



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/5005/98 final

WP 9

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

**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

The use of contractual provisions in the context of transfers of personal data to third countries

1. Introduction

In the discussion document adopted by the Working Party on 26 June 1997 entitled 'First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy', the Working Party promised to examine in its future work the circumstances in which *ad hoc* contractual solutions may be an appropriate means of securing protection for individuals when personal data are transferred to a third country where the level of protection is not generally adequate. This document is intended to provide a basis for such an examination.

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. Article 26(1) sets out certain exemptions to that rule. These exemptions are not examined in this paper. The purpose of this paper is to examine the additional 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.¹ 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.²

¹ '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

² See the presentation of Alexander Dix of this case at the International Data Protection and Privacy Commissioners' Conference, September 1996, Ottawa.

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 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 of the protection provided by the

directive, and indeed by the general framework of Community law³) 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.

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 the "First Orientations..." discussion document.⁴ This document sets out an approach consisting of a series of basic data protection principles together with the three further requirements: that there be a good level of compliance with these principles in practice, that support and help be available to individual data subjects in the exercise of their rights, and that an appropriate means of redress be available to the injured party when the principles are not complied with.

(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 the "First Orientations" paper apply to the processing of the data transferred to the third country. These basic principles are:

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 (e.g. national security, the investigation of criminal offences).⁵

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 the Articles 13 of the directive, or Article 11(2) which allows organisations who have not collected data directly from the data

³ 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 "First Orientations on Transfers of Personal Data to Third Countries - Possible Ways forward in Assessing Adequacy", Discussion document adopted by the Working Party on 26 June 1997.

⁵ It should be noted that statistical and scientific research purposes are generally considered to be compatible, provided appropriate safeguards are in place.

subject to be exempted from the requirement to provide information if to do so would be impossible or involve a disproportionate effort

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 to non-parties to the contract** - 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.

Furthermore in some situations additional principles must be applied:

1) **sensitive data** - where 'sensitive' categories of data are involved (those listed in article 8), 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.

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.

(ii) *Rendering the substantive rules effective*

The "First Orientations..." document 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:

1) 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 is important in ensuring respect for rules, as of course are systems of direct verification by authorities, auditors, or independent data protection officials.

2) 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 needs to be some sort of structure or mechanism allowing independent investigation of complaints.

3) provide **appropriate redress** to the injured party where rules are not complied with. This is a key element. It must involve a system which provides impartial judgements and which allows compensation to be paid and sanctions imposed where appropriate.

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 transferring party 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, however, 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 set down the way the recipient is to apply the basic data protection principles in such detail that, in effect, 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 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 country⁶, and furthermore the data controller will continue to be liable under that Member State law for any damage caused as a result of an unlawful processing operation.⁷

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.⁸

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 need 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.

⁶ By virtue of Article 4(1)(a) of directive 95/46/EC.

⁷ See Article 23 of directive 95/46/EC.

⁸ 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.

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.

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 of 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.⁹ 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.¹⁰ 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 generally¹¹ 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.

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

⁹ 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.

¹⁰ See Article 28(1) of directive 95/46/EC

¹¹ The French delegation could envisage situations where the supervisory authority was a party to the contract.

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.¹² 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. 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.

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

¹² 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.

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 regulation¹³. 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

- 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

¹³ In the Citibank 'Bahncard' case, the Berlin data protection commissioner cooperated with the American banking supervisory authorities.

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.