional condition over and above those for transfer to a third party or to a processor located within the EU/EEA as laid down in your national data protection act. The data protection laws of all Member States are available here.

No additional authorisation of your national data protection authority is needed in this particular case as Member States are bound to comply with the decisions of the Commission in this field.

8. DO I HAVE TO INFORM DATA SUBJECTS ABOUT THE TRANSFER OF THEIR PERSONAL DATA TO A THIRD COUNTRY?

In order to guarantee the fair processing of personal data, data controllers should inform the data subject, prior to the transfer, about the transfer of their data to a third country (including whether this third country ensures an adequate level of protection) and the purposes of this international transfer. Therefore, prior to a transfer of personal data, it is important to check on the national data protection requirements. The data protection laws of all Member States are available here. For more information on the applicable national laws, please contact your national data protection authority. For a list of the Member States' national data protection authorities and their contact details, click here.

9. MAY COMPANIES TRANSFER PERSONAL DATA TO THIRD COUNTRIES WHICH DO NOT ENSURE AN ADEQUATE LEVEL OF PROTECTION?

Yes, but only under the following (**alternative**) conditions:

1. The national data protection authority of your Member State has authorised the transfer on the basis that the company has adduced 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.

   E.g. you have concluded a contract with the data importer which includes appropriate written contractual clauses relating to data protection and the data protection authority of your Member State has accepted these clauses.

2. The company has concluded a contract with the data importer using one of the three sets of EU approved standard contractual clauses. For more details, please refer to the FAQs on the standard contractual clauses.

3. A multinational corporation has adopted binding corporate rules for transfers of personal data between companies belonging to the same multinational corporation which have been approved by the relevant data protection authorities. For more details, please refer to the FAQs on binding corporate rules.

4. One of the following exceptional situations provided for in Article 26(1) of the Data Protection Directive applies (see Section D of the FAQs):

(a) the data subject has unambiguously given his free and informed consent to the proposed transfer (more details);
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request (more details);

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (more details);
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (more details);
(e) the transfer is necessary in order to protect the vital interests of the data subject (more details);
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (more details).

To determine whether you are allowed to rely on any of the derogations quoted here above, please read carefully the questions related to the derogation(s) which seem(s) relevant to your situation (click on "more details"). All derogations do indeed must be interpreted strictly and do cannot be presumed to apply to all conceivable situations.

10. IN THE CASE OF A TRANSFER TO A THIRD COUNTRY WHICH DOES NOT ENSURE AN ADEQUATE LEVEL OF PROTECTION, IF MORE THAT ONE WAY IS AVAILABLE TO ENSURE COMPLIANCE WITH THE APPLICABLE NATIONAL LAW ON CROSS-BORDER DATA FLOWS, IS THE COMPANY ALLOWED TO CHOOSE BETWEEN THEM?

The Article 29 Working Party in its paper entitled "*Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*" (available here) is of the opinion that the derogations in Article 26(1) of the Data Protection Directive (i.e. the derogations detailed under point 4(a) to (f) in the previous question) have to be interpreted strictly, being a limitations of a fundamental right.

Consequently, when two or more solutions can be applied to a particular case, the following order should be respected so that the derogation which ensures the highest level of data protection is applied:

1. the transfer has been authorised on a case-by-case basis by the national data protection authority, because the data controller offers "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". These safeguards may, in particular result from the following:

    a. for multinationals, binding corporate rules have been adopted and the transfer occurs between companies belonging to the same multinational;
    b. one set of the existing standard contractual clauses has been included in the contract with the data importer; in some Member States, an additional authorisation of the national data protection authority is still needed;
    c. other adequate safeguards have been adopted by the data controller (e.g. self-drafted contractual clauses) and authorised by the national data protection authority;

the transfer falls under one of the derogations laid down in Article 26(1) of the Data Protection Directive.
For example, if the transfer of personal data to a country not ensuring an adequate protection can be performed by obtaining the consent of the data subjects OR by concluding a contract with the data importer which includes the EU approved standard contractual clauses, the second solution should be applied, because it ensures a higher level of data protection.

11. WHAT HAPPENS IF I TRANSFER PERSONAL DATA TO A THIRD COUNTRY WITHOUT COMPLYING WITH THE LEGAL RULES APPLICABLE IN THE MEMBER STATE WHERE THE PROCESSING ACTIVITY TAKES PLACE?

Such transfer is unlawful; it violates the national data protection legislation. National authorities are required by the Data Protection Directive to take measures to enforce compliance with the laws they adopt to implement the Data Protection Directive. In addition to possible fines or sanctions which they may impose in accordance with their national law (administrative or criminal penalties), they may require t the transfers to the third country to cease. Finally, any data subject who has suffered damage as a result of the transfer may seek compensation for that damage.

12. WHOM SHOULD I CONTACT FOR CLARIFICATION?

For specific questions relating to an envisaged transfer of personal data to a third country, you are invited to contact your national data protection authority. For a list and contact details of the Member States' national data protection authorities in the EU and the EEA, please click here.

B. Frequently Asked Questions: standard contractual clauses

Article 26(4) of the Data Protection Directive empowers the Commission to decide that certain standard contractual clauses offer sufficient safeguards as required by Article 26(2), that is, they provide 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.

The effect of such a decision is that by incorporating the standard contractual clauses into a contract, personal data may be transferred from a data controller established in any of the 27 EU Member States and three EEA member countries (Iceland, Liechtenstein and Norway) to a data controller or processor established in a country not ensuring an adequate level of data protection.

Introduction: three sets of contractual clauses — which one should I choose?

Up to now, the Commission has approved three sets of contractual clauses.

Two of these sets of contractual clauses apply to transfers from data controllers in the EU/EEA to controllers in third countries: see Decision 2001/497/EC (Set I) and Decision 2004/915/EC (the so-called "business clauses" — Set II).
The third set applies to transfers from data controllers in the EU/EEA to processors in third countries (Decision 2002/16/EC).
Consequently, companies will either have the possibility to choose between two sets of standard contractual clauses (for transfers from EU/EEA controllers to non-EU/EEA controllers — Set I and Set II) or only have the opportunity to use one set (for transfers from EU/EEA controllers to non-EU/EEA processors). As explained in question 4 below, this does not, however, prevent companies relying on different contracts approved at national level by data protection authorities.

A number of questions regarding the standard contractual clauses are common to the three sets; these are examined in the first section before going deeper into the issues raised by each set of specific clauses.

FAQs regarding the standard contractual clauses: contents list

B.1. General FAQs regarding the three sets of rules

1. WHAT ARE THE PRINCIPLES BEHIND THE STANDARD CONTRACTUAL CLAUSES?

They reflect the requirements in the Data Protection Directive that:

- Personal data should be collected only for specified, explicit and legitimate purposes;
- The persons concerned should be informed about such purposes and the identity of the data controller;
- Any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect; and
- If something goes wrong, appropriate remedies must be available to put things right, including compensation or damages through the competent courts.

The principal aim of the clauses is to ensure that these principles are applied when personal data is transferred outside the European Union or European Economic Area.
In many cases the free flow of personal information will be essential for the efficient conduct of economic activity on an international basis.

2. ARE THE STANDARD CONTRACTUAL CLAUSES COMPULSORY FOR COMPANIES INTERESTED IN TRANSFERRING DATA OUTSIDE THE EU/EEA?

No. The standard contractual clauses are neither compulsory for businesses nor are they the only way of lawfully transferring data to countries outside the EU (and the EEA).

First of all, organisations do not need contractual clauses if they want to transfer personal data to recipients in third countries that have been recognised as providing an adequate level of protection of personal data (see the list of adequate countries).

Secondly, under Article 26(2), national authorities may authorise on a case-by-case basis specific transfers to a third country not considered to offer an adequate level of protection where the exporter in the EU 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. This could be done, for example, through contractual arrangements between the exporter and the importer of data, subject to the prior approval of national data protection authorities. Please refer to your national rules for this.

Thirdly, for multinationals, the adoption of binding corporate rules, approved by national data protection authorities, could be the appropriate solution for cross-border data transfers within the framework of the multinational corporation.

Finally, even if the third country of destination or the recipient of the data does not offer an adequate level of protection, as discussed above, data may be transferred in specific, exceptional circumstances. These are listed in Article 26(1) and include cases where:

1. the data subject has unambiguously given his free and informed consent to the proposed transfer; or
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
5. the transfer is necessary in order to protect the vital interests of the data subject; or
6. the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

The Article 29 Working Party in its paper entitled "*Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*" (available here) is of the opinion that such derogations should however be applied restrictively and the adoption of standard contractual clauses or other solutions should be preferred where possible.

3. DO THESE CLAUSES SET A MINIMUM STANDARD FOR INDIVIDUAL CONTRACTS OR FUTURE MODEL CONTRACTS?

No. The standard contractual clauses do not have any effect on the individual contracts themselves or on future model contractual clauses.
The Commission Decisions simply require Member States to recognise that the contractual clauses annexed to the decision provide adequate safeguards and fulfil the requirements laid down in Article 26(2) of the Data Protection Directive for data transfers to third countries that do not ensure an adequate level of protection for personal data.

4. CAN COMPANIES STILL RELY ON DIFFERENT CONTRACTS APPROVED AT NATIONAL LEVEL?

Yes. The standard contractual clauses do not prejudice past or future contractual arrangements authorised by national data protection authorities pursuant to national legislation.
Authorisations at national level may be granted if national data protection authorities consider that the safeguards adduced by controllers exporting personal data to a third country to protect the individual's privacy are sufficient in relation to the specific transfer. The content of these national contracts may differ from the Commission's standard contractual clauses. These contracts need to be notified by the Member States to the Commission and the other Member States.

5. WHEN USING THE STANDARD CONTRACTUAL CLAUSES, DO COMPANIES STILL NEED A NATIONAL AUTHORISATION TO PROCEED WITH THE TRANSFER?

Member States are under the obligation to recognise the standard contractual clauses approved by the Commission as fulfilling the requirements laid down by the Data Protection Directive for the export of data to a third country, and consequently may not refuse the transfer. In most cases there is no need for a prior national authorisation to proceed with the transfer but some Member States maintain a licensing system. Where they do so, the national

data protection authority will compare the clauses actually contained in the contract with the standard contractual clauses and verify that no change has been made. In this case, the authorisation is automatically granted and its requirement can in no way delay or hinder the performance of the contract.

6. Is the deposit of the contract with the Member States compulsory? And can the transfer take place before the deposit?

The answer may vary from one Member State to another, as this is an option under the standard contractual clauses. Some Member States request the deposit of the contract. Others may request the presentation of the contract or decide that no deposit or presentation will be necessary. Should the deposit or presentation of the contract be requested at national level, Member States will determine the procedure dealing with this question.

The deposit of the contract is only a formality, to facilitate the work of the national data protection authorities and should not unduly delay the performance of the contract.

7. How can companies protect their confidential information if they have to deposit a copy of these clauses with the supervisory authorities and provide the data subject with a copy on request?

In the case of standard contractual clauses, the clauses relating to the protection of personal data are those already in the public domain, and published in the Annex to the Commission Decision. All other clauses relating to the company's business can remain confidential. Moreover, national data protection authorities and the European Commission are bound by a duty of confidentiality when exercising their duties.

8. Can Member States block or suspend data transfers using the standard contractual clauses?

Yes, but only in the exceptional circumstances referred to in Article 4 of the Commission Decisions. These include cases where:

(a) it is established that the law of the third country to which the data importer is subject requires him to derogate from the relevant data protection rules beyond the restrictions necessary in a democratic society as provided for in Article 13 of the Data Protection Directive and those derogations 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 continuing transfer would create an imminent risk of grave harm to the data subjects.

It is expected that this safeguard clause will be very rarely used as it caters for exceptional cases only. As provided for in Article 4(3) of the Decisions, the European Commission will be informed of any use made by the Member States of this safeguard clause and will forward the information received to the other Member States.

It is also important to recall that prior to the transfer it is the national law implementing the Data Protection Directive that applies to the processing of personal data and not the standard contractual clauses. In other words, transfers to a third country can be lawfully made only if the data have been collected and further processed in accordance with the applicable national laws by the data controller established in the EU.

Therefore, companies interested in using the standard contractual clauses would still need to comply with the conditions for the lawfulness of the disclosure of the personal data in the Member State of the EU/EEA where the data exporter is established. Where a disclosure of data to a third party recipient within a Member State would not be lawful, the mere circumstance that the recipient may be situated in a third country does not change this legal evaluation.

9. CAN COMPANIES INCLUDE THE STANDARD CONTRACTUAL CLAUSES IN A WIDER CONTRACT AND ADD SPECIFIC CLAUSES?

Yes. Parties are free to agree to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses approved by the Commission or prejudice fundamental rights or freedoms of the data subjects. It is possible, for example, to include additional guarantees or procedural safeguards for the individuals (e.g. on-line procedures or relevant provisions contained in a privacy policy). All these other clauses that parties may decide to add would not be covered by the third-party beneficiary rights and would benefit from confidentiality rights where appropriate.

Member States may also add additional items to the Appendix to the set of clauses adopted in 2001. In this Appendix, parties to the contract are expected to provide certain information about the categories of data being transferred and the purposes of the transfer.

In all cases, the standard clauses have to be fully respected if they are to have the legal effect of providing an adequate safeguard for the transfer of personal data as required by the Data Protection Directive.

10. CAN COMPANIES AMEND AND CHANGE THE STANDARD CONTRACTUAL CLAUSES APPROVED BY THE COMMISSION?

No. Once they change the standard contractual clauses these are no longer “standard”. The companies will consequently not benefit from the specific favourable treatment attached to the standard contractual clauses, i.e. that Member States have to recognise the standard contractual clauses as fulfilling the requirements laid down by the Data Protection Directive for the export of data and consequently may not refuse the transfer (except as stated in question 8 above).
When amending the standard contractual clauses, the companies fall under Article 26(2) of the Data Protection Directive, which provides that national authorities may authorise on a case-by-case basis specific transfers to a country not considered as offering an adequate level of protection where the exporter in the EU 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.

Thus if they amend the standard contractual clauses, companies will need to seek the prior approval of national authorities for their contractual arrangements.

11. CAN US-BASED ORGANISATIONS THAT HAVE JOINED THE SAFE HARBOR SCHEME USE THE STANDARD CONTRACTUAL CLAUSES TO RECEIVE DATA FROM THE EU/EEA?

As a general rule, standard contractual clauses are not necessary if the data recipient is covered by a system providing adequate data protection such as the Safe Harbor scheme. However, if the transfer concerns personal data that are not covered by their Safe Harbor commitments or concerns a sector outside the supervision of the FTC or the Department of Transport, use of the standard contract clauses is one way of providing the necessary safeguards.

12. CAN US-BASED COMPANIES THAT HAVE NOT JOINED THE SAFE HARBOR SCHEME USE THE SAFE HARBOR RULES UNDER THE CONTRACT?

Yes, provided that they also apply the three mandatory data protection principles in Annex 3 to Commission Decision 2001/497/EC (applicable to all countries of destination): the purpose limitation, restrictions on onward transfers and the right of access, rectification, deletion and objection.

B.2. FAQs regarding Sets I and II: transfer of personal data from controller to controller outside the EU/EEA

The controller of the processing of personal data who intends to transfer personal data to another controller located in a country outside the EU/EEA, which does not provide an adequate level of protection, in accordance with his national data protection rules, can use either Set I (Decision 2001/497/EC) or Set II (Decision 2004/915/EC) insofar as he chooses the contractual solution to meet the adequacy requirements of the Data Protection Directive (see other possible solutions).

2.1. General questions — difference between the two sets

Before going deeper into the issues raised by each of these sets, we will tackle a few general questions:

1. Why are there two sets of standard contractual clauses and what are the main differences between them?
2. Can companies combine the clauses of Sets I and II?

1. WHY ARE THERE TWO SETS OF STANDARD CONTRACTUAL CLAUSES AND WHAT ARE THE MAIN DIFFERENCES BETWEEN THEM?

The first set of clauses has been applied successfully in many cases but there was demand from businesses for a wider choice of such clauses. The Commission announced in May 2003, in its first report on the implementation of the 1995 Data Protection Directive, that it was open to offering businesses such a wider choice, based on proposals by business representatives themselves, provided this did not diminish the level of protection for data subjects. The coalition of business associations which negotiated the new clauses with the Commission believes that this new set of clauses is more in line with business needs, as some clauses, such as those related to litigation, allocation of responsibilities or auditing requirements, are more business-friendly.

From the standpoint of data protection and data subjects, however, the clauses adopted in 2004 (Set II) provide for a similar level of data protection as those of 2001 (Set I). In addition, in order to prevent abuses with the system laid down by Set II, the data protection authorities are given more powers to intervene and impose sanctions where necessary, for instance by more easily prohibiting or suspending data transfers based on Set II of contractual clauses.

2. CAN COMPANIES COMBINE THE CLAUSES OF SETS I AND II?

No, each set of contractual clauses as a whole forms a model and accordingly companies cannot combine the sets of clauses without losing the benefit of the specific regime attached to these standard contractual clauses, i.e. that Member States have to recognise the standard contractual clauses as fulfilling the requirements laid down by the Data Protection Directive for the export of data and consequently may not refuse the transfer.

2.2. FAQs regarding Set I (Decision 2001/497/EC)

1. What is meant by “restrictions necessary in a democratic society” in Article 4(1)(a) of the Decision?
2. What is covered by the term “legislation” in Clause 5(a)? And what specific action should the data importer take to ascertain that he is not prevented from fulfilling his obligations under the contract?
3. Recital 9 of the Commission Decision 2001/497/EC states that Member States should retain the power to particularise the information the parties are required to provide. What does this mean?
4. Does compliance with the “mandatory data protection principles” (see Clause 5(b) and Appendices 2 and 3) mean compliance with the provisions of the Data Protection Directive?
5. The model contract of Set I allows the data subject the right of access to his or her personal information (Appendices 2 and 3). Does the right of access apply to both the data exporter and the data importer?
6. What is an onward transfer (Appendices 2 and 3)?
7. Do the restrictions on onward transfers apply to onward transfers to recipients that have been found to provide for adequate protection?
8. What does joint and several liability mean (Clause 6(2); recitals 18-20 of the Decision 2001/497/EC)?
9. But will this not impose unfair burdens on exporters and/or importers who have done nothing wrong?
10. Does joint and several liability mean that the liability of the parties is strict?

1. WHAT IS MEANT BY "RESTRICTIONS NECESSARY IN A DEMOCRATIC SOCIETY" IN ARTICLE 4(1)(A) OF THE DECISION?

Article 4(1)(a) of the Commission Decision approving Set I of standard contractual clauses lays down that the national data protection authority may prohibit or suspend data flows to a third country made on the basis of Set I of standard contractual clauses, in order to protect individuals where "*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 Data Protection Directive 95/46/EC, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses*".

A general principle of the EU data protection legal framework is that any restrictions of the basic data protection principles must be limited to those which are necessary for the protection of fundamental values in a democratic society. These criteria cannot be laid down for all countries and all times but should be considered in the light of the given situation in the country in question. The interests protected are listed in Article 13 of the Data Protection Directive and include all such measures that are necessary to safeguard:

(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of the State, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.

The condition "necessary in a democratic society" derives from Articles 8 to 11 of the European Convention on Human Rights and extensive case law has been developed by the European Court of Human Rights on this issue. The same principle is also included in Council of Europe Convention 108 in respect of restrictions on the data protection principles (Article 9). These texts have been taken into account by the European Court of Justice in its interpretation of Article 13 of the Data Protection Directive (see Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003] ECR I-4989).

2. WHAT IS COVERED BY THE TERM "LEGISLATION" IN CLAUSE 5(A)? AND WHAT SPECIFIC ACTION SHOULD THE DATA IMPORTER TAKE TO ASCERTAIN THAT HE IS NOT PREVENTED FROM FULFILLING HIS OBLIGATIONS UNDER THE CONTRACT?

Clause 5 of the contractual clauses (Set I) lays down the obligations imposed on the data importer. According to Clause 5(a), "*the data importer agrees and warrants 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".

The term "legislation" in Clause 5(a) refers to the legal system as a whole; it also covers case law, rules or regulations that may impede the performance of the contract. The data importer should take reasonable care to ascertain whether there are any such rules that might prevent him from fulfilling his obligation.

3. Recital 9 of the Commission decision 2001/497/EC states that Member States should retain the power to particularise the information the parties are required to provide. What does this mean?

Appendix 1 to the contract contains the minimum information that should be included in the contract. That said, it may be necessary to add additional requirements laid down in national law and needed to make the transfer from a specific Member State lawful. For this reason Member States retain the power to add such specifications, relating for example to the details of the intended transfer, the purposes of the transfers, the categories of data. If a Member State decides to particularise the Appendix to the contract, it is that modified Appendix which must be used when personal data are transferred from that Member State.

4. Does compliance with the "mandatory data protection principles" (see Clause 5(b) and Appendices 2 and 3) mean compliance with the provisions of Data Protection Directive ?

No. The mandatory data protection principles reflect a set of substantive data protection principles that guarantee an adequate, not an equivalent or the same, level of protection as in the EU/EEA in case of a transfer of personal data to a third country. They have been construed on the basis of the Working Party's Opinion 12/98.

5. The model contract of set I allows the data subject the right of access to his or her personal information (Appendices 2 and 3). Does the right of access apply to both the data exporter and the data importer?

Both the data exporter and the data importer agree and warrant to respond properly and reasonably to inquiries from the data subjects about the processing of the data transferred. As indicated in Clause 4(d) of Set I, the data exporter will respond to the extent reasonably possible as the questions posed by data subjects would relate to the processing of personal data carried out by the data importer.
Clause 5(c) stipulates that the data importer warrants 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.
Therefore, if a data exporter receives an access request from a data subject concerning processing operations carried out by the data importer, the data exporter is expected to enforce Clause 5(c) against the data importer, if necessary, to give satisfaction to the access request made by the data subject.

The data subject may also directly approach the data importer, who will have to deal promptly and properly with this request.

The "*mandatory data protection principles*" described in Appendices 2 and 3 should be read and interpreted in the light of the provisions (principles and relevant exceptions) of Data Protection Directive. These "mandatory data protection principles", when they refer to the right of access, make explicit reference to Article 12 of the Data Protection Directive.

6. WHAT IS AN ONWARD TRANSFER (APPENDICES 2 AND 3)?

There is an "onward transfer" within the meaning of Set I and Set II of contractual clauses every time personal data is transferred from the data importer to another natural or legal person, also established in a third country, that autonomously determines the purpose and means of processing (i.e. another "controller") .
Processing means any operation which is performed on personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, blocking, erasure or destruction.

7. DO THE RESTRICTIONS ON ONWARD TRANSFERS APPLY TO ONWARD TRANSFERS TO RECIPIENTS THAT HAVE BEEN FOUND TO PROVIDE FOR ADEQUATE PROTECTION?

No, the restrictions on onward transfers apply only to those cases where the second recipient is established in a third country not providing adequate protection or not covered by a Commission decision recognising that a third country ensures an adequate level of protection (**click here** for the **list of adequate countries**).
The restrictions on onward transfers do not apply either when the recipient is established in a Member State of the EU or in an EEA member country (Iceland, Liechtenstein and Norway).

8. WHAT DOES JOINT AND SEVERAL LIABILITY MEAN (CLAUSE 6(2); RECITALS 18-20 OF THE DECISION 2001/497/EC)?

Joint and several liability means that, when data subjects have suffered damage as a consequence of the violation of the rights conferred on them by the contract entered into by the EU data exporter and the third country data importer, they are entitled to obtain compensation from either the data exporter or the data importer or both. Joint and several liability covers those clauses expressly listed in Clause 3 ("*third-party beneficiary clause*") which grant the data subject the right to take action and obtain compensation from the data exporter, the data importer or both.

Without joint and several liability, the data protection safeguards provided for by the standard contractual clauses would be severely diminished. Finding ways of ensuring that the rights of data subjects — who are not parties to the contracts — are adequately safeguarded was the principal challenge of preparing the Commission Decision on standard contractual clauses.
When trying to enforce their rights under a contract between two controllers, one inside and one outside the EU, data subjects are faced with two main difficulties. First, when a data subject becomes aware of a violation of his/her data protection rights, it is often very difficult to know exactly who is responsible for the violation. Were data unlawfully disclosed by the data exporter before the transfer took place or by the data importer after the transfer? Joint and several liability prevents this uncertainty from becoming an obstacle to pursuit of the claim for compensation.

Secondly, even if the data subject knows that the violation has been committed by the importer, it may be very difficult in practical terms for him to enforce the contract and obtain compensation from the importer outside the EU. Making the importer subject to European jurisdiction does not completely solve the problem, because the recognition and enforcement of rulings of EU courts is not always possible in the country where the importer is established. In any event, it is much more straightforward to pursue the claim against the data exporter, who is established in the EU.

9. BUT WILL THIS NOT IMPOSE UNFAIR BURDENS ON EXPORTERS AND/OR IMPORTERS WHO HAVE DONE NOTHING WRONG?

No. Several steps have been taken to ensure that this is avoided. In particular, the scope and applicability of joint and several liability is strictly limited. It only applies to violations of those clauses which produce rights for data subjects (see the "third-party beneficiary clause", Clause 3) and only in cases where it is necessary to compensate individuals for damage resulting from the violation.
As a result, various scenarios that were of concern to industry commentators during the preparation of the Decision are clearly excluded. For instance, companies outside the EU objected that they might be held responsible and brought to court in the EU for the data exporter's violations of the national law (unlawful processing operations) taking place before the data transfer, but this is ruled out by the limited scope of Clause 3. The contractual clauses only cover violations resulting from the transfer itself to a third country, not a breach of national data protection law to which the EU data exporter is subject as controller for his activities of processing personal data within the EU/EEA. Such a violation will be examined and decided in accordance with national data protection law and the rights of the data subject will result from this law (see question 11 in this section)
Companies within the EU, on the other hand, are concerned that they may be required to compensate data subjects for damage resulting from a violation committed by the data importer. This effect is offset by the mutual indemnification clause which, in such a case, would give the exporter the right to recover from the importer any compensation it has had to pay to the data subject (Clause 6(3)). The general rule is that every party to the contract is responsible for his/her acts *vis-à-vis* the data subject.

It may be argued that claiming indemnification will in itself be a burden for exporters. This is recognised, but it is considered fairer to place this burden on exporters rather than on individuals, who will often have had nothing to do with the transfer. Moreover, if the effect of seeking to avoid any such burdens is to make data exporters choose more carefully their data importers this is a wholly welcome effect.

10. DOES JOINT AND SEVERAL LIABILITY MEAN THAT THE LIABILITY OF THE PARTIES IS STRICT?

No. A party can be exempted from liability if it proves that it is not responsible for the violation of the contractual terms that constitutes the event causing the damage (Clause 6 paragraphs 1 and 3). It does not need to prove that the other party is responsible for the damage but at the same time it cannot be exempted from liability simply by alleging that the other party is responsible for the event causing the damage. By way of example, exemption from liability might be possible in cases of *force majeure* or to the extent that the data subject contributes to the event causing the damage.

11. DOES JOINT AND SEVERAL LIABILITY MEAN THAT THE DATA IMPORTER CAN BE SUED FOR THE DATA EXPORTER'S VIOLATION BEFORE THE TRANSFER HAS TAKEN PLACE?

No. This case is excluded from the third-party beneficiary's rights (Clause 3), since the contractual clauses refer to the transfer of personal data from the EU data exporter to the third country data importer. They do not apply to the processing of personal data performed by the EU data exporter within the EU. The Data Protection Directive expressly lays down that prior to the transfer the processing activity must respect the other provisions of the Directive. (See Section A: general questions, question 2).

Data subjects can, however, exercise their rights in the European Union against the data exporter for unlawful processing in the EU in accordance with the national data protection law governing the processing activities of the data exporter.

12. DOES JOINT AND SEVERAL LIABILITY MEAN THAT THE DATA IMPORTER WILL NEVER BE SUED?

Not necessarily. The data subjects may decide to sue the data exporter, the data importer or both. Although an individual may find it easier and therefore prefer to take action against the data exporter before a European court to obtain compensation, he or she may also decide to take action against the data importer; for example if the data exporter has filed for bankruptcy. In these cases, the data subject may decide whether to sue the data exporter or the data importer before the data exporter's courts (Clause 7(1)(b)).

13. DOES JOINT AND SEVERAL LIABILITY MEAN THAT THE DATA EXPORTER HAS TO PAY FOR ANY DAMAGES CAUSED TO INDIVIDUALS AS A CONSEQUENCE OF VIOLATIONS COMMITTED BY THE DATA IMPORTER IN A THIRD COUNTRY?

Yes, but only to the extent that the provision violated is covered by the third-party beneficiary's rights (Clause 3). However "joint and several liability" does not need to leave one party paying for the damages resulting from the unlawful processing by the other party. Clause 6(3) provides for "mutual indemnification" (see recital 20). Subsequently the data exporter may have the right to recover any cost, charge, damages, expenses or loss from the data importer, to the extent that the latter is liable (see Clause 6(3).
Please note, however, firstly that this clause is optional and secondly that what happens in practice will depend on the national laws applicable to the litigation between the exporter and the importer to recover the amount paid.

2.3. FAQs regarding Set II (Decision 2004/915/EC)

1. What are the main differences between this set of clauses and Set I adopted in 2001 by the Commission?
2. Does this set of clauses supersede the set of clauses adopted by the Commission in 2001?
3. Does this set of clauses provide for a lower level of data protection than the clauses adopted by Decision 2001/497 (Set I)?
4. What does "due diligence" mean (recital 5 of Commission Decision 2004/915/EC)? How does it differ from the "joint and several liability" regime provided for in Set I?

1. WHAT ARE THE MAIN DIFFERENCES BETWEEN THIS SET OF CLAUSES AND SET I ADOPTED IN 2001 BY THE COMMISSION?

The Set II clauses (Commission Decision 2004/915/EC) were suggested by a coalition of business associations with a view to providing different models of standard contractual clauses. Most of the clauses of Set II are more extensively detailed and use business vocabulary.

Regarding liability, Set II does not refer to "joint and several liability", but rather relies on the concept of *due diligence* (see FAQ4 below).

The "mandatory principles" in Appendix 2 of Set I are described in Set II under the term "data processing principles". In addition, in order to prevent abuses with the system, the data protection authorities are given more powers to intervene and impose sanctions where necessary.

Finally, the contract contains optional clauses which can be added by the parties, for instance a clause for disputes resolution between the data exporter and the data importer.

2. DOES THIS SET OF CLAUSES SUPERSEDE THE SET OF CLAUSES ADOPTED BY THE COMMISSION BY THE DECISION 2001/497?

No. Both sets of standard contractual clauses remain fully applicable and it is up to the operators to choose the one which best meets their needs. Note that the new set does not cover data transfers to data processors in third countries.

3. DOES THIS SET OF CLAUSES PROVIDE FOR A LOWER LEVEL OF DATA PROTECTION THAN THE CLAUSES ADOPTED BY DECISION 2001/497 (SET I)?

No. Both sets of clauses provide for a similar (adequate) level of data protection standards and principles. Differences between both sets are mainly of a technical nature (for example, the conditions under which a data protection authority may carry out an audit in the data importer's premises) or relate to the differences in the system of liability already explained above.

4. WHAT DOES "DUE DILIGENCE" MEAN (RECITAL 5 OF COMMISSION DECISION 2004/915/EC)? HOW DOES IT DIFFER FROM THE "JOINT AND SEVERAL LIABILITY" REGIME PROVIDED FOR IN SET I?

Set II relies on the concept of "due diligence obligations". The data exporter and the data importer would indeed be liable *vis-à-vis* the data subjects for their respective breach of their contractual obligations, but 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)*. These reasonable efforts may include carrying out audits in data importers' premises or requesting appropriate insurance cover for any damages caused. In the event of damage to the data subject through a data importer's wrongdoing, the data exporter who failed to act with due diligence would also be deemed liable for the damages caused. The data exporter has the burden of proving that it has taken reasonable efforts. The liability regime is detailed in Clause III.

"Joint and several liability" is the concept used in Set I of contractual clauses (see question 8 in section 2.2.). It means that, when data subjects have suffered damage as a consequence of violation of the rights conferred on them by the contract, they are entitled to obtain compensation from either the data exporter or the data importer, or both.

B.3. FAQs regarding the set of clauses for the transfer of personal data to processors established in third countries (Commission Decision 2002/16/EC)

1. IN WHAT SITUATIONS IS IT APPROPRIATE TO USE THIS SET OF CLAUSES?

The clauses have been drafted for the transfer of personal data by controllers established in the Community to recipients established outside the territory of the EU (and the EEA) who act only as processors.
In the case of controllers and processors belonging to the same multinational corporation, another possible solution could be the adoption of binding corporate rules approved by national data protection authorities (see Section C: binding corporate rules).

2. WHAT IS THE LIABILITY SYSTEM USED IN THESE CLAUSES?

The data exporter and the data importer are not jointly and severally liable as in the case of Set I of contractual clauses approved by Decision 2001/497/EC. As the data exporter is the controller of the processing, it remains in any case responsible for the processing. The data subject — who benefits from the "third-party beneficiary clause" (Clause 3) — will thus, in the event of breach of the clauses laid down in Clause 3, mainly take action against the exporter in the EU (i.e. the controller).
As a matter of fact, the data exporter which has been held liable for a violation of the clauses committed by the data importer (the processor), is entitled — to the extent to which the processor is actually liable — to claim indemnification from the data importer for any cost, charges, damages, expenses or loss that it has incurred.

The data subject will only be entitled to enforce the clauses determined in Clause 3 directly against the data importer if it is actually the data importer who breached any of its obligations **and** if the data exporter (the controller) has disappeared or has ceased to exist in law or has become insolvent (Clause 6(2)).

C. Frequently Asked Questions: Binding Corporate Rules

Article 26(2) of the Data Protection Directive provides that a transfer or set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) can be authorised 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. According to the Article 29 Working Party, such adequate safeguards can be provided by the use of binding corporate rules.

1. WHAT ARE "BINDING CORPORATE RULES"?

Binding corporate rules (BCRs) for data protection are a l code of practice based on European data protection standards, which multinational organisations draw up and follow voluntarily to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of a same corporate group and that are bound by these corporate rules. The Article 29 Working Party believes that as long as such corporate rules are binding (both in law and in practice) and incorporate the essential content principles (see question 9) identified in the Working Document (WP 12), there is no reason why national data protection authorities should not authorise transfers between companies belonging to the same multinational group in accordance with their national law.

The Article 29 Working party has issued a first Working Document developing the concept of binding corporate rules and indicating the minimum requirements that should be included in a set of binding corporate rules. The paper called "*Working Document on Binding Corporate Rules for International Data Transfer*" (WP 74), is available here. It has also published a Working Document *setting up a table with the elements and principles to be found in Binding Corporate Rules*" (WP 153) that gives a quick overview of the content required by BCRs with references to the basic document WP 74 and document WP108 "E*stablishing a Model Checklist Application for Approval of Binding Corporate Rules*".

Moreover the Article 29 Working Party has issued further documents in order to facilitate the establishment of binding corporate rules by organisations and clarify questions that may arise to organisations which consider the use of binding corporate rules for their intra group transfers: Working Document *setting up a framework for the structure of Binding Corporate Rules* (WP 154), with a view to help companies in the drafting of BCRs as well a document with specific questions related to the binding corporate rules (WP 155).

A Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data has also been developed by the Article 29 Working Party (WP 133).

2. FOR WHICH COMPANIES ARE BINDING CORPORATE RULES A SUITABLE TOOL?

According to the Article 29 Working Party's opinion (WP 74), binding corporate rules are a suitable tool for closely-knit, highly hierarchically structured multinational companies but not for loose conglomerates. The diversity between their members and the broad scope of the processing activities in which loose conglomerates are involved would not make it possible to meet all the conditions required for binding corporate rules to be legally enforceable.

3. FOR WHICH DATA TRANSFERS ARE BINDING CORPORATE RULES A SUITABLE TOOL?

Binding corporate rules are designed to regulate only **intra-group transfers** world-wide, in other words, exchanges of personal data between companies that are part of the same corporate group and that are bound by these corporate rules.

Binding corporate rules do not cover international transfers of personal data to companies outside the corporate group. Such international transfers would remain possible, not on the basis of the arrangements put in place by legally enforceable binding corporate rules but by virtue of other legal grounds laid down by the Data Protection Directive: Article 25 (transfer to an adequate country), or Article 26 (e.g. the Commission's standard contractual clauses or ad hoc contractual solutions authorised by the data protection authority under Article 26(2) concluded with the recipients of the information), or under one of the derogations laid down in Article 26(1) (see the FAQs in Section D on the Article 26(1) derogations).

In its document WP155, the Article 29 Working Party has explained that BCRs are a legal means to provide adequate protection to personal data covered by the Data Protection Directive and transferred out of the EU/EEA 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/EEA, does not have to be covered by the rules.

However, in the opinion of the Article 29 Working Party, 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 (see also infra FAQs 7 & 8 in this section).

With regard to whether or not BCRs apply to data processors who are not part of the group, the Article 29 Working Party points out that 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. In this respect, 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 the Data Protection Directive. 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 Data Protection Directive.

If the processors are not part of the group and are based outside of the EU/EEA, the transfers by members of the group to them will therefore have to comply with Articles 25 and 26 of the Data Protection Directive on transborder data flows and ensure an adequate level of protection as indicated before in this FAQ. The BCRs will need to address these situations. (WP 155 and WP154, points 11 and 12)

4. How do binding corporate rules work in practice?

Binding corporate rules must apply generally throughout the corporate group, irrespective of the place of establishment of the companies involved in transfers of personal data or the nationality of the individuals whose personal data is being processed or any other criteria or consideration. The Article 29 Working Party has also stressed that there are two conditions that must be satisfied in all cases if corporate rules are to be used to adduce safeguards for data exports: the binding nature and legal enforceability of these binding corporate rules. To establish the binding nature and legal enforceability of BCRs, it is also necessary to take account of national legal systems. .

5. What does "binding nature" mean?

The binding nature of the rules means, **in practice**, that the members of the corporate group which will use the binding corporate rules for their intragroup transfers, as well as each employee within it, must be compelled to comply with the rules. In that respect, relevant features could include the existence of disciplinary sanctions in the event of a breach of the rules, individual and effective information of employees, setting up special education programmes for employees and subcontractors and an internal complaint system to deal with complaints lodged by data subjects. In document WP 108 (model checklist), the Article 29 Working Party suggests several features that may demonstrate the internally binding character of corporate rules.

The Article 29 Working Party has indicated that, ideally, the corporate rules should be signed off by the board of directors of the ultimate parent of the group to ensure compliance across the entire organisation (WP 74).

Binding corporate rules should also contain a clear provision to the effect that that where a member of the corporate group has reasons to believe that the legislation applicable to it may prevent it from fulfilling its obligations under the binding corporate rules and may have a substantial adverse effect on the guarantees provided by them, it must promptly inform the headquarters in the EU, or the EU member with delegated data protection responsibilities (see question 6), unless otherwise prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

In order to determine the instrument that should be used to establish the binding character in each Member State, it is necessary to take into account the legal systems of each Member State where the BCRs are to be applied. The headquarters in the EU or, where the group has its headquarters outside the EU, the EU member with delegated data protection responsibilities should take a responsible decision and must consult the competent data protection authorities (WP 74).

6. WHO HAS THE RESPONSIBILITY TO GUARANTEE THE BINDING NATURE OF THE RULES?

The internally binding nature of the rules must be clear and sufficient to be able to guarantee compliance with them outside the EU/EEA, normally under the responsibility of the European headquarters, which must take any necessary measures to guarantee that any foreign member brings their processing activities into line with the undertakings contained in the binding corporate rules.
If the headquarters of the corporate group were not in the EU/EEA but somewhere else, the headquarters should delegate these responsibilities to a member based in the EU in order that the effective adducer of the safeguards remains responsible for the effective compliance with the rules and guarantees enforcement (WP 74). This member would accept liability for breaches of the rules outside of the EU/EEA. 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. This liability only needs to extend to data transferred from the EU/EEA under the binding corporate rules

However, the Article 29 Working Party has seen that 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 Article 29 Working Party would accept that where the group can demonstrate why it is not possible for them to nominate a single entity in the EU/EEA, it 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 (SET I) or to define an alternative liability scheme based on due diligence obligations as prescribed in the EU Standard Contractual Clauses 2004/915/EC (SET II). A last possibility, specific for transfers made from controllers to processors is the application of the liability mechanism of the Standard Contractual Clauses 2002/16/EC.

Data protection authorities may accept those alternative solutions mentioned above to liability on a case-by-case basis where sufficient and adequate assurance 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. For more detail please refer to document WP 155.

7. WHAT DOES "LEGAL ENFORCEABILITY" MEAN?

Legal enforceability means that the individuals whose personal data is being processed (data subjects) must become third-party beneficiaries, either by virtue of the relevant national law or by contractual arrangements between the members of the corporate group. Data subjects should be entitled to enforce compliance with the rules by lodging a complaint before the EU/EEA competent data protection authority **and** before courts in the EU/EEA (see question 8). See document WP 155 with specific frequently asked questions related to the Binding Corporate Rules.

8. TO WHAT RIGHTS SHOULD THE DATA SUBJECTS BE ENTITLED?

The Article 29 Working Party has stated that 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 courts, according to the rules defined by documents WP74, WP108, 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.

The principles which a data subject should be entitled to enforcer 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.

The Article 29 Working Party has indicated that 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)

The scope of third-party beneficiary rights must be clear in the contractual arrangements allowing for them. These rights mirror the rights granted to data subjects by the third-party beneficiary clause provided for in the standard contractual clauses approved by Commission Decision 2001/497/EC (Set I). For more details on these additional principles, please refer to documents WP 153, WP 154 and WP 155.

Information about third party beneficiary rights 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 (WP74). The Article 29 Working Party has stated that when 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, they should be made transparent and easily accessible to any data subject benefiting from those rights. (See WP 155).

9. WHAT SUBSTANTIAL CONTENT PRINCIPLES NEED TO BE PRESENT IN BINDING CORPORATE RULES?

Given the self-regulatory character of binding corporate rules, their content is entirely determined by the organisation that decides to be bound by them. Although there is no official template or set of model rules to be followed, as the whole point of this concept is to create a tailored solution for a corporation, the Article 29 Working Party has published a Working document setting up a framework for the structure of Binding Corporate Rules in order to help the companies in the drafting of their BCR (WP154). In any case, in addition to the procedural principles (see question 10) binding corporate rules must at least address the so-called "content principles", set out by the Article 29 Working Party in Working Paper WP 12 on transfers of personal data to third countries, namely:

- **The purpose limitation principle**. Data must be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the original purpose. The only exemptions permitted should be in line with Article 13 of the Data Protection Directive.

- **The data quality and proportionality principle**. 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 it is used.

- **The transparency principle**. Individuals must be provided with information as to the purpose of the processing and the identity of the controller, and any other information that is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive.

- **The security principle**. Technical and organisational security measures must be taken by the controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

- **The rights of access, rectification and opposition**. Individuals must have a right to obtain a copy of all data relating to them, and a right to rectification of such data where it

is shown to be inaccurate. In certain situations, individuals must also be able to object to the processing of their personal data (see also question 8). The only exemptions permitted should be in line with Article 13 of the Data Protection Directive.

- **Restrictions on onward transfers**. Further transfers of the personal data by the recipient of the original data transfer must only be permitted where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.

These principles need to be developed and detailed (see question 11) 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. Furthermore, in some cases these principles would need to be supplemented with additional principles relating to sensitive personal data, direct marketing and automated decisions. For more details on these additional principles, please refer to the "*Working Document on Binding Corporate Rules for International Data Transfer*" (WP 74), which is available here. For a global view of all the principles that BCR should contain see documents WP 153 and WP154.

10. WHAT PROCEDURAL PRINCIPLES NEED TO BE PRESENT IN BINDING CORPORATE RULES?

In addition to the rules dealing with substantial data protection principles, any binding corporate rules for international data transfers must also contain the following principles developed by the Article 29 Working Party in Working Paper WP 12 on transfers of personal data to third countries:

- **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 applicant corporate group must also be able to demonstrate that its internal policy is known, understood and effectively applied throughout the group by its employees, who have 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.

- **Audits**. The binding corporate 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. 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 cooperation with the data protection authority.

- **Complaint handling**. The binding corporate 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 enjoy an appropriate level of independence in the exercise of their duties.

- **The duty of cooperation with data protection authorities**. The binding corporate rules must contain clear duties of cooperation with data protection authorities so that

individuals can benefit from sufficient institutional support. There must be an unambiguous undertaking that the corporate group as a whole and any of its members separately will accept audits carried out by supervisory authority inspectors themselves or by independent auditors on behalf of the supervisory authority. 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.

- **Liability**. The binding corporate rules should indicate that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the binding corporate rules is entitled to receive compensation from the controller for the damage suffered. In addition to this general right, the rules must also contain provisions on liability and jurisdiction aimed at facilitating its practical exercise. 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 for any damages resulting from violation of the binding corporate rules by any member bound by the rules.

  The corporate group will attach to its request for 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 cover 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.

  Moreover, BCRs must state that the entity that has accepted liability will also have the burden of proof to demonstrate that the member of the group outside the EU is not liable for any violation of the binding corporate rules which has resulted in the data subject claiming damages. 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.

- **Rule on jurisdiction**. The corporate group must accept that data subjects would be entitled to take action against the corporate group, as well as to choose the jurisdiction:
  (a) either the jurisdiction of the member that has originated the transfer, or
  (b) the jurisdiction of the European headquarters or that of the European member with delegated data protection responsibilities.

- **Transparency**. Corporate groups 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 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. For more details you may refer to documents of the Article 29 Working Party WP153 and WP154.

11. How can binding corporate rules be recognised as providing sufficient safeguards for cross-border data flows?

In all EU/EEA Member States it is a legal requirement that binding corporate rules are submitted to the local data protection authority for approval. The current system requires companies to submit binding corporate rules to the local data protection authority in each EU/EEA Member State from which they intend to transfer data.

In order to facilitate the proceedings, corporate groups interested in a licence for similar types of data export from several Member States may make use of a **coordinated** procedure. Such a procedure has been developed by the Article 29 Working Party. The paper entitled "*Working Document Setting Forth a Cooperation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules*" (WP 107) is available here. The main idea behind these procedural arrangements is to allow companies to go through one process of application for authorisation via the data protection authority of one Member State (leading coordinator authority) that will, through the coordination process between the data protection authorities involved, lead to the granting of the required authorisations, in accordance with the respective national laws, by all the different data protection authorities of the Member States where this company operates. The coordination procedure is not a system of mutual recognition of the authorisation granted by the leading coordinator data protection authority which would bind all the other national data protection authorities involved in the process. Several data protection authorities of EU/EEA countries have recently agreed on recognising the decision given by the leading coordinator data protection authority stating that the binding corporate rules presented by an international corporation meet all the safeguards required. This recognition is aimed at facilitating the subsequent local approval process of the BCR by the authorities concerned, according to the procedural obligations set by the national law. National data protection authorities working on it.

The Article 29 Working Party has also established a Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP 133). The purpose of this standard form is to help companies demonstrate how they meet the requirements laid down in documents WP 74 and 108. The Article 29 Working Party has also adopted documents *setting up a framework for the structure of Binding Corporate Rules* (WP 154), a *table with the elements and principles to be found in Binding Corporate Rules* (WP 153) as well a document with specific questions related to the binding corporate rules (WP 155)

12. To which data protection authority should you apply to for approval of your binding corporate rules?

A corporate group interested in submitting draft binding corporate rules for the approval of several data protection authorities should propose a data protection authority as the **lead authority** for the cooperation procedure. The factors to be taken into account in order to determine the lead data protection authority are set out in the Article 29 Working Party's Working Document "*establishing a Model Checklist Application for Approval of Binding Corporate Rules (WP 108)*" (available here):

- If the ultimate parent or operational headquarters of the corporate group is a company incorporated in a Member State of the EU, you should apply to the data protection authority of that Member State.

- If it is not clear where the ultimate parent or operational headquarters of the corporate 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 following criteria: the location of the group's European headquarters, the location of the company within the group 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; the place where most decisions in terms of the purposes and the means of the processing are taken; and the Member States within the EU from which most transfers outside the EEA will take place. Priority is given to the location of the group's European headquarters.

13. WHO MUST SUBMIT THE APPLICATION?

Any application for approval of binding corporate rules must be made by the entity in the Member State in which the headquarters of the organisation is located. Where the head office of an organisation is located outside the EU, these "data protection responsibilities" must be delegated to a member of the group located within the EU. See question 12.

14. WHAT INFORMATION IS REQUIRED FOR YOUR APPLICATION?

In order to facilitate the application, the Article 29 Working Party has developed a Working Document WP 153 that gives a quick overview of the required content for BCRs with references to Documents WP 74 and 108. This Document called *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*" is available here.
Moreover in order to have a view on a possible structure of a BCR, it is suggested to consult the Working Document of the Article 29 Working Part *setting up a framework for the structure of Binding Corporate Rules"* (WP 154).
A Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data has also been developed by the Article 29 Working Party (WP 133) (click here).

The Article 29 Working Party recommends that in order to facilitate the review of BCRs by Data Protection Authorities and at the same time make BCRs more transparent for data subjects, BCRs would be established in a single 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).

The applicant is recommended to use the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data has also been developed by the Article 29 Working Party (WP 133) in order to help an organisation in the submission of its Binding Corporate Rules to national data protection authorities. (click here)

For more detailed information please refer to the Article 29 Working Party document with specific frequently asked questions related to the binding corporate rules (WP 155).

D. Frequently Asked Questions: derogations

Article 26(1) of the Directive states that transfers of personal data to a third country that does not ensure an adequate level of protection may take place if one of the following conditions is met:

> (a) the data subject has unambiguously given his consent to the proposed transfer;
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
> (e) the transfer is necessary in order to protect the vital interests of the data subject;
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

1. WHEN CAN A COMPANY RELY ON ONE OF THESE DEROGATIONS TO TRANSFER DATA TO A THIRD COUNTRY THAT DOES NOT ENSURE AN ADEQUATE LEVEL OF PROTECTION?

The Article 29 Working Party has issued a working document providing guidance as to how the derogations in Article 26(1) of the Data Protection Directive should be understood and applied by data controllers intending to initiate data transfers to countries that do not ensure an adequate level of protection. The paper entitled "*Working document on a common interpretation of Article 26(1) of the Data Protection Directive of 24 October 1995*" is available here. The Article 29 Working Party recommends that the derogations in Article 26(1) of the Directive should be interpreted restrictively and preferably be applied to cases in which it would be genuinely inappropriate, or even impossible, for the transfer to take place on the basis of Article 26(2), i.e., providing adequate safeguards through, for example, (the standard) contractual clauses or binding corporate rules. Only if this is truly not practical and/or feasible should the data controller consider using the derogations in Article 26(1).

This is the case in particular for transfers of personal data that might be described as repeated, mass or structural. These transfers should, where possible, and precisely because of their importance, be carried out within a specific legal framework (Article 25 or 26(2)). Only for instance when recourse to such a legal framework is impossible in practice can these mass or repeated transfers be legitimately carried out on the basis of Article 26(1).

Consequently, when two or more solutions can be applied to a particular case, the following order should be respected:

1. the transfer may occur because the third country offers an adequate level of protection and the European Commission has recognised this in one of its decisions;

2. the transfer has been authorised on a case-by-case basis by the national data protection authority, because the data controller offers "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". These safeguards may, in particular, result from the following:

    a. one set of the existing standard contractual clauses has been included in the contract with the data importer. In some Member States, an additional authorisation of the national data protection authority is still needed;
    b. other adequate safeguards have been adopted by the data controller (e.g. self-drafted contractual clauses) and authorised by the national data protection authority;
    c. for multinationals, binding corporate rules have been adopted and the transfer occurs between companies belonging to the same multinational.

3. the transfer falls under one of the derogations laid down in Article 26(1) of the Data Protection Directive.

2. WHICH LEGAL REQUIREMENTS SHOULD A COMPANY MEET WHEN RELYING ON ONE OF THESE DEROGATIONS?

When transferring data to a third country on the basis of one of the derogations in Article 26(1), a company needs to respect all the other relevant provisions of the Directive, and in particular those relating to sensitive data (Article 8), fair and lawful processing and compatible use (Article 6). For more details, see here.

3. WHEN MAY A TRANSFER OF PERSONAL DATA OCCUR ON THE BASIS THAT THE DATA SUBJECT HAS UNAMBIGUOUSLY GIVEN HIS CONSENT TO THE PROPOSED TRANSFER (DEROGATION 1(A))?

Article 26(1)(a) states that a transfer of personal data may be made to a country that does not ensure an adequate level of protection on condition that "the data subject has given his consent unambiguously to the proposed transfer".

To be valid, this consent, whatever the circumstances in which it is given, must be *a freely given, specific and informed indication of the data subject's wishes*, as defined in Article 2(h) of the Directive.

- **Consent must be a clear and unambiguous indication of wishes**. The importance of consent constituting a positive act excludes *de facto* any system whereby the data subject would have the right to oppose the transfer only *after* it has taken place: specific consent to a transfer must genuinely be required for the transfer to take place. Any doubt as to whether consent has really been given would make the derogation inapplicable. This is likely to mean that many situations where consent is implied (for example because an individual has been made aware of a transfer and has not objected) would not qualify for this exemption.

- **Consent must be given freely**. Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered to be valid. Specific difficulties might occur in considering a data subject's consent to be freely given in an employment context, due to the relationship of subordination between employer and employee. Valid consent in such a context means that the employee must have a real opportunity to withhold his consent without suffering any harm, or to withdraw it subsequently if he changes his mind. In such situations of hierarchical dependence, an employee's refusal or reservations about a transfer might indeed cause him non-material or material harm, which is completely contrary to the letter and spirit of European personal data protection legislation. In this light, the Article 29 Working Party recommends employers not to rely solely on their employees' consent when transferring their data, apart from in cases in which it is established that employees would not suffer any consequences if they wished not to give their consent to a transfer, or if they did give their consent but subsequently wished to withdraw their consent, in cases where this would be possible.

- **Consent must be specific**. To constitute a valid legal basis for a possible transfer of data, the data subject's consent must be *specifically given* for the particular transfer or category of transfers in question. Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer, e.g. if the occurrence and specific

circumstances of a transfer are not known at the time consent is requested and so the impact on the data subject cannot be assessed. To cite an example, a company, when obtaining its customers' data for a specific purpose, cannot ask them to give their prior consent to the transfer of their data to a third country in the event of the company being taken over by another company. However, it is possible to envisage that a person may validly consent to the transfer of his data to a third country in advance, when the details of the transfer are already predetermined, notably in terms of purpose and categories of recipients.

- Consent must be informed. This condition is particularly important. It requires the data subject to be properly informed in advance of the specific circumstances of the transfer (its purpose, the identity and details of the recipient(s), etc.) in accordance with the general principle of fairness. The information given to data subjects must also include the specific risk resulting from the fact that their data will be transferred to a country that does not provide adequate protection. Only this information will enable the data subject to consent with full knowledge of the facts; if it is not supplied, the derogation will not apply.

4. WHEN MAY THE DATA TRANSFER OCCUR ON THE BASIS THAT THE TRANSFER IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT BETWEEN THE DATA SUBJECT AND THE CONTROLLER OR THE IMPLEMENTATION OF PRECONTRACTUAL MEASURES TAKEN IN RESPONSE TO THE DATA SUBJECT'S REQUEST?

In order to fall within this derogation it is necessary to show that the transfer is *necessary* for the performance or conclusion of the contract. The Article 29 Working Party stresses that this "necessity test" here requires a close and substantial connection between the data subject and the purposes of the contract (WP 114).

This could be for instance the transfer by travel agents of personal data concerning their individual clients to hotels or other commercial partners that would be involved in the organisation of these clients' stay or the transfer of personal data necessary for a credit card payment by the data subject in a third country.

Certain international groups would like to be able to avail themselves of this derogation in order to transfer data on their employees from a subsidiary to the parent company, for example in order to centralise the group's payment and human resources management functions. They believe that such transfers could be deemed necessary for performance of the employment contract concluded between the employee and the data controller. In this regard the Article 29 Working Party, in its working document interpreting Article 26(1), considers that such an interpretation is excessive since it is highly questionable whether the concept of an employment contract can be interpreted so broadly, as there is no direct and objective link between performance of an employment contract and such a transfer of data (WP 114).

Finally, this derogation cannot be applied to transfers of additional information not necessary for the purpose of the transfer, or transfers for a purpose other than the performance of the contract; for additional data, other means of adducing adequacy should be used.

5. WHEN MAY A COMPANY CONSIDER THAT THE TRANSFER IS NECESSARY FOR THE CONCLUSION OR PERFORMANCE OF A CONTRACT CONCLUDED IN THE INTEREST OF THE DATA SUBJECT BETWEEN THE CONTROLLER (THE COMPANY) AND A THIRD PARTY?

The interpretation of this derogation is necessarily similar to the preceding one, namely that a transfer of data to a third country which does not ensure adequate protection cannot be deemed to fall within the derogation unless it can be considered to be truly "necessary for the conclusion or performance of a contract between the data controller and a third party, in the interest of the data subject", and pass the corresponding "necessity test".

In the present case, the Article 29 Working Party stresses that this test requires a *close and substantial connection between the data subject's interest and the purposes of the contract.*

Some data controllers have sometimes expressed the wish to have recourse to this derogation as a basis for international data transfers concerning their employees to providers, established outside the EU, to which they outsource their payroll management. According to them, such transfers would be necessary for the performance of their outsourcing contract, and would be in the interest of the data subject since the purpose of the transfer is the management of the employee's pay. In this case, however, the Article 29 Working Party is of the opinion that a close and substantial link between the data subject's interest and the purposes of the contract is not established, and that the derogation cannot apply.

Also, certain international groups would like to be able to apply this derogation when managing stock option schemes for certain categories of their employees. To do this, these groups classically use the services of financial service providers, specialising in the management of such schemes, established in third countries. The groups allege that transfers could thus be made to such a service provider for the purpose of performing the contract concluded between the provider and the data controller, in the interest of the beneficiaries of the scheme. The Article 29 Working Party, in its working document on Article 26(1), points out that the data controller would have to satisfy a data protection authority that the data transferred is necessary for the performance of that contract.

6. WHEN MAY A COMPANY ASSUME THAT THE TRANSFER IS NECESSARY OR LEGALLY REQUIRED ON IMPORTANT PUBLIC INTEREST GROUNDS, OR FOR THE ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS?

This derogation must be interpreted using the same strict criterion as that applied for the previous derogations. Hence, a transfer of data to a third country that does not ensure an adequate level of protection cannot be deemed to fall within this derogation unless it can be considered to be really "necessary" or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims in accordance with the strict interpretation of "necessary" referred to above.
Recital 58 of the Data Protection Directive refers by way of example to transfers between tax authorities or bodies responsible for social security.

The Article 29 Working Party has already stressed that the concept of "important public interest grounds" must be interpreted strictly. Only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in

this connection. It is not acceptable for a unilateral decision taken by a third country, on public interest grounds specific to it, to lead to regular bulk transfers of data protected by the Data Protection Directive. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Data Protection Directive.

The Article 29 Working Party emphasises that the concept of "establishment, safeguarding or defence of legal claims" must here again be subject to strict interpretation. Thus, for example, the parent company of a multinational group, established in a third country might be sued by an employee of the group currently posted to one of its European subsidiaries. The derogation in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defence. In any event, this derogation cannot be used to justify the transfer of all the employee files to the group's parent company on the ground of the possibility that such legal proceedings might be brought one day. In addition, this derogation can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably those deriving from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" Convention) and of 25 October 1980 ("Access to Justice" Convention).

7. WHEN MAY A COMPANY CONSIDER THAT THE TRANSFER IS NECESSARY IN ORDER TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT?

The derogation in Article 26(1)(e) obviously applies when data are transferred in the event of a medical emergency, where they are considered to be directly necessary in order to give the medical care required.

Thus, for example, it must be legally possible to transfer data (including certain personal data) to a third country where, in the course of a tourist journey, the data subject becomes ill or suffers an accident and needs urgent medical care, and only his usual doctor, established in an EU country, is able to supply these data.

The transfer must relate to the individual interest of the data subject and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, the Article 29 Working Party is of the opinion that this derogation could not be used to justify transferring personal medical data to persons responsible for treatment and established outside the EU if their purpose is not to treat the particular case of the data subject but, for example, to carry out general medical research that will not yield results until some time in the future. In these cases, alternative solutions such as binding corporate rules or standard contractual clauses must be used. The Article 29 Working Party has followed this interpretative line in its Working Document on the processing of personal data relating to health in electronic health records (EHR) (WP 131).

8. WHEN IS THE FOLLOWING DEROGATION FULFILLED: THE TRANSFER IS MADE FROM A REGISTER WHICH ACCORDING TO LAWS OR REGULATIONS IS INTENDED TO PROVIDE INFORMATION TO THE PUBLIC AND WHICH IS OPEN TO CONSULTATION EITHER BY THE PUBLIC IN GENERAL OR BY ANY PERSON WHO CAN DEMONSTRATE LEGITIMATE INTEREST, TO THE EXTENT THAT THE CONDITIONS LAID DOWN IN LAW FOR CONSULTATION ARE FULFILLED IN THE PARTICULAR CASE?

This derogation concerns transfers "*from a public register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case*".

This provision of the Data Protection Directive is a logical consequence of the open nature of the registers referred to, which can be freely consulted. If such a register can be consulted by anyone in the country or by any person with a legitimate interest in doing so, it seems logical to allow it to be consulted by a person established in a third country if any conditions to which the register is subject are complied with.

However, this freedom to transfer data cannot be total. Recital 58 of the Data Protection Directive states that "*in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register*". It would not be in keeping with the spirit of the derogation if this legal ground for transfer were used to empty such registers of their content, with the risk that their use by entities established in third countries could ultimately lead them to be used for purposes other than that for which they were originally set up.

Furthermore, reference will have to be made to the laws and regulations of the EU Member State in which the register was set up in order to verify whether this derogation can apply in certain specific cases. In particular, these laws and regulations will define the concepts of "*intended to provide information to the public*" and "*legitimate interest*" on the basis of which the derogation might be used.

9. WHOM MAY I CONTACT FOR CLARIFICATION?

For specific questions relating to the interpretation of one of the aforementioned derogations you are invited to contact your national data protection authority. For a list of the Member States' national data protection authorities and their contact details, please click here.