EUROPEAN COMMISSION
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

DG XV D/5025/98
WP 12

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

Working Document

Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive

Adopted by the Working Party on 24 July 1998

Table of contents

Introduction

This document seeks to bring together the previous work done by the Working Party of EU Data Protection Commissioners established under Article 29 of the Data Protection Directive[1] into a more comprehensive set of views covering all the central questions raised by flows of personal data to third countries in the context of the application of EU data protection directive (95/46/EC). It is organised according to the system provided for international transfers of personal data set out in Articles 25 and 26 of the directive. (The text of these articles is attached as Annex 2)

Article 25, paragraph (1), sets out the principle that Member States shall only allow a transfer to take place if the third country in question ensures an adequate level of protection. Paragraph (2) explains that 'adequacy' should be assessed on a case by case basis 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'. Paragraph (6) provides that the Commission may determine that certain countries offer adequate protection. **Chapter One** of this paper deals with this central question of adequate protection. It seeks to explain what is meant by 'adequate' and outlines a framework for how the adequacy of protection should be assessed in a particular case.

The application of this approach is further dealt with in Chapters Two and Three. **Chapter Two** deals with transfers to countries that have ratified the Council of Europe Convention 108, while **Chapter Three** assesses the issues surrounding transfers where the protection of personal data is provided for mainly or entirely by self-regulatory mechanisms and not by rules of law..

Where there is an absence of adequate protection in the sense of Article 25 (2), the directive also envisages in Article 26(2) the possibility of *ad hoc* measures, notably of a contractual nature, which could result in the establishment of adequate safeguards on the basis of which the transfer in question could proceed. In **Chapter Four** of this paper the circumstances in which *ad hoc* contractual solutions may be appropriate are examined and some recommendations as to the possible form and content of such solutions are set out.

Chapter Five deals with the third and final situation envisaged by the directive: those limited sets of cases contained in Article 26(1) where there is effectively an exemption to the requirement of 'adequate protection'. The precise scope of these exemptions is

[1]See **WP 4 (5020/97)** " First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy", a discussion document adopted by the Working Party on 26 June 1997;
WP 7 (5057/97) Working document: "Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?", adopted by the Working Party on 14 January 1998;
WP 9 (5005/98) Working Document: "Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries", adopted by the Working Party on 22 April 1998.

examined, with illustrative examples of the kinds of cases that might be covered together with those that would seem not to be.

Finally **Chapter Six** contains some comments on procedural matters arising in connection with the making of judgements on the adequacy (or non-adequacy) of protection and the achieving of a coherent Community-wide approach to these questions.

Attached as annex 1 are a series of illustrative case studies which seek to demonstrate how the approach set out in this document might apply in practice.

CHAPTER ONE: ASSESSING WHETHER PROTECTION IS ADEQUATE

(1) What constitutes 'adequate protection'?

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and obligations on those who process data, or who exercise control over such processing. The obligations and rights set down in directive 95/46/EC build upon those set down in Council of Europe Convention N°108 (1981), which in turn are not dissimilar from those included in the OECD guidelines (1980) or the UN guidelines (1990). It would therefore appear that there is a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the Community.

However, data protection rules only contribute to the protection of individuals if they are followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country, but also the system in place to ensure the effectiveness of such rules. In Europe, the tendency historically has been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress. Furthermore such laws have generally included additional procedural mechanisms, such as the establishment of supervisory authorities with monitoring and complaint investigation functions. These procedural aspects are reflected in directive 95/46/EC, with its provisions on liabilities, sanctions, remedies, supervisory authorities and notification. Outside the Community it is less common to find such procedural means for ensuring compliance with data protection rules. Parties to Convention 108 are required to embody the principles of data protection in law, but there is no requirement for additional mechanisms such as a supervisory authority. The OECD guidelines carry only the requirement that they be 'taken into account' in domestic legislationand provide for no procedural means to ensure that the guidelines actually result in effective protection for individuals. The later UN guidelines, on the other hand, do include provisions on supervision and sanctions, which reflects a growing realisation worldwide of the need to see data protection rules properly enforced.

Against this background it is clear that any meaningful analysis of adequate protection must comprise the two basic elements : the content of the rules applicable and the means for ensuring their effective application.

Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements. The degree of risk that the transfer poses to the data subject will be an important factor in determining the precise requirements of a particular case. Despite this proviso, the compilation of a basic list of minimum conditions is a useful starting point for any analysis.

(i) Content Principles

The basic principles to be included are the following:

1) **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.[2]

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

3) **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)[3] and 13 of the directive.

4) **the security principle -** technical and organisational security measures should be taken by the data 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.

5) **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

6) restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive (These exemptions are examined in Chapter Five.)

Examples of additional principles to be applied to specific types of processing are:

---

[2] Article 13 permits a restriction to the 'purpose principle' if such a restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest, or the protection of the data subject or the rights and freedoms of others.

[3] Article 11(2) stipulates that when data are collected from some-one other than the data subject, information need not be provided to the data subject if this proves impossible, involves a disproportionate effort, or if the recording or disclosure of the data is expressly required by law.

1) **sensitive data -** where 'sensitive' categories of data are involved (those listed in article 8 of the directive[4]), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

2) **direct marketing -** where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

3) **automated individual decision -** where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

(ii) Procedural/ Enforcement Mechanisms

In Europe there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system. Elsewhere in the world, however, these features are not always present.
To provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

The objectives of a data protection system are essentially threefold:

1) to deliver a **good level of compliance** with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

2) to provide **support and help to individual data subjects** in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

3) to provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

[4] 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.

CHAPTER TWO: APPLYING THE APPROACH TO COUNTRIES THAT HAVE RATIFIED COUNCIL OF EUROPE CONVENTION 108

Convention 108 is the only existing international instrument with binding force in the data protection field apart from the directive. Most of the parties to the Convention are also Member States of the European Union (all 15 have now ratified it) or countries, such as Norway and Iceland, which may in any case be bound by the directive by virtue of the European Economic Area agreement. However, Slovenia, Hungary and Switzerland have also ratified the Convention, and other third countries are likely do so in the future, particularly given that the Convention is also open to non Council of Europe countries. It is therefore of more than purely academic interest to examine whether countries that have ratified the Convention can be considered to afford an adequate level of protection in the sense of Article 25 of the directive.

As a starting point it is useful to examine the text of the Convention itself in the light of the theoretical outline of 'adequate protection' set out in Chapter One of this document.

As regards the content of the basic principles, the Convention could be said to include the first five of the six 'minimum conditions'. [5] The Convention also includes the requirement for appropriate safeguards for sensitive data which should be a requirement for adequacy whenever such data are involved.

A missing element of the Convention in terms of the content of its substantive rules is the absence of restrictions on transfers to countries not party to it. This creates the risk that a Convention 108 country could be used as a 'staging post' in a data transfer from the Community to a further third country with entirely inadequate protection levels.

The second aspect of 'adequate protection' concerns the procedural mechanisms in place to ensure that the basic principles are rendered effective. The Convention requires its principles to be embodied in domestic law and that appropriate sanctions and remedies for violations of these principles be established. This should be sufficient to ensure a reasonable level of compliance with the rules and appropriate redress to data subjects where the rules are not complied with (objectives (1) and (3) of a data protection compliance system). However, the Convention does not oblige contracting parties to establish institutional mechanisms allowing the independent investigation of complaints, although in practice ratifying countries have generally done so. This is a weakness in that without such institutional mechanisms appropriate support and help to individual data subjects in the exercise of their rights (objective (2)) may not be guaranteed.

[5] There may be some doubts about the 'transparency principle'. Article 8 (a) of the Convention may not equate to the *active* duty to provide information which is the essence of Articles 10 and 11 of the directive. Furthermore the Convention includes no specific 'opt-out' rights where data are used for direct marketing purposes nor any provisions on automated individual decisions (profiling).

This brief analysis seems to indicate that most transfers of personal data to countries that have ratified Convention 108 could be presumed to be allowable under Article 25(1) of the directive provided that

- the country in question also has appropriate mechanisms to ensure compliance, help individuals and provide redress (such as an independent supervisory authority with appropriate powers); and
- the country in question is the final destination of the transfer and not an intermediary country through which the data are transiting, except where onward transfer is back into the EU or to another destination offering adequate protection. [6]

Of course this is a rather simplified and superficial examination of the Convention. Specific cases of data transfers to Convention countries may raise new problems not considered here.

[6] Convention 108 is currently being re-examined, a process which may result in changes which address these and other difficulties.

CHAPTER THREE: APPLYING THE APPROACH TO INDUSTRY SELF-REGULATION

Introduction

Article 25(2) of the data protection directive (95/46/EC) requires the level of protection afforded by a third country to be assessed in the light of *all the circumstances* surrounding a data transfer operation or set of such operations. Specific reference is made not only to rules of law but also to "professional rules and security measures which are complied with in that country."

The text of the directive therefore requires that account be taken of non-legal rules that may be in force in the third country in question, provided that these rules *are complied with*. It is in this context that the role of industry self-regulation must be considered.

What is self-regulation?

The term "self-regulation" can mean different things to different people. For the purpose of this document, self-regulatory code (or other instrument) should be taken to mean any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned.

This is a broad definition which would encompass, at one end of the scale, a voluntary data protection code developed by a small industry association with only a few members, to at the other end, the kind of detailed codes of professional ethics applicable to entire professions, such as doctors and bankers, which often have quasi-judicial force.

Is the body responsible for the code representative of the sector?

As this chapter will go on to argue, one important criterion for judging the value of a code is the degree to which its rules can be enforced. In this context, the question of whether the association or body responsible for the code represents all the operators in a sector or only a small percentage of them, is probably less important than the strength of the association in terms of its ability to, for example, impose sanctions on its members for non-compliance with the code. However, there are several secondary reasons which render industry-wide or profession-wide codes with clearly comprehensive coverage more useful instruments of protection than those developed by small groupings of companies within sectors. First is the fact that, from the consumer's point of view, an industry that is fragmented and characterised by several rival associations, each with its own data protection code, is confusing. The co-existence of several different codes creates an overall picture which lacks transparency for the data subject. The second point is that, particularly in industries such as direct marketing, where personal data is routinely passed between different companies of the same sector, situations can arise where the company disclosing personal data is not subject to the same data protection code as the company that receives it. This is a source of uncertainty as to the rules applicable, and it might also render more difficult the investigation and resolution of complaints from individual data subjects.

Evaluating self-regulation - the approach to take

Given the wide variety of instruments which fall within the notion of self-regulation, it is clear that there is a need to differentiate between the various forms of self-regulation in terms of their real impact on the level of data protection applicable when personal data are transferred to a third country.

The starting point for the evaluation of any specific set of data protection rules (whether categorised as self-regulation or regulation) must be the general approach set down in Chapter One of this document. The cornerstone of this approach is an examination not only of the content of the instrument (it should contain a series of core principles) but also of its effectiveness in achieving:

- a good level of general compliance,
- support and help to individual data subjects,
- and, crucially, appropriate redress (including compensation where appropriate).

Evaluating the content of a self-regulatory instrument

This is a relatively easy task. It is a question of ensuring that the necessary 'content principles' set out in Chapter One are present. This is an objective evaluation. It is a question of what the code contains, and not how it was developed. The fact that an industry or profession has itself played the major role in developing the content of the code is not in itself relevant, although clearly if the opinions of data subjects and consumer organisations have been taken into account during its development, it is more likely that the code will reflect more closely the core data protection principles which are required.

The transparency of the code is a crucial element; in particular, the code should be drafted in plain language and offer concrete examples, which illustrate its provisions.

Furthermore, the code should prohibit the disclosure of data to non-member companies who are not governed by the code, unless other adequate safeguards are provided.

Evaluating the effectiveness of a self-regulatory instrument

Assessing the effectiveness of a particular self-regulatory code or instrument is a more difficult exercise, which requires an understanding of the ways and means by which adherence to the code is ensured and problems of non-compliance dealt with. The three functional criteria for judging the effectiveness of protection must all be met if a self-regulatory code is to be considered as providing adequate protection.

Good level of compliance

An industry or professional code will typically be developed by a representative body of the industry or profession concerned, and it will then apply to members of that particular representative body. The level of compliance with the code is likely to depend on the degree of awareness of the code's existence and of its content among members, on the steps taken to ensure transparency of the code to consumers in order to allow the market forces to make an effective contribution, on the existence of a

system of external verification (such as a requirement for an audit of compliance at regular intervals) and, perhaps most crucially, on the nature and enforcement of the sanction in cases of non-compliance

Important questions are therefore:

- what efforts does the representative body make to ensure that its members are aware of the code?
- does the representative body require evidence from its members that it has put the provisions of the code into practice? How often?
- is such evidence provided by the member company itself or does it come from an external source (such as an accredited auditor)?
- does the representative body investigate alleged or suspected breaches of the code?
- is compliance with the code a condition of membership of the representative body or is compliance purely "voluntary"?
- where a member has been shown to breach the code, what forms of disciplinary sanction are available to the representative body (expulsion or other) ?
- is it possible for an individual or company to continue working in the particular profession or industry, even after expulsion from the representative body?
- is compliance with the code enforceable in other ways, for example by way of the courts or a specialist tribunal? Professional codes of ethics have legal force in some countries. It might also be possible in some circumstances to use general laws relating to fair trading practice or even competition to enforce industry codes.

When examining the types of sanction in place, it is important to distinguish between a "remedial" sanction which simply requires a data controller, in a case of non-compliance, to change its practices so as to bring them into line with the code, and a sanction which goes further by actually punishing the controller for its failure to comply. It is only this second category of "punitive" sanction which actually has an effect on the future behaviour of data controllers by providing some incentive to comply with the code on an ongoing basis.

The absence of genuinely dissuasive and punitive sanctions is therefore a major weakness in a code. Without such sanctions it is difficult to see how a good level of overall compliance could be achieved, unless a rigorous system of external verification (such as a public or private authority competent to intervene in case of non compliance with the code, or a compulsory requirement for external audit at regular intervals) were put in place.

Support and help to individual data subjects

A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his/her personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed. This institutional support should ideally be impartial, independent and equipped with the necessary powers to investigate any complaint from a data subject. Relevant questions for self-regulation in this regard are:

- is there a system in place allowing for investigation of complaints from individual data subjects?

- how are data subjects made aware of this system and of the decisions taken in individual cases?

- are there any costs involved for the data subject?

- who carries out the investigation? Do they have the necessary powers?

- who adjudicates on an alleged breach of the code? Are they independent and impartial?

The impartiality of the arbiter or adjudicator in any alleged breach of a code is a key point. Clearly such a person or body must be independent in relation to the data controller. However, this in itself is not sufficient to ensure impartiality. Ideally the arbiter should also come from outside the profession or sector concerned, the reason being that fellow members of a profession or sector have a clear commonality of interests with the data controller alleged to have breached the code. Failing this the neutrality of the adjudicating body could be ensured by including consumer representatives (in equal numbers) alongside the industry representatives.

Appropriate Redress

If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject. This remedy must put right the problem (e.g. correct or delete any inaccurate data, ensure that processing for incompatible purposes ceases) and, if damage to the data subject has resulted, allow for the payment of appropriate compensation. It should be borne in mind that "damage" in the sense of the data protection directive includes not only physical damage and financial loss, but also any psychological or moral harm caused (known as "distress" under UK and US law).

Many of the questions regarding sanctions listed above in the section "Good level of compliance" are relevant here. As explained earlier sanctions have a dual function: to punish the offender (and thus encourage compliance with the rules by the offender and by others), and to remedy a breach of the rules. Here we are primarily concerned with the second of these functions. Additional questions would therefore include:

- is it possible to verify that a member who has been shown to contravene the code has changed his practices and put the problem right?

- can individuals obtain compensation under the code, and how?

- is the breach of the code equivalent to a breach of contract, or enforceable under public law (e.g. consumer protection, unfair competition), and can the competent jurisdiction award damages on this basis?

Conclusions

- Self-regulation should be evaluated using the objective and functional approach set out in Chapter One.
- For a self-regulatory instrument to be considered as a valid ingredient of "adequate protection" it must be binding on all the members to whom personal data are

transferred and provide for adequate safeguards if data are passed on to non-members.

- The instrument must be transparent and include the basic content of all core data protection principles.
- The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another.
- The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.
- The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

CHAPTER FOUR : THE ROLE OF CONTRACTUAL PROVISIONS

1. Introduction

The data protection directive (95/46/EC) establishes the principle in Article 25(1) that transfers of personal data to third countries should only take place where the third country in question ensures an adequate level of protection. The purpose of this Chapter is to examine the possibility for exemption from the 'adequate protection' principle of Article 25 set out in Article 26(2). This provision allows a Member State to authorize a transfer or set of transfers to a 'non-adequate' third country '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'. The provision goes on to specify that 'such safeguards may in particular result from contractual clauses'. Article 26(4) also gives a power to the Commission, acting in accordance with the procedure laid down in Article 31, to decide that certain standard contractual clauses offer the sufficient guarantees envisaged in Article 26(2).

The idea of using contracts as a means of regulating international transfers of personal data was not of course invented by the directive. As long ago as 1992 the Council of Europe, the International Chamber of Commerce and the European Commission were jointly responsible for a study on the issue.[7] More recently an increasing number of experts and commentators, perhaps noticing the explicit reference in the directive, have made comments on the use of contracts in studies and articles. Contracts have also continued to be used in the 'real world', as a means of dealing with data protection problems arising from the export of personal data from certain EU Member States. They have been widely used in France since the late 1980s. In Germany the recent example of the 'Bahncard' case involving Citibank received a considerable amount of publicity.[8]

2. The use of contracts as a basis for intra-Community flows of data

Before examining the requirements of contractual provisions in the context of data flows to third countries, it is important to clarify the difference between the third country situation and that pertaining within the Community. In this latter case, the contract is the mechanism used to define and regulate the split of data protection responsibilities when more than one entity is involved in the data processing in question. Under the directive one entity, the 'data controller', must take the principal

[7] 'Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum', study made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce, Strasbourg 2 November 1992

[8] See the presentation of Alexander Dix of this case at the International Data Protection and Privacy Commissioners' Conference, September 1996, Ottawa.

responsibility for complying with the substantive data protection principles. The second entity, the 'processor', is responsible only for data security. An entity is deemed to be a controller if it has the decision-making power over the purposes and means of the data processing, whereas the processor is simply the body that physically provides the data processing service. The relationship between the two is regulated by Article 17(3) of the directive, which stipulates that:

> *the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
> *- the processor shall act only on instructions from the controller*
> *- the obligations set out in Paragraph 1 (the substantive provisions regarding data security), as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.*

This elaborates on the general principle established under Article 16 that any person acting under the authority of the controller, including the processor himself, must not process personal data except on instructions from the controller (unless required to do so by law).

Where personal data are transferred to third countries it will also normally be the case that more than one party will be involved. Here the relationship in question is between the entity transferring the data (the 'transferer') and the entity receiving the data in the third country (the 'recipient'). In this context one purpose of the contract should still be that of determining how the responsibility for data protection compliance is split between the two parties. However, the contract must do much more than this: it must provide additional safeguards for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection.

3. The objective of a contractual solution

In the context of third country transfers, therefore, the contract is a means by which adequate safeguards can be provided by the data controller when transferring data outside of the Community (and thus outside the protection provided by the directive, and indeed by the general framework of Community law[9]) to a third country where the general level of protection is not adequate. For a contractual provision to fulfil this function, it must satisfactorily compensate for the absence of a general level of adequate protection, by including the essential elements of protection which are missing in any given particular situation.

[9] The exercise of an individual's data protection rights is facilitated within the Community by the general legal framework, for example the Strasbourg Agreement (1977) on the transmission of applications for legal aid.

4. The specific requirements of a contractual solution

The starting point for assessing the meaning of 'adequate safeguards', as used in Article 26(2), is the notion of 'adequate protection' already developed at some length in Chapter One. This consists of a series of basic data protection principles together with certain conditions necessary to ensure their effectiveness.

(i) The substantive data protection rules

The first requirement of the contractual solution is, therefore, that it must result in an obligation on the parties to the transfer to ensure that the full set of basic data protection principles set out in Chapter One apply to the processing of the data transferred to the third country. These basic principles are:

- the purpose limitation principle
- the data quality and proportionality principle
- the transparency principle
- the security principle
- the rights of access, rectification and opposition
- restrictions on onward transfers to non-parties to the contract[10]

Furthermore in some situations additional principles relating to sensitive data, direct marketing and automated decisions must be applied.

The contract should set out the detailed way in which the recipient of the data transfer should apply these principles (i.e. purposes should be specified, data categories, time limits for retention, security measures, etc.). In other situations, for example where protection in a third country is provided by a general data protection law similar to the directive, other mechanisms which clarify the way data protection rules apply in practice (codes of conduct, notification, the advisory function of the supervisory authority) are likely to be in place. In a contractual situation this is not so. Detail is therefore imperative where the transfer is based on a contract.

[10] Further transfers of the personal data from the recipient to another third party should not be permitted, unless a means is found of contractually binding the third party in question providing the same data protection guarantees to the data subjects.

(ii) Rendering the substantive rules effective

Chapter One sets out three criteria by which the effectiveness of a data protection system should be judged. These criteria are the ability of the system to:

- to deliver a **good level of compliance** with the rules
- to provide **support and help to individual data subjects** in the exercise of their rights
- and, as a key element, to provide **appropriate redress** to the injured party where rules are not complied with.

The same criteria must apply in judging the effectiveness of a contractual solution. Clearly this is a major though not impossible challenge. It is a question of finding means which can make up for the absence of oversight and enforcement mechanisms, and which can offer help, support and ultimately redress to a the data subject who may not be a party to the contract.

Each of these questions must be examined in detail. For ease of analysis, they are taken in reverse order.

Providing redress to a data subject

Providing a legal remedy to a data subject, (i.e. a right to have a complaint adjudicated by an independent arbiter and to receive compensation where appropriate), by way of a contract between the 'transferer' of the data and the 'recipient' is not a simple question. Much will depend on the nature of the contract law chosen as the national law applicable to the contract. It is expected that the applicable law will generally be that of the Member State in which the transferer is established. The contract law of some Member States permits the creation of third party rights, whereas in other Member States this is not possible.

As a general rule the more the recipient is limited in terms of his freedom to choose the purposes, means and conditions under which he processes the transferred data, the greater will be the legal security for the data subject. Bearing in mind that we are dealing with cases of inadequate general protection, the preferred solution would be for the contract to provide that the recipient of the transfer has no autonomous decision-making power in respect of the transferred data, or the way in which they are subsequently processed. The recipient is bound in this case to act solely under the instructions of the transferer, and while the data may have been physically transferred outside of the EU, decision-making control over the data remains with the entity who made the transfer based in the Community. The transferer thus remains the data controller, while the recipient is simply a sub-contracted processor. In these circumstances, because control over the data is exercised by an entity established in an EU Member State, the law of the Member State in question will continue to apply to the processing carried out in the third country[11], and furthermore the data controller

[11] By virtue of Article 4(1)(a) of directive 95/46/EC.

will continue to be liable under that Member State law for any damage caused as a result of an unlawful processing operation.[12]

This type of arrangement is not dissimilar to that set out in the "Inter-territorial Agreement" which resolved the Citibank 'Bahncard' case mentioned earlier. Here the contractual agreement set out in detail the data processing arrangements, particularly those relating to data security, and excluded all other uses of data by the recipient of the transfer. It applied German law to data processing carried out in the third country and thus guaranteed a legal remedy to data subjects.[13]

There will of course be cases where this kind of solution cannot be used. The recipient of the transfer may not be simply providing a data processing service to the EU-based controller. Indeed the recipient may, for example, have rented or bought the data to use them for his own benefit and for his own purposes. In these circumstances the recipient will possess a certain freedom to process the data as he wishes, thus in effect becoming a 'controller' of the data in his own right.

In this kind of case it is not possible to rely on the continued automatic applicability of a Member State law and the continued liability for damages of the transferer of the data. Other more complex mechanisms need to be devised to provide the data subject with an appropriate legal remedy. As mentioned above, some legal systems allow third parties to claim rights under a contract, and this could be used to create data subject rights under an open, published contract between transferer and recipient. The position of the data subject would be further strengthened if, as part of the contract, the parties committed themselves to some sort of binding arbitration in the event of a data subject challenging their compliance. Some sectoral self-regulatory codes include such arbitration mechanisms, and the use of contracts in combination with such codes could be usefully envisaged.

Another possibility is that the transferer, perhaps at the moment of obtaining the data initially from the data subject, enters into a separate contractual agreement with the data subject stipulating that he (the transferer) will remain liable for any damage or distress caused by the failure of the recipient of a data transfer to comply with the agreed set of basic data protection principles. In this way the data subject is granted a means of redress against the transferer for the misdemeanors of the recipient. It would be up to the transferer to then recover any damages he was forced to pay out to the data subject, by taking action for breach of contract against the recipient.

Such an elaborate three-way solution is perhaps more feasible than it might appear. The contract with the data subject could become part of the standard terms and conditions under which a bank or a travel agency, for example, provide services to their customers. It has the advantage of transparency: the data subject is made fully aware of the rights that he has.

---

[12] See Article 23 of directive 95/46/EC.

[13] Although because this case arose under a law which predated the directive, the law itself did not automatically apply to all processing controlled by a German-established controller. The legal remedy for the data subject was instead created by the ability of German contract law to create third party rights.

Finally, as an alternative to a contract with the data subject, it could also be envisaged that a Member State lay down in law a continuing liability for data controllers transferring data outside the Community for damages incurred as a result of the actions of the recipient of the transfer.

Providing support and help to data subjects

One of the main difficulties facing data subjects whose data are transferred to a foreign jurisdiction is the problem of being unable to discover the root cause of the particular problem they are experiencing, and therefore being unable to judge whether data protection rules have been properly followed or whether there are grounds for a legal challenge.[14] This is why an adequate level of protection requires the existence of some sort of institutional mechanism allowing for independent investigation of complaints.

The monitoring and investigative function of a Member State supervisory authority is limited to data processing carried out on the territory of the Member State.[15] Where data are transferred to another Member State, a system of mutual assistance between supervisory authorities will ensure that any complaint from a data subject in the first Member State will be properly investigated. Where the transfer is to a third country, there will in most cases be no such guarantee. The question, therefore, is what kind of compensatory mechanisms can be envisaged in the context of a data transfer based on a contract.

One possibility would be simply to require a contractual term which grants the supervisory authority of the Member State in which transferer of the data is established a right to inspect the processing carried out by the processor in the third country. This inspection could, in practice, be carried out by an agent (for example a specialist firm of auditors) nominated by the supervisory authority, if this was felt to be appropriate. A difficulty with this approach, however, is that the supervisory authority is not generally[16] a party to the contract, and thus in some jurisdictions may have no means of invoking it to gain access. Another possibility could be a legal undertaking provided by the recipient in the third country directly to the EU Member State supervisory authority involved, in which the recipient of the data agrees to allow access by the supervisory authority or a nominated agent in the event that non-compliance with data protection principles is suspected. This undertaking could also require that the parties to the data transfer inform the supervisory authority of any complaint that they receive from a data subject. Under such an arrangement the existence of such an undertaking would be a condition to be fulfilled before the transfer of data could be permitted to take place.

[14] Even if a data subject is granted rights under a contract, he/she will often not be able to judge whether the contract has been breached, and if so by whom. An investigative procedure outside of formal civil court proceedings is therefore necessary.
[15] See Article 28(1) of directive 95/46/EC
[16] The French delegation could envisage situations where the supervisory authority was a party to the contract.

Whatever the solution chosen there remain significant doubts as to whether it is proper, practical, or indeed feasible from a resource point of view, for a supervisory authority of an EU Member State to take responsibility for investigation and inspection of data processing taking place in a third country.

Delivering a good level of compliance

Even in the absence of a particular complaint or difficulty faced by a data subject, there is a need for confidence that the parties to the contract are actually complying with its terms. The problem with the contractual solution is the difficulty in establishing sanctions for non-compliance which are sufficiently meaningful to have the dissuasive effect needed to provide this confidence. Even in cases where effective control over the data continues to be exercised from within the Community, the recipient of the transfer may not be subject to any direct penalty if he were to process data in breach of the contract. Instead the liability would rest with the Community-based transferer of the data, who would then need to recover any losses in a separate legal action against the recipient. Such indirect liability may not be sufficient to encourage the recipient to comply with every detail of the contract.

This being the case it is probable that in most situations a contractual solution will need to be complemented by at least the possibility of some form of external verification of the recipient's processing activities, such as an audit carried out by a standards body, or specialist auditing firm.

5. The problem of overriding law

A specific difficulty with the contractual approach is the possibility that the general law of the third country may include requirements for the recipient of a data transfer, in certain circumstances, to disclose personal data to the state (the police, the courts or the tax authorities, for example), and that such legal requirements might take precedence over any contract to which the processor was subject.[17] For processors within the Community this possibility is evoked in Article 16 of the directive which requires processors to process data only on instructions from the controller *unless required to do so by law.* However, under the directive any such disclosures (which are by their nature for purposes incompatible with those for which the data were collected) must be limited to those necessary in democratic societies for one of the 'ordre public' reasons set out in Article 13(1) of the directive (see footnote 2 on page 4). Article 6 of the Amsterdam Treaty also guarantees respect for the fundamental rights set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms. In third countries similar limitations on the ability of the state to require the provision of personal data from companies and other organisations operational on their territory may not always be in place.

[17] The extent of state powers to require the disclosure of information is also an issue when making more general assessments of the adequacy of protection in a third country.

There is no easy way to overcome this difficulty. It is a point that simply demonstrates the limitations of the contractual approach. In some cases a contract is too frail an instrument to offer adequate data protection safeguards, and transfers to certain countries should not be authorised.

6. Practical Considerations for the Use of Contracts

The preceding analysis has demonstrated that there is a need for any contractual solution to be detailed and properly adapted to the data transfer in question. This need for detail as regards the precise purposes and conditions under which the transferred data are to be processed does not rule out the possibility of developing a standard contract format, but it will require each contract based on this format to be completed in a way which matches the particular circumstances of the case.

The analysis has also indicated that there are particular practical difficulties in investigating non-compliance with a contract where the processing takes place outside of the EU and where no form of supervisory body is provided for by the third country in question. Taken together, these two considerations mean that there will be some situations in which a contractual solution may be an appropriate solution, and others where it may be impossible for a contract to guarantee the necessary 'adequate safeguards'.

The need for detailed adaptation of a contract to the particularities of the transfer in question implies that a contract is particularly suited to situations where data transfers are similar and repetitive in nature. The difficulties regarding supervision mean that a contractual solution may be most effective where the parties to the contract are large operators already subject to public scrutiny and regulation[18]. Large international networks, such as those used for credit card transactions and airline reservations, demonstrate both of these characteristics and thus are situations in which contracts may be most useful. In these circumstances, they could even be supplemented by multi-lateral conventions creating better legal security

Equally where the parties to the transfer are affiliates or part of the same company group, the ability to investigate non-compliance with the contract is likely to be greatly re-inforced, given the strong nature of the ties between the recipient in the third country and the Community-based entity. Intra-company transfers are therefore another area where there is a clear potential for effective contractual solutions to be developed.

Main Conclusions and Recommendations

[18] In the Citibank 'Bahncard' case, the Berlin data protection commissioner cooperated with the American banking supervisory authorities.

- Contracts are used within the Community as a means of specifying the split of responsibility for data protection compliance between the data controller and a sub-contracted processor. When a contract is used in relation to data flows to third countries it must do much more: it must provide additional safeguards for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection.
- The basis for assessing the adequacy of the safeguards delivered by a contractual solution is the same as the basis for assessing the general level of adequacy in a third country. A contractual solution must encompass all the basic data protection principles and provide means by which the principles can be enforced.
- The contract should set out in detail the purposes, means and conditions under which the transferred data are to be processed, and the way in which the basic data protection principles are to be implemented. Greater legal security is provided by contracts which limit the ability of the recipient of the data to process the data autonomously on his own behalf. The contract should therefore be used, to the extent possible, as a means by which the entity transferring the data retains decision-making control over the processing carried out in the third country.
- Where the recipient has some autonomy regarding the processing of the transferred data, the situation is not straightforward, and a single contract between the parties to the transfer may not always be a sufficient basis for the exercise of rights by individual data subjects. A mechanism may be needed through which the transferring party in the Community remains liable for any damage that may result from the processing carried out in the third country .
- Onward transfers to bodies or organisations not bound by the contract should be specifically excluded by the contract, unless it is possible to bind such third parties contractually to respect the same data protection principles.
- Confidence that data protection principles are respected after data are transferred would be boosted if data protection compliance by the recipient of the transfer were subject to external verification by, for example, a specialist auditing firm or standards/certification body.
- In the event of a problem experienced by a data subject, resulting perhaps from a breach of the data protection provisions guaranteed in the contract, there is a general problem of ensuring that a data subject complaint is properly investigated. EU Member State supervisory authorities will have practical difficulties in carrying out such an investigation.
- Contractual solutions are probably best suited to large international networks (credit cards, airline reservations) characterised by large quantities of repetitive data transfers of a similar nature, and by a relatively small number of large operators in industries already subject to significant public scrutiny and regulation. Intra-company data transfers between different branches of the same company group is another area in which there is considerable potential for the use of contracts.
- Countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers based on contractual clauses.

CHAPTER FIVE: EXEMPTIONS FROM THE ADEQUACY REQUIREMENT

Article 26(1) of the directive sets out a limited number of situations in which an exemption from the 'adequacy' requirement for third country transfers may apply. These exemptions, which are tightly drawn, for the most part concern cases where the risks to the data subject are relatively small or where other interests (public interests or those of the data subject himself) override the data subject's right to privacy. As exemptions from a general principle, they must be interpreted restrictively. Furthermore Member States may provide in domestic law for the exemptions not to apply in particular cases. This might be the case, for example, where it is necessary to protect particularly vulnerable groups of individuals, such as workers or patients.

The first of these exemptions covers cases where the data subject gives his/her consent *unambiguously* to the proposed transfer. An important point to bear in mind is that the consent, following the definition in Article 2(h) of the directive, must be freely given, specific and informed. The requirement for information is particularly relevant in that it requires that the data subject be properly informed of the particular risk that his/her data are to be transferred to a country lacking adequate protection. If this information is not provided, this exemption will not apply. Because the consent must be unambiguous, any doubt about the fact that consent has been given would also render the exemption 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 his exemption. The exemption could, however, be useful in cases where the transferer has direct contact with the data subject and where the necessary information could be easily provided and unambiguous consent obtained. This may often be the case for transfers undertaken in the context of providing insurance, for example.

The second and third exemptions cover transfers *necessary* either 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) or for the conclusion or performance of a contract concluded *in the interest of the data subject* between the controller and a third party. These exemptions appear potentially quite wide, but, as with the fourth and fifth exemptions discussed below their application in practice is likely to be limited by the 'necessity test' : all of the data transferred must be necessary for the performance of the contract. Thus if additional non-essential data are transferred or if the purpose of the transfer is not the performance of the contract but rather some other purpose (follow-up marketing, for example) the exemption will be lost. As regards pre-contractual situations, this would only include situations initiated by the data subject (such as a request for information about a particular service) and not those resulting from marketing approaches made by the data controller.

In spite of these caveats, these second and third exemptions will not be without impact. They are likely often to be applicable, for example, to those transfers necessary to reserve an airline ticket for a passenger or to transfers of personal data necessary for the operation of an international bank or credit card payment. Indeed the exemption for contracts "in the interest of the data subject" (Article 26(1)(c)) specifically covers the transfer of data about the beneficiaries of bank payments, who, although data subjects, may often not be party to a contract with the transferring controller.

The fourth exemption has two strands. The first covers transfers necessary or legally required on important public interest grounds. This may cover certain limited transfers between public administrations, although care must be taken not to interpret this provision too widely. A simple public interest justification for a transfer does not suffice, it must be a question of *important* public interest. Recital 58 suggests that data transfers between tax or customs administrations or between services responsible for social security will generally be covered. Transfers between supervisory bodies in the financial services sector may also benefit from the exemption. The second strand concerns transfers taking place in the context of international litigation or legal proceedings, specifically transfers that are necessary for the establishment, exercise or defence of legal claims.

The fifth exemption concerns transfers necessary in order to protect the vital interests of the data subject. An obvious example of such a transfer would be the urgent transfer of medical records to a third country where a tourist who had previously received medical treatment in the EU has suffered an accident or has become dangerously ill. It should be borne in mind, however, that recital 31 of the directive interprets 'vital interest' fairly narrowly as an interest "which is essential for the data subject's life". This would normally exclude, for example, financial, property or family interests.

The sixth and final exemption concerns transfers made from registers intended by law for consultation by the public, provided that in the particular case the conditions for consultation are fulfilled. The intention of this exemption is that where a register in a Member State is available for public consultation or by persons demonstrating a legitimate interest, then the fact that the person who has the right to consult the register is actually situated in a third country, and that the act of consultation in fact involves a data transfer, should not prevent the information being transmitted to him. Recital 58 makes it clear that entire registers or entire categories of data from registers should not be permitted to be transferred under this exemption. Given these restrictions this exemption should not be considered to be a general exemption for the transfer of public register data. For example, it is clear that mass transfers of public register data for commercial purposes or the trawling of publicly available data for the purpose of profiling specific individuals would not benefit from the exemption.

CHAPTER SIX: PROCEDURAL ISSUES

Article 25 envisages a case by case approach whereby the assessment of adequacy is in relation to individual transfers or individual categories of transfers. Nevertheless it is clear that, given the huge number of transfers of personal data leaving the Community on a daily basis and the multitude of actors involved in such transfers, no Member State, whatever the system it chooses to implement Article 25[19], will be able to ensure that each and every case is examined in detail. This does not of course mean that no cases will be examined in detail, but rather that mechanisms will need to be developed which rationalise the decision-making process for large numbers of cases, allowing decisions, or at least provisional decisions, to be made without undue delay or excessive resource implications.

Such rationalisation is needed irrespective of who is making the decision, whether it be the data controller, the supervisory authority, or some other body established by Member State procedure.

(i) Use of Article 25(6) of the directive

An obvious way of contributing to such rationalisation, foreseen in the directive itself, is would be to determine that certain third countries ensure an adequate level of protection. Such findings would be 'for guidance only', and therefore without prejudice to cases which might present particular difficulties. Nevertheless, this would be a practical response to the problem.
Such determinations would in particular provide a degree of certainty for economic operators regarding those countries which could be considered as generally ensuring an 'adequate' level of protection. They would also offer a clear and public incentive to those third countries still in the process of developing and improving their systems of protection. Moreover, a series of such determinations at Community level would contribute to the establishment of a coherent approach on this issue and prevent the development of a multiplicity of differing and perhaps conflicting 'white lists' issued by Member State governments or data protection authorities.

This approach is not, however, without its difficulties. Principal among them is that many third countries do not have uniform protection in all economic sectors. For instance many countries have data protection law in the public sector but not in the private. Some countries, for example the United States, have specific laws for particular areas (credit reporting and video rental records in the case of the US), but not for others. An added difficulty occurs for countries which have federal constitutions such as the US, Canada and Australia, where differences often exist between the various states that make up the federation. As a result, it seems unlikely that, at present, many third countries could be considered to offer adequate protection across the board. The fewer countries for which postive findings could be made, the less useful the exercise would be, of course, in terms of providing greater certainty to

[19] Member States may set down different administrative procedures to discharge their obligations under Article 25. These may include imposing a direct obligation on data controllers and/or developing systems of prior authorisation or ex post facto verification by the supervisory authority.

data controllers. A further risk is that some third countries might come to see the absence of a finding that they provided adequate protection as politically provocative or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgement on their data protection system.

Having weighed these different arguments carefully, it is nevertheless the opinion of the Working Party that initiating work to make a series of findings under Article 25(6) would be a useful step. Such a process should be seen as a continuing one, not one that would produce a definitive list, but rather a list that would be constantly added to and revised in the light of developments. A positive finding should not in principle be limited to countries having horizontal data protection laws, but should also cover specific sectors within countries where data protection is adequate, even though in other sectors the same country's protection may be less than adequate.

It should be noted that the Article 29 group has no explicit role in making decisions about particular data transfers or in determinations of "adequacy" under Article 25(6). Both are subject to the comitology procedure laid down in Article 31. It should be recalled, however, that one of the specific duties of the Article 29 group is to give the Commission an opinion on the level of protection in third countries (see Article 30(i)b). It therefore falls well within the remit of the Article 29 group to examine the situation in particular third countries and come to a provisional view as to the adequacy of protection. Positive findings, once confirmed in accordance with Article 25(6) would need to be widely promulgated in order to be useful. Where a country is not found to have adequate protection, on the other hand, this need not imply that the country is implicitly or explicitly 'black-listed'. The public message would rather be that no general guidance regarding that particular country is yet available.

(ii) Risk analysis of specific transfers

Although the use of Article 25(6) as described above will be a valuable aid to the decision-making process in respect of large numbers of data transfers, there will nevertheless still be many cases where the third country in question is not the subject (in whole or in part) of a positive finding. How Member States deal with these cases may well vary according to the way Article 25 is transposed into national law (see footnote on the previous page). If a specific role is given to the supervisory authority either to authorise data transfers before they take place, or to carry out an *ex post facto* check, the shear volume of transfers involved may mean that a system to prioritise the efforts of the supervisory authority will need to be envisaged. Such a system could take the form of an agreed set of criteria which enable a particular transfer or category of transfer to be considered as a priority on the grounds of posing a particular threat to individual privacy.

The effect of such a system would not of course change the obligation on each Member State to ensure that only those transfers where the third country ensures an adequate level of protection are permitted to take place. It would constitute guidance regarding which cases of data transfer should be considered as 'priority cases' for examination or even investigation, and thereby allow the resources available to be

directed towards those transfers which raise the greatest concerns in terms of the protection of data subjects.

The Working Party considers that among those categories of transfer which pose particular risks to privacy and therefore merit particular attention are the following:

- those transfers involving certain sensitive categories of data as defined by Article 8 of the directive;
- transfers which carry the risk of financial loss (e.g. credit card payments over the Internet);
- transfers carrying a risk to personal safety;
- transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- repetitive transfers involving massive volumes of data (such as transactional data processed over telecommunications networks, the Internet etc.);
- transfers involving the collection of data using new technologies, which, for instance could be undertaken in a particularly covert or clandestine manner (e.g. Internet cookies).

(i) Standard Contract Clauses

As discussed at length in Chapter Four the directive envisages the possibility that, even where the level of protection is not adequate, a data controller may adduce adequate safeguards for a data transfer by way of a contract. Article 26(2) of the directive allows Member States to authorise transfers on the basis of such contractual provisions, a decision which must then be notified to the Commission. If there are objections to the authorisation, the decision may be overturned or confirmed by the Commission following the comitology procedure laid down in Article 31. In addition to Member State authorisations, Article 26(4) of the directive also allows the Commission, again following the comitology procedure laid down in Article 31, to make judgements as to whether certain standard contractual clauses offer sufficient safeguards. These judgements are then binding on Member States.

Given the evident complexity and difficulty of such contractual solutions, there is clearly a need for agreed guidance to those data controllers who envisage using contracts in this way. At Member State level, the competent national authorities are likely to bear a major responsibility for providing this guidance, particularly when preparing authorisations in the context of Article 26(2). Member State authorities and the Commission should co-operate and exchange opinions on contract clauses submitted to them. Where proposed standard clauses are submitted either to Member State authorities or directly to the Commission, a procedure should be developed to ensure that these clauses also be examined by the Working Party, so as to avoid differences in national practices developing and to ensure that the Commission is able to benefit from the appropriate expert advice before making any decision under Article 26(4).

ANNEX 1

WHAT ARTICLES 25 AND 26 OF THE DIRECTIVE MAY MEAN IN PRACTICE FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Introduction

The main body of this document sets out an overall approach to the issue of third country transfers including:

- an assessment of adequate protection within the meaning of Article 25 of the data protection directive;
- an assessment of alternative means of adducing adequate safeguards through contractual solutions, as envisaged by Article 26(2) ;
- an assessment of the exemptions from the requirement for adequate protection as set out in Article 26(1).

An understanding of the issues would not, however, be complete without an illustration of how this overall approach is likely to impact upon real transfers of personal data. In this annex, therefore, a number of realistic (though fictional) case studies of data transfers are examined in the way it is envisaged that such cases are likely to be examined once the national laws implementing the directive enter into force.

Three different cases are set out. With each case the first step is to assess whether protection in the destination country is adequate by virtue of relevant laws or effective private sector self-regulation. If it is not then the second step is to search for a solution to the problem among the possibilities set out in Article 26, paragraphs 1 (exemptions) and 2 (contractual solutions). Only then, if no solution is appropriate, would the third step be to block the transfer.

CASE (1) : A transfer of data regarding credit-worthiness

A community citizen wishes to buy a holiday home in Country A outside the EC and applies for credit to a financial institution in that country. The financial institution requests a credit report from a credit reporting agency. The agency has no file on the individual but arranges for the individual's full credit history to be transferred from its 'sister' Credit Reference Agency in the UK. Country A is an advanced industrialised nation, with long-standing and stable democratic institutions. The judicial system is well-resourced and functions effectively. It has a federal constitutional structure.

STEP ONE : ASSESSING THE ADEQUACY OF THE PROTECTION

The relevant applicable rules

The receiving data controller is subject to a federal law which sets down rules regarding personal information held for the assessment of credit risks. The data controller additionally claims to comply with its own published privacy policy. No state law is applicable and there is no industry-wide self-regulatory code.

Evaluation of the content of the applicable rules

First it should be noted that the communication made by the UK based credit reference agency would, like any communication to a data controller elsewhere in the UK or another Member State, be subject to the normal requirements of UK law which implement all the articles of the directive other than articles 25 and 26. This is important because it eliminates the need to examine the lawfulness of the communication itself. The focus of attention is rather the protection that will be afforded to the data once transferred to Country A.

Evaluation of rule content should logically start with the federal legislation. Where gaps are found here, the 'softer' law of the privacy policy could be considered to see if it fills these gaps. What follows is a list of the content that would appear necessary, and a judgement as to whether this necessary content is present either in the law or the privacy policy.

The purpose limitation principle can in this context concern itself solely with the requirement that any secondary uses and disclosures of the transferred data are not incompatible with the purpose for which they were transferred. The inclusion of the data in a mailing list to be sold or rented on the open market might be considered incompatible, as would the disclosure of the data to prospective employers or business partners interested in the solvency of the individual concerned. Disclosures of the data to other credit grantors (banks, credit card companies), however, might be considered compatible.
In this case the federal law does lay down a limited number of purposes for which personal credit information can be legitimately disclosed. However, these purposes

include “employment” and “legitimate business need related to a business transaction involving the individual”. This latter concept includes certain marketing uses of data which could involve the marketing of goods or services other than credit by third parties.
It would therefore appear that the purpose is not sufficiently limited by the federal law, and that on this point protection is not adequate. The company’s privacy policy does not improve the situation.

The transparency principle should result in the data subject being made aware of the identity of the credit reporting agency in Country A and of any new purposes for which data are to be processed. The precise way in which this is done should be comparable with that set out in Article 11 of the directive.
In this case the federal law has no specific provisions on transparency which impact directly on the credit reporting agency. The credit grantor in Country A is, however, required to inform the individual that a credit report will be requested from the Credit Reporting Agency, although the name and address of the agency need not be given.
The individual therefore has no legal guarantee of being informed about the fact that the specific Credit Reporting Agency concerned is processing data about him. However, given that the agency has no direct contact with the individual, for the agency to be under an obligation to contact the individual specifically to inform him/her would appear to represent a “disproportionate effort” in the sense of Article 11 of the directive. The level of protection regarding transparency would therefore appear to be sufficient.

The quality and proportionality principle includes several different elements. There is no restriction on the collection and processing of unnecessary data in the federal law. As to duration of storage, there are rules that prevent the dissemination of obsolete information (bankruptcy judgements more than 10 years old), which effectively lead to the erasure of this information. There is no general legal requirement to keep data accurate, although when an individual who has applied for access to his credit report disputes some of the information, data which can’t be verified must be deleted.
Once again protection does not seem entirely adequate, and the company’s privacy policy goes no further than the federal law.

The security principle is reflected in the federal law by a requirement to take reasonable measures to prevent unlawful disclosure. The privacy policy of the company makes it clear that stringent controls are in place to prevent unauthorised access to and manipulation of credit information. These controls take the form of both technical devices (passwords etc.) and instructions to employees which if broken can result in disciplinary proceedings. This would seem to ensure an adequate level of security.

The rights of access and rectification are included in the federal law and are comparable to those found in the directive. Where an individual has been refused credit the access to the credit report is free of charge. There is, however no right of opposition although an individual can complain to a specialist federal agency or go to court (see below) where his legal rights under the federal law have been violated.

Sensitive data about the individual's health form part of the data transferred. The federal law does include stricter provisions for the processing of information relating to criminal records, sex, race, ethnic origin, age and marital status, but not for health information. However, in its privacy policy the credit reporting agency states that health data will not be used for credit assessment purposes, but only for employment or insurance checks. In these two situations the use of such data will be authorised by the individual on an employment application or insurance form.
There would therefore appear to be substantively reinforced protection for the health data involved in this example, even though this protection is not provided by statute.

Use of the data for direct marketing purposes by the credit reporting agency (and the disclosure of the data to others for such purposes) is an issue here. There is no real statutory impediment to such use and no legal requirement to offer an opt-out. This is clearly inadequate particularly as in this case not only will the data be used by the agency (to carry out host mailings for credit granting financial institutions) but also disclosed to third parties for the marketing of both related financial services products and unrelated products such as lawn-mowers and holidays.

It would appear that the purpose of the transfer may be to enable an automated decision to be made about whether the data subject should be granted credit. The data subject should therefore benefit from additional safeguards in this regard. Although the federal law includes provisions permitting the individual to dispute information held on a credit report and attach explanations to the report if necessary, there are no provisions allowing a decision made on the basis of erroneous or incomplete information to be challenged, reviewed and, if the challenge is justified, changed. The mechanism allows a credit report to be altered so as to avoid future problems, but it does not necessarily address the problem of a credit decision already taken. This non-retroactive legal protection is not sufficient.

Restrictions on onward transfers of the data to a further third country or to organisations in other sectors within Country A not subject to the rules laid down in the federal law. There are no such provisions either in the federal law or the company privacy policy.

Scope of the federal law and privacy policy
One further check should be made to ensure that both the law and the privacy policy apply to data about all individuals, and not just data about residents or nationals of Country A. In this case, no such restrictions to the scope are present.

Evaluating the effectiveness of the protection

The federal law in question has the force of law and also establishes a public authority with some external supervisory powers. Individuals may also take private law suits under the legislation to enforce their rights. However, the public authority is not under a clear obligation to investigate all individual complaints, and, according to some commentators, has not always been particularly active in enforcing the law. Private law suits are an expensive and often time-consuming means for individuals to ensure

redress, particularly where the individual data subject lives in a country other than the country where the legal proceedings are taking place.

The company's internal privacy policy contains no independent mechanism allowing an individual to enforce his/her rights, but it does contain some disciplinary sanctions for employees who violate the policy. Several employees have indeed already been disciplined regarding past violations.

The combination of legislation and internal privacy code must be evaluated according to the 'objectives' that have been laid down for procedural mechanisms. In this case the key questions could include:

Good level of general compliance

The main encouragement for the company to comply with its own privacy policy is the risk of harmful publicity in the press if it is found not to deliver on its promises. In addition individuals within the company may be subject to disciplinary measures if they flout rules on security.
However, these mechanisms do not in themselves seem sufficient to ensure that the privacy policy is complied with in practice.
This conclusion may have been different different if :
(1) the company's privacy policy had been mirrored in an industry-wide code of conduct established by the industry trade association, under which any company found to be in breach of the code would be immediately expelled from the association; or
(2) a general principle of law allowed a company found to be in breach of its own published privacy code to be prosecuted by a public agency on the grounds of "unfair and deceptive" practices.

As far as the federal law is concerned, compliance is encouraged by the possibility of private law suits in the case of non-compliance. The prospect of being taken to court would have some deterrent effect on the data controller. There is, however, very little in the way of direct external verification of data processing procedures, as the public authority reacts only where a problem is drawn to its attention by a complainant or by the press, for example.

Support and help to individual data subjects
Clearly a public agency does exist and it does serve as a focal point for complaints from individuals about their credit reports. Complaint investigation carries no cost to the individual.

Appropriate Redress
For breaches of the fairly narrow legal obligations of the federal law, the individual can obtain redress from a court. This is, however, a relatively expensive process, and the individual often does not receive support from the public agency in these legal proceedings. The court can order the data controller to pay damages to the individual (where it finds that damage has been caused) and to amend its data processing procedures and the content of the credit file in question. For breaches of those data protection principles enshrined only in the privacy policy, no such redress is possible.

The Verdict

1) Certain of the data protection principles set down as 'core principles' in the discussion paper can be found in some form in the federal law applicable to the credit file. Certain others are found in the privacy policy. Even taken together, though, the complete set of 'core principles' cannot be said to be present, and some of those that are present (e.g. the purpose limitation principle) are in a fairly weak form.
2) There is a more general problem of whether the privacy policy of the company is in any case a sufficiently effective mechanism to be taken into account at all. Unless the policy is underpinned and made more enforceable by way of powers of external control given to an industry association or public body, its provisions are largely unenforceable and can therefore be left to one side.
3) Although the public body established to enforce the federal law does not have quite the same powers as the typical European data protection authority, the law nevertheless provides a certain legal security, particularly in the context of a judicial system that functions well and the "litigation culture" found in Country A. The law contains clear provisions on perhaps the most important data protection principle of all - the right of access and rectification, and some limitations on the purpose for which data can be used.

Conclusion
Protection is inadequate because the law covers too few of the "core principles" and the privacy policy, standing alone, is not an effective means of providing protection. An adequate verdict could result either if the law were developed to include principles such as transparency and protection for health data, or if the privacy policy were rendered more effective by one of the methods suggested above (i.e. making compliance a condition for membership of an industry association, or giving a public agency powers to prosecute the company for misleading and deceptive practices if it failed to comply with its own policy).

STEP TWO : SEARCHING FOR A SOLUTION

Of the possible exemptions set out in Article 26(1), only (a), the consent of the data subject, would appear to be appropriate. The exemption in (b) which deals with a transfers necessary for contractual reasons is not applicable because the transferring party, the UK-based credit reference agency has no contractual relationship with the data subject. It is also difficult to make an argument that the transfer is necessary on the basis of a contract "in the interests of the data subject" as required by exemption (c).

Data subject consent would, however, seem to be a relatively straightforward solution to the problem. Consent could be obtained either directly by the UK-based credit reference agency, or on behalf of the UK agency by the financial institution in Country A, who could ask for consent on the loan application form. Whatever method chosen, the data subject should be informed of the particular risk resulting from the fact that his data are to be transferred to a Ccountry lacking adequate protection.

Given the fact that this kind of transfer is still relatively rare, the obtaining of consent on a one-off basis is probably the most practical solution. If credit reporting and reference agencies around the world begin to exchange data on a more systematic basis, then other arrangements, such as contractual solutions or an international code of conduct could be developed.

CASE (2) : A transfer of sensitive data in the airline industry

A Portuguese citizen books a ticket at a Lisbon travel agency for a flight on board an airline based in Country B. The data collected include details of the fact that the citizen is disabled and uses a wheelchair. The data are entered on an international computer reservation system, and from there are down-loaded by the airline onto its passenger database located in Country B, where they are retained indefinitely. The airline plans to use the data to provide better service to the passenger if he were to travel with the airline in the future, as well as for internal management planning purposes.[20]

STEP ONE : ASSESSING THE ADEQUACY OF THE PROTECTION

The relevant applicable rules

Although there is an international code of conduct applying to the data held on computer reservation system, no data protection rules are in place regarding the data held on the airline's own database in Country B.

Evaluation of the content of the applicable rules

None are applicable.

Evaluating the effectiveness of the protection

Not applicable

Verdict

Protection levels in Country B are not adequate, particularly given the sensitivity of the data involved.

STEP TWO : SEARCHING FOR A SOLUTION

The transfer of data onto the Computer Reservation System and its use by the airline for the purpose of providing the appropriate service to the disabled passenger for the flight in question is a transfer necessary for the performance of the contract between the passenger and the airline (Article 26(1)(b)). However, the continued retention of the data (including sensitive data about the data subject's health) on the airline's database cannot be justified on these grounds. The transfer of data to the airline must therefore be covered by a different exemption.

As with Case (1), data subject consent would seem to be the best solution. Consent could be obtained by the travel agent in Lisbon on behalf of the airline. The risks of the

[20] This case has some similarities with a real case that has arisen under existing Swedish law, involving American airlines and Lufthansa. The case is still under appeal.

data being held in Country B should be pointed out to the data subject, as should the fact that the transfer and retention of data in airline's own database is not necessary for the reasons pertaining to the specific flight being booked.

CASE (3) : A transfer of marketing list data

A company in the Netherlands specialises in the creation of mailing lists. Using many disparate sources of public information available in the Netherlands, together with client lists rented from several other Dutch companies, the resulting lists purport to include individuals fitting particular a particular socio-economic profile.. These lists are then sold by the Dutch company to client companies not only in the Netherlands and the EU, but in a multitude of other third countries. The recipient client companies then use the lists (which include postal e-mail addresses, telephone numbers, and often e-mail addresses) to contact the individuals on the lists with a view to selling a bewildering array of different products and services. A large number of individuals included in the lists have complained to the Dutch data protection authority about the marketing approaches they have received.

The relevant applicable rules

Some of the client companies who buy in the mailing lists offered by the Dutch company are based in countries which have general data protection legislation in place which includes a right for individuals to opt-out of receiving such marketing approaches. Others are in countries without such laws, but are members of self-regulatory associations which have developed a data protection codes. Others are subject to no data protection rules at all.

Evaluation of the content of the applicable rules

This single case would require the evaluation of a multitude of different laws and codes. If the Netherlands-based company is to maintain its approach of selling or renting its lists to companies based in any country of the world, then there are necessarily going to be situations where the level of protection is not adequate.

STEP TWO : SEARCHING FOR A SOLUTION

In this example, because the data are collected from public sources and without any direct contact with the data subject it would be very problematic for the Netherlands company to seek consent from each and every data subject to his/her inclusion on the mailing lists. In view of this it is unlikely that any of the exemptions in Article 26(1) are likely to be useful.

The Netherlands company has two possibilities, which could be used as alternatives or together. First would be to limit his trade in mailing lists to companies in jurisdictions which clearly appeared to ensure adequate protection by virtue of laws or effective self-regulatory instruments. In making this decision the company could be guided by any available "White list".

The second possibility would be to require contractual undertakings from all client companies (or at least those in "non-adequate" jurisdictions) regarding the protection

of the data transferred. These contractual arrangements should follow the advice set out in Chapter Four of the main paper. In particular they should seek to create a situation under which the Netherlands company remained liable under Netherlands law for any violation of data protection principles resulting from the actions of the client company to whom the mailing lists had been transferred.

Such a contractual solution, if properly implemented, would help overcome the effective barrier to trade that the lack of adequate data protection in certain third countries creates.

Done at Brussels, 24 July 1998

For the Working Party

The Chaiman

P.J. HUSTINX