Study contracts involving the transfer of personal data between Parties to Convention Ets 108 and third countries not providing an adequate level of protection (2001), by Mr. Jérôme HUET

Agrégé des facultés de droit, Professor of the University of Paris II (Panthéon-Assas), Director of the CEJEM (Centre of Multimedia Legal and Economic Studies) (France)

Report considered by the Drafting Group of the Consultative Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108), at it's 6th meeting, Strasbourg, 7-9 February 2001

SUMMARY OF CONTENTS

INTRODUCTION

The automated processing of personal data in European countries is protected by legislation on account of the risks that such operations present to the data subjects. These

countries began to pass such legislation in the seventies. On 28 January 1981, a convention was signed under the aegis of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, which entered into force in 1985.

The existence of such instruments to regulate data processing within the national territories to which they apply has rendered it necessary to consider the way in which to harness the international transfer of such data, a transfer that is facilitated by the existence of digital telecommunication systems and which the internationalisation of the economy renders inevitable. The question, which initially involves relations between large-scale private enterprises, particularly those established in several places throughout the world, is a particularly vexed one if the transfer is likely to be made to a country that does not provide an adequate level of protection for such data.

Article 12 of the 1981 convention, for example, establishes the principle of the free flow of personal data between contracting states in paragraph 2 but goes on, in paragraph 3, to grant each party the right to prohibit or restrict transfrontier flows in respect of certain categories of data covered by specific regulations, except where the regulations of the recipient state provide equivalent protection. At the same time, paragraph 3.b provides for the restriction or prohibition of the flow of personal data across national borders into non-contracting states.

Moreover, various national laws contain restrictions on transfrontier flows of personal data.

Use of contractual clauses

In order to contain, and thus legitimise, such exchanges, the possibility was considered of relying on the rules of contract. In fact, it seemed that in contractual relations between two companies, one "exporting" data and the other "importing" data, the means of transmitting, processing, using and keeping data would be in accordance with the legal requirements of the country of the first company provided that the second company gave undertakings to protect the security of the data in question and respect both the purpose for which they had been collected and the rights of the data subjects.

The basis for such a system would be that even in countries where there is no protective legislation or personal data protection system, some companies of impeccable integrity are able to enter into agreements expressed in such a way as to get round the absence of national legislation and to render the transfer of the information in question legally acceptable.

Such clauses were drawn up during the nineties by international courts anxious to devise a suitable form for the transfer of data, by the Council of Europe, by the International Chamber of Commerce, and by some data protection authorities. Thus, the Council of Europe took the initiative together with the International Chamber of Commerce and the European Community to circulate, in 1992, "A Model Contract to Ensure Equivalent

Data Protection in the Context of Transborder Data Flows" (doc. T-PD (92) 7, as revised).

Development of the problem

The development of the law since that time, and in particular with the adoption by the European Community in 1995 of a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, together with a directive specifically dealing with telecommunications in 1997, calls for an evaluation of this system.

The 1995 directive, moreover, contains specific provisions governing the transfer of data to third countries, in particular Article 25, under which transfers can only be made to countries guaranteeing "an adequate level of protection".

Another reason for change lies in the development of electronic communications thanks to the Internet, and more specifically to an upsurge of electronic trade. In fact, electronic trade promotes the collecting of personal data, particularly in relation to visitors to the websites set up by the companies, or to customers. Visitors and customers are, moreover, frequently solicited when they return to the website by means of "cookies" that were implanted on the hard drive of their computer at the time of their previous visit. Concerns for the protection of people who fall prey to such practices, and of others, were debated during the summit meeting organised by the OECD in Ottawa in 1998, and one of the resolutions passed on that occasion concerned "the protection of privacy on world networks" (see Information and Telecommunications Law Review, 1998-3, from p. 101, commentary of E. Caprioli).

This side of things, however important it may be, nevertheless does not get to the heart of the subject under discussion. In fact, this type of application of electronic trade calls into play relations between the companies and their customers or prospective customers, and leads one to wonder how the former collect data on the latter. However, the object of this study is different, being concerned with the transfer of personal data between companies and on the contractual clauses enabling such transfers.

Definition of the scope of the study

The author of this study has been instructed to evaluate the workings of the contractual clauses used for the transfer of personal data, in the light of existing practices and of developments within the context in which they operate.

It was specified that this evaluation should take account principally of the underlying principles of contract. The object of the study is, therefore, mainly to compare the mechanisms used in this area and for these specific purposes with the general law of contract.

As a peripheral issue, this study will evaluate the adequacy of the existing model clauses in the light of the development of data protection over recent years.

Preliminary points

At this stage, three preliminary points should be made:

1. In regard to the development of personal data protection, the key instrument is the European Community directive of 1995, Article 7 of which lays down the principle that such data may only be processed with the consent of the data subject (such consent having been given "unambiguously") and Articles 10 and 11 of which provide for the data subject to be specifically informed at the time of the collection of data, and where such data are disclosed to a third party.

To a lesser extent, account is taken of instruments such as the EEC-USA Agreement of 20 July 2000 based on the so-called "safe harbour principles".

2. In regard to the rules of contract, and by virtue of the fact that the problem inevitably has an international dimension, it has not been possible to refer exclusively to one particular national body of legislation: I have, therefore, opted to rely on universally accepted principles on the subject, such as "Unidroit principles for international commercial contracts" (and see in this context: "Unidroit principles for international commercial contracts: a new lex mercatoria?", International Chamber of Commerce, published by the Institute of Law and Practice of International Commerce, 1995).

In any case, it may be presumed that the parties to the transfer of personal data to a country outside the European Community will have designated, as the governing law, the law of the country in which the exporter is established, that is, the law of a European country, and therefore a law that is in harmony with Unidroit principles.

3. Finally, in regard to existing practices, in order to arrive at a proper understanding of the problem, the following have been examined: the standard form contract drawn up jointly by the Council of Europe, the EEC and the ICC in 1992 – and the version that is being currently distributed by the ICC – together with certain model agreements drafted by national authorities, particularly in Germany (Berlin) and the United Kingdom (for the Commonwealth); in addition, the work initiated in 2000 by the European Community pursuant to Article 26 (4) of the 1995 directive, has also been taken into account (see the Preliminary draft of a Commission decision on standard clauses for the transfer of personal data to third countries, December 2000).

However, it does not fall within the scope of this study to carry out a detailed examination, or critique, of these various contractual models. They have simply served as the basis for consideration.

In order to carry out the evaluation as instructed, I have decided to study the contract for the transfer of data in relations between the parties (I), then to examine it having regard to

relations with third parties (II) and then, finally, to consider the methods of settling disputes (III).

I. Contract for transfer of data and relations between the parties

In relations between the parties, first the subject matter of the contract and the mutual obligations of the parties should be identified (A), then there should be set out the guarantees for the due performance of the contract (B) and, finally, the means by which this is to be achieved (C).

A. Subject matter of the contract and obligations of the parties

The subject matter of a contract involving the transfer of personal data may differ to some extent according to the situation (1), but the obligations of the parties in relation to the transferred data will always have certain points in common (2).

1. Subject matter of the contract

There are a number of possibilities. Three particularly typical categories of situation may be identified.

- First case: involving data relating to customers, where the aim of the data exporter is to process them in a foreign country either in order to cut costs or to concentrate data processing relating to his group in that country.

- Second case: the data relate both to employees and to directors of the various subsidiaries of a group of companies established in several countries, and their transfer from one subsidiary to another is necessary for the efficient management of the group as a whole.

- Third case: involving data relating to the customers and prospective customers of a company which then transfers them to another company situated in a foreign country so that the latter may use them in its commercial activity of establishing a customer base.

The data being processed can vary considerably in nature: those relating to customers may be fairly basic (name, address, activity and size of operation...), but they are sometimes sensitive (for example, a life insurance file, data relating to health); data relating to employees may, while being of a minor nature, also encroach on their private lives…

The very diversity of the scenarios makes it hard to classify them (a); it is, moreover, rare for the contractual clauses used to distinguish between the types of personal data transferred (b).

a. Type of contract: deposit or transfer (cession)

The transfer of personal data can be categorised in various ways. For example, a case in which data on employees in a group are to be circulated within that group might fall into a category which could be called “pooling of resources”.

However, a more conventional approach would be to distinguish between contracts according to whether the transfer of personal data is ancillary to the contract or constitutes its main subject.

When the parties are contemplating, for example, the processing of personal data by a sub-contracted processor (as in the case of “outsourcing”), the service contract comprising that outsourcing is the main subject of the contract. The imposition of a number of binding obligations governing the transfer of personal data is ancillary to the contract as a whole.

On the other hand, the transfer of personal data is the main subject of the contract in the event of data relating to customers or prospective customers being passed from one company to another in order that the other company may use them to canvass for business.

In the first of those cases, the transfer of data might be described as an ancillary deposit for services rendered (rather as one would pay a deposit to a garage when leaving a car there for repair). Perceiving it as a deposit in the hands of a third person, in this case the data importer gives rise to a number of consequences:

- the data exporter retains overall control of the data, as he has merely entrusted them to another;

- the data importer would not be entitled to use the personal data concerned for his own ends, nor a fortiori to his own advantage;

- the data importer is obliged to return them (or to destroy them, where they are non-material goods capable of being reproduced) at the end of the contract;

- the contract is based on mutual trust between the parties and the exporter may terminate it if at any time that confidence is breached.

Thus defined, this type of situation may be regarded, on the face of it, as presenting few risks for the data subjects, and moreover the preliminary draft of a Commission decision on standard clauses for the transfer of personal data to third countries of December 2000 appears to consider it so mundane as to exclude it from the scope of its application (instrument cited above, Article 2 (3), which ends: “this contract does not concern transfers to a third party processor who remains under the control of the Data Exporter”.)

In the second case, the transfer of data is a licensing of data or, at the least, a final delivery and thus falls within the category of contracts transferring title, such as a contract of sale. Certainly, in legal terms everything depends on ascertaining whether the

governing law – it was emphasised that it would be prudent for the parties to choose that of the exporter's country – regards a client file as constituting a non-material asset protected by intellectual property law (for example, literary and artistic property). But, in any event, it is obvious that the parties will have clarified the possibility of the importer using the data in his professional activities, where necessary combining them with information coming from other sources.

This categorisation in turn gives rise to a number of consequences:

- the exporter to a large extent loses control of the data in question, having granted a licence for their use to a third party;

- the importer is entitled to use the data in the context of his activity and in particular to use them for financial gain;

- at the end of the contract, it is not necessary for the data to be returned by the importer to the exporter;

- the contract is not based on mutual trust and cannot therefore be repudiated unilaterally.

The situation thus created would appear to pose more risks for the data subjects, as indicated by the fact that the Council of Europe in 1992 purports to exclude it in specifying that "the objective is not to transfer the right of property of personal data, but merely a right to use these data" (instrument cited above, paragraph 33). However, situations of this kind frequently occur and the extent of the risk has to be assessed in relation to the type of data being transferred: if the data are not sensitive, it may be minimal.

The Commission of the European Communities, for its part, appears to have taken note of this possibility and the risks that it presents, as in one of its working documents on this subject it states: "The recipient of the transfer may not be simply providing a data It is possible that the recipient of the transfer is not merely providing a data processing service to 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. (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, DG XV D/5005/98 final, 22 April 1998, "Preliminary views on the use of contractual provisions for the transfer of personal data to third countries", p. 7.

This gives an indication of the variety of situations which may arise. There is no point in going any further into the distinctions even though other categories could be considered, for example "data leasing" – a case in which access is temporary but combined with the possibility for the recipient to consult a relatively wide range of data – or mere remote consultation of personal data files from a non-member country of the Council of Europe.

b. Data involved and their application

It is useful to conclude this initial consideration of the subject matter of the contract with an examination of the types of data transferred.

In this context, one should adopt the classic distinction between personal data according to whether or not they are sensitive. The concept of sensitive data was, as we know, brought into general use at European level through the 1995 directive: they include racial or ethnic origin, political, philosophic or religious convictions, membership of a trade-union and data relating to health. To this it could be added that considerable caution should be exercised in dealing with information relating to social mores and, indeed to the tastes of the data subjects; for example, consumers and employees, and it would thus be wise to specify such data in contracts. Such data could be classified as "semi-sensitive".

Contractual clauses for the transfer of data seldom in practice include the concept of sensitive data. The 1992 model contract of the Council of Europe contains no reference to it (instrument cited above). On the other hand, the EEC-USA Agreement of 26 July 2000 mentions them specifically, specifying that the data subjects must have been given affirmative or explicit choice if the data is to be disclosed to a third party (instrument cited above, under "Choice".)

The distinction between various types of contract, as mentioned above, could be happily combined with this latter distinction.

In fact, it seems that the basis of mutual trust, such as the ancillary lodging of a deposit in a service contract, could be extended to the transfer of sensitive data (no doubt with additional safety measures), for the very reason that they rely on the trust that the data exporter has towards the importer. On the other hand, as they are not based on mutual trust, contracts relating to the licensing of data should not, as a general rule, involve sensitive data.

These findings would suggest that there would be an advantage in drawing up of contractual clauses for the transfer of personal data to third countries to distinguish both according to the type of contract being entered into and the type of data involved.

2. Liabilities of the exporter

The data exporter assumes obligations both in relation to the data (a) and in relation to the data subjects (b).

a. Obligations in relation to data

As these relate to the data themselves, the exporter – quite apart from the fact that model contracts generally include a statement to the effect that the exporter has processed the data exactly as required by the law – undertakes before all else to inform the importer of

the regime applying to them and, in particular, pertinent legislation. The latter will thus be in a position to know which regulations will govern, ab initio, the processing of the data.

It would be advisable for model contracts to contain, in this context, an undertaking on the part of the exporter to provide a copy of the instrument setting out the purpose of the processing, for example, the declaration submitted to the supervising authority: this would enable the importer to have a clear idea of the declared purpose of the processing, of the recipients of the data, and of how long it is intended to keep them.

As far as general contract law is concerned, the only requirement is to ensure that this disclosure can be made with respect for business confidentiality.

b. Obligations towards data subjects

The data exporter also assumes obligations towards data subjects, as it is vital for them to be able to exercise their rights of access, of verification and of rectification of the data (see Part II below). One of the obligations assumed by the exporter in this regard is the inclusion in the contract of a clause conferring rights on a third party in order that the data subjects may be able to assert their prerogatives in relation to the importer (see Part II below).

However, under the 1995 EEC directive, it must be assumed that the exporter is required to go further. It has, in fact been emphasised (see above, under Introduction) that this instrument imposes the requirement to obtain the consent of the data subject for the processing of data relating to him (Article 7) and provides that in the event of data being circulated he would be informed of their transfer (Articles 11 and 12).

Consequently, if the data subjects' initial consent for the data to be processed was confined to the party who collected the data from them, precluding any transmission to third parties (which is quite frequently the case, for example with banking data), it appears that, in order for data to be exported to a third party, they would have to agree in principle to the operation or at least be notified of transfers before they are carried out. And the obligation would appear to be even more binding where, as in the case in point, the transfer is to a country not providing an adequate level of protection.

In this context, model contracts should contain a specific declaration by the exporter that he has fulfilled his obligation of notifying data subjects of the transfer of data across national boundaries.

The EEC-USA Agreement of 26 July 2000 imposes an obligation on an organisation to "inform individuals about the purpose for which it collects and uses information about them… (and) third parties to which it discloses the information", an obligation that should be carried out in the case of a transfer of personal data "before it discloses it for the first time to third parties" (instrument cited above, under "Notice"), such notification

offering individuals the opportunity to choose, that is, the right to opt out from the transfer of data (instrument quoted above, under “Choice”).

3. Undertakings of the importer

In common with the exporter, the data importer assumes obligations both in relation to the data (a) and in relation to data subjects (b).

a. Obligations in relation to the data

In the commonly used model contracts, the data importer gives an initial undertaking to respect the regulations governing data processing in the country of origin in accordance with the information which he has been given in this connection.

In particular, he will undertake not to use the data beyond the terms of the contract and to ensure that unauthorised third parties cannot have access to them.

In particular, he will undertake to safeguard, through technical means, the data in question, and he will agree to allow the exporter access to his organisation in order to carry out controls in this regard (see on this point B below).

Such obligations are perfectly acceptable under general contract law.

b. Obligations towards data subjects

With regard to data subjects, the data importer enters into an obligation not only to respect the declared purpose of the processing and to guarantee its protection in accordance with the law governing the original collection of the data, but also to comply with any requests on the part of data subjects to avail themselves of their right of access, of verification and of rectification.

To this end, he will include in the contract for their benefit a clause conferring rights on a third party (for the effectiveness of this, see Part II below).

B. Safeguards for the due performance of the contract

The contract must include safeguards to ensure due performance: as a preventive means, the control mechanisms will preclude any exceeding of the scope of the contract (1), and the parties will be responsible for seeking redress in the case of any breach of undertaking (2).

As we shall see, the relative non-availability of any mechanism for imposing liability renders preventive means all the more important.

1. The control of technical protection mechanisms

The preventive mechanism is generally well developed in existing contracts. It comprises means of control of the effective use of the data with regard to the declared purpose of the processing, together with protective measures that must be taken: these means of control are available to the exporter and they also involve the importer.

While this type of mechanism is not frequently found in private law contracts, it is to be seen occasionally. In practice some commercial agreements make provision for one of the parties to be able to control the activities of the other: such is the case with accounting (audit), the production process (quality control) and the factors involved in the setting of prices (cost control)…

There is, therefore, no legal problem in accepting the validity of the process. Provided that the arrangements made are sufficiently clear, the system should work well.

Nonetheless, there is a question-mark over the effectiveness of these controls. If their purpose is to obviate the need to seek legal redress a posteriori, it may be extremely difficult to set them up in practice, and they may even be unacceptable under the business law governing the data importer in the third country.

2. Liability for non-performance giving rise to a penalty

In existing model contracts, non-performance is penalised, in accordance with the general principles of contract law (see the Unidroit principles cited above, Article 7.4.1 et seq.), by the seeking of damages. There is, however, some doubt as to the adequacy of such a penalty.

a. The mechanism for liability

As a sanction for non performance of their obligations by the parties, and in particular those of the data importer, the contracts include penalty clauses in the event of one or both of the parties being in breach.

In practice, it is likely to be a data subject who will have a cause of action as the result of suffering loss or damage. In such an eventuality, it is important for the contracts to be clear as to whether or not there is joint and several liability as between the exporter and the importer: the existing models do not always contain adequate terminology (for example: the Preliminary draft on standard clauses, in the French version, speaks of "joint" liability, meaning in all likelihood "joint and several liability"; and see on this point Part II below).

The loss or damage suffered may take a number of different forms: an invasion of privacy as the result of the divulging of confidential data (for example: details relating to health), the refusal of a service on the basis of inaccurate information (for example: the reservation of a hotel room)… And, of course, the data subjects will be required to provide evidence of the alleged loss or damage.

Subject to this condition, the data subjects, as third parties to the contract between the exporter and the importer, are entitled to seek damages for breach of contract by virtue of the clause conferring rights on them as third parties (see Part II below).

The data exporter may also find that he has a cause of action for damages if he suffers loss or damage as the result of the misuse of the personal data by the importer (for example: a slur on the good name of the company as the result of a "case" concerning the distribution of those data.

b. The adequacy of the sanction

I would stress once again that contractual liability and the payment of damages to which it may give rise, is a mechanism that is not at all well adapted to the situation.

In fact, in this context loss and damage is often piecemeal and there are difficulties in proving both its existence and its extent, its causes being difficult to pin down… It is, moreover, not uncommon for the use of data in a manner beyond the terms of the contract, or breaches of security undertakings to have consequences that do not come to the notice of the data subjects for a long time.

One might well wonder, moreover, if the mere threat of having to pay damages for the loss or damage caused constitutes an adequate disincentive to prevent abuse.

A comparison with what happens under the domestic law of the exporter's country is useful in this respect: the processing of data is notified to the data protection authorities, who in turn have the means of investigation to bring to light any violation of the law (for the impossibility of taking such action in relation to the data importer, see Part II below); and in the event of any breach, they will normally impose penalties.

All this helps to ensure the enforcement of the legal provisions and provides an a priori means of penalising misconduct, quite apart from any claim for loss or damage on the part of any of the parties concerned.

There is, therefore, a fine line of distinction to be drawn between the means for implementing the data protection regulations where the data remain within one or more countries having an adequate level of protection, and recourse to contractual clauses within a third country in order to compensate for the lack of protection.

C. Conclusion of the contract

The conclusion of the contract will vary according to whether it is a contract of deposit ancillary to a service agreement or whether it takes the form of a standard contract for the licensing of data.

In the former case, the contract will continue over a period, often for some considerable time. At its conclusion legal relations with sub-contracted processors will be at an end and this will normally be marked by the return of the object that was in the possession of the other party – or, in the case of computerised data, by the destruction of the data, which is the equivalent.

In the second example, the contract is often required to be performed immediately, or at least is of fairly limited duration. At all events, the exporting of data has a feeling of permanence: the importer has contracted for the licensing of the data to him, in order that he may use them as he wishes. Certainly, he assumes general obligations in relation to the data, in particular to respect the purpose of the processing as originally declared. But the conclusion of the contract does not, in general, lead to the return of the data.

It may be useful, therefore, whatever the case in point, for the agreement between the parties to include the post-contractual period: in particular, the obligations that will continue to be binding (confidentiality, security…), together with any claims that may be brought subsequently.

II. Contracts for the transfer of data and relations with third parties

With contracts for the transfer of data, a number of third parties may be involved: first of all, the data subjects (A); then the third parties to whom the data are to be re-exported by the importer; and lastly, the national data protection authorities of the jurisdiction under whose authority the data come (C).

It will be readily appreciated that the fact that the third party is a third party to the contract for the transfer of data or simply a third party within the country of origin of the data can give rise to difficulties in implementing the contractual mechanism.

A. Data subjects

The position of third party data subjects is fundamental: they are at the heart of the provision, inasmuch as the contract is drawn up principally for their protection, where the country to which the data are being transferred is not sufficiently protective of their interests. It is, therefore, essential for the effectiveness of the provision that they be able to assert their rights in relation to the contract in question. This is ensured by a legal mechanism, that of the “clause conferring rights on a third party”.

Over and above this contractual process, the purpose of which is evident, there are statutory provisions deriving from data protection law to protect the data subjects: the data processing must have been declared to involve a transfer abroad (recipients of the data); and the 1995 directive would appear to require that the data subjects must have consented to such a transfer or, at the least, must have been notified of that possibility (see above, Part I).

Without straying from contract law, it should be emphasised that the concept of a clause conferring rights on a third party is not accepted to the same degree under different national laws (1). But to the extent that it is able to operate, such a concept enables the data subjects to require of a contracting party, in this instance the data importer, the fulfilment of the obligations set out in the contract (2). However, it should also be stressed that, in order to be able to take advantage of the clause, data subjects should be notified of the fact that they are covered by it (3).

1. Clause conferring rights on a third party for the benefit of data subjects

The clause conferring rights on a third party is a promise given by one of the parties to a contract, generally in exchange for an undertaking given by the other party, to provide a benefit to a third party. This mechanism is, for example, used in insurance: insurance taken out by the controller (covering goods being transported, which could be sold over and over again during that time: the benefit of the insurance will fall to the person who owns the goods at the time of the insured incident), life insurance (for the benefit of the surviving spouse, or born or unborn children)…

In contracts for the transfer of personal data, the importer gives a number of undertakings to the exporter, mainly in the matter of security, but also in relation to a third party: in particular, he undertakes to give right of access, of verification and of rectification to the data subjects.

The effectiveness of this type of undertaking will depend on the governing law.

The clause conferring rights on a third party is, in fact, recognised largely without restriction under the law of most European countries, for example under French law and German law, but it is not recognised in all of them. For many years it was an unknown concept to English law, in particular (see on this point T. Weir, An Introduction to Comparative Law, 2nd Edition, 1987, Volume II, from p. 145 for German law, from p. 148 for French law and from p. 151 for English law). Although it has now been recognised, under the Contracts (right of third parties) Act of 1999, some fairly strict conditions are laid down. In particular, under section 1, sub-section 3 of the Act, the third party covered by the clause must be expressly identified, or must be a “member of a class” or “answer a particular description”. It will be worth seeing whether the English courts consider that the subjects of automatic processing of personal data by a corporate body, which can involve data of an extremely diverse nature, constitute members of a class or answer a particular description.

Because of this divergence, the clause conferring rights to a third party does not feature in the provisions relating to international contracts adopted by Unidroit (cited above). The reasoning of English lawyers is that the contract cannot extend beyond the parties ("privity of contract") and that third parties offering no "consideration" cannot assert any rights under the contract.

On the other hand, systems recognising the concept of a clause conferring rights on a third party base their reasoning on contractual freedom, the absence of any prejudice to the third parties (the provision is to their advantage), together with the practical advantages of the mechanism.

The system of contracts for the transfer of data relying on undertakings entered into by the recipient companies, particularly towards data subjects, is, therefore, not effective under the law of all European countries.

2. The rights of data subjects by virtue of the clause conferring rights on a third party

Where the governing law – and, as we have seen, the contract should stipulate that this is the law of the country of the data exporter – recognises the concept of the clause conferring rights upon a third party, the latter will acquire rights under the contract in which he is included as a third party. In practice, the persons acquiring such rights will be the data subjects.

Such rights may take the form of enforcing the performance of the contract (in English law, "specific performance" or "performance in kind"), provided that the governing law recognises such right to enforce the contract (a). Otherwise, the right asserted will be an entitlement to damages (b), the principle of which has already been discussed, with emphasis on the fact that this type of sanction certainly fails to offer the necessary degree of effectiveness (see Part I above), and which leaves room for doubt as to whether it is joint and several liability as between exporter and importer or joint liability (c).

a. Specific performance: access, verification and right to rectify

The first thing that the data subjects will require will be the same rights of access, of verification and of rectification of the data concerning them as in their own country. The importer gives an undertaking to this effect in the commonly used contracts for the transfer of data.

There is no problem if the importer agrees to fulfil his undertakings, effectively giving the data subject the means of enforcing such rights. But where there is an unwillingness on his part, the question arises as to whether it is possible to obtain his compliance by means of a court injunction.

Here again we find a stumbling block in English law, which does not usually allow specific performance (see on this subject T. Weir, cited above, from p. 169), although it

would be available in Germany and in France. Here a certain trend of judicial reasoning under French law could be put to good effect, which, while it goes contrary to prevailing opinion, has recently been upheld: namely the assertion of Article 1142 of the Civil Code, according to which obligations to do or to refrain from doing something can be resolved in terms of damages.

However, in principle most European countries recognise specific performance of contracts, and if this principle is combined with the efficiency of the clause conferring a benefit on a third party, it would seem that as a matter of law the data subjects could, more often than not, assert their legal rights against the data importer for access, verification and rectification of the data relating to them.

b. Liability: penalty sanction in relation to undertakings given and compensation for loss or damage

Where he has failed to obtain satisfaction in asserting his rights, or where he has already suffered loss or damage, the third party data subject can seek redress from the exporter or the data importer. Such a right will depend to some degree, as far as the importer is concerned, on whether or not the governing law provides for the seeking of redress from a party to the contract by a third party: such is the case in countries recognising the validity of the clause conferring rights on a third party (see 1 above).

As we have already noted, this mechanism can prove less than effective in ensuring the efficiency of a data protection system which has to take account of the data concerned, the given purpose of the processing and the recipients of the data (see Part I above).

The right to damages remains, however, a mechanism that cannot be ignored when it comes to compensation for the loss or damage suffered. There will still remain, however, questions arising as to which law should apply.

The clause conferring rights on a third party would seem to favour contract law, and hence in principle, as was suggested, the law of the place in which the exporter of the processing is based, which will often coincide with the law of domicile of the data subject (an employee of the company, a customer within the country…) However, as this is loss or damage to the person, and not economic loss, some European countries might favour the concept of liability in tort. In this context, there is universal agreement that the law applicable is that of the country where the loss or damage arises: this could be either that of the country where the action took place (that of the importer) or that of the country where the harm was suffered (that of the victim)… With different consequences according to which one chooses

This question is rendered all the more vexed in that the rules governing liability are not identical in every country: some will be reluctant to grant damages for non-pecuniary damage, and in any event it might be difficult to obtain such damages under the law of contract…. Breaches of the regulations governing personal data might well give rise to damage of such a kind.

c. Types of liability: joint liability or joint and several liability

Another point that should be raised, which the contracts in common use do not always make clear, is the way in which exporters and importers are to be considered liable for any loss or damage incurred by a data subject: jointly or jointly and severally.

Part of the difficulty comes from the differences in vocabulary between one legal system and another. Thus, what French lawyers would term "solidairement responsable" becomes in English "jointly and severally liable".

There are two possible solutions and a clear choice must be made. The first is that of simple "joint" liability: each of two parties is responsible, on his side, for any loss or damage that he causes and, in the case of insolvency, neither will be responsible for the other. If, on the other hand, there is "joint and several" liability, each of the parties, importer and exporter, will be liable both for the loss or damage that he has caused and for that caused by the other and he will, in particular, be liable for making reparation where the other fails to do so.

The second solution appears more advantageous to data subjects and it would seem that in order to ensure the best protection by a mechanism that has already proved somewhat inadequate, the best option would be joint and several liability.

3. Awareness among data subjects of clauses conferring rights on third parties inserted in contracts for their benefit

A final comment must be made regarding the system of clauses conferring rights on third parties, namely that the beneficiaries of such clauses must be in a position to know that they have been inserted for their benefit in contracts between data exporters and importers. It is by no means certain that this is the case.

This line of enquiry brings us back to the question of how data subjects give their consent to transfers or how they are notified thereof (see Part I.A.1.b) above). If their consent for transfers to third countries was given right from the outset as soon as processing began (for example, where employees are concerned, when they are taken on and sign their work contract or, in the case of customer surveys, when customers send back questionnaires), it is clear that it would be appropriate to inform them at this stage about any clause conferring rights on third parties from which they might benefit, and possibly also about any data exporters who might be required to comply with such a clause. If, in the absence of initial consent, the data subjects are merely notified of transfers of data, any such notifications should also mention the existence of such clauses and give details of those who are required to comply with them.

This formal approach may seem unduly cumbersome, but it is difficult to see how it can be dispensed with if we want to ensure that the system of clauses conferring rights on third parties is not simply a theoretical mechanism with no practical effects.

B. Recipients of a re-exportation of data

Having accepted the premise that personal data forming the subject of a transfer can in turn be transferred to another country, the recipients of such a re-exportation will constitute third parties who maintain close relations with the initial transfer contract.

The very principle of such a transfer is, certainly, debatable (a) and, if it is agreed to, its implementation should be sharply delineated (b).

1. The possibility of re-exportation

The difficulty arises where the second transfer is to be made to yet another country not providing an adequate level of protection. In such an eventuality, everything will once again depend on contractual provisions. This in turn leads to an increase in risk for the data subjects, while their chances of being able to assert contractual rights against the new recipient of data diminishes.

The second recipient of the data is, in effect, third parties to the contract under which the transfer of the data abroad was originally made. This means that the data subjects cannot, without further authority, rely on the clause conferring rights on a third party that had been inserted in the contract for their benefit against the new recipient. For them to be able to assert contractual rights against him, the second contract for the transfer of data would also have to contain a clause conferring rights on a third party…. It is evident that as the contractual system becomes more complicated, so it becomes more fragile.

This is even more the case in that an additional difficulty arises in determining the law applying to the second contract: it would be sensible to make this the same as the law governing the first contract, which we suggested should be the law of the exporter's country, but this would be a law alien to the importer and the new recipient of the data…

It would therefore be advisable to restrict as far as possible, indeed, to prohibit, such re-exportations of data, particularly when they are sensitive, or semi-sensitive data.

There are some model contracts, however, that allow this with virtually no restrictions. Thus the Preliminary draft of a Commission decision on standard clauses for the transfer of personal data to third countries, December 2000 provides for such an eventuality by simply specifying that the new transfer can only be made with the prior written agreement of the data exporter (instrument cited above, at Article 6 (h)). And in the EEC-USA Agreement of 26 July 2000 such re-exportation is also allowed subject to a certain number of precautions (instrument cited above, under "Onward Transfer").

2. Conditions for re-exportation

The conditions for re-exportation must be examined from two perspectives: within the first contract and within the second contract.

In the first contract, a provision must be included that the data importer may not export them without ensuring that the new recipient of the data enters into the same undertakings as himself, both in relation to security and respect for the given purpose of the processing and in relation to the data subjects (access, rectification….).

In the second contract, the undertakings will be reiterated and a clause conferring rights on a third party will be included for the benefit of the data subjects. However, the efficiency of this will be exposed to the same judicial risks as we have already observed in examining this mechanism, inasmuch as the law of some countries does not recognise it.

Certainly, the best safeguard would be to include in the first contract a model for the second contract, which would give some measure of control over its contents. Such a model would deal with the delicate question of the governing law.

C. The data protection authorities

Mention should be made, finally, of a final category of third party: the data protection authorities.

These find themselves in a delicate position in regard to the transfer of data to a country not providing an adequate level of protection inasmuch as, in an exclusively contractual situation involving the controller of data, in this case the importer, they are bereft of their traditional powers of investigation, inquiry, injunction, prosecution…In fact, these are powers and prerogatives deriving from police law, and are thus restricted to the national territory.

Such powers could, in any event, only be used against the data exporter, within the national territory over which the authority has jurisdiction, or through his agent.

This point is made in commentaries to some contractual models. This is the case with the document Outsourcing and Privacy issued by the Privacy Advisory Committee of the United Kingdom, a document drawn up for the Commonwealth (cited above, 1994), where it is stated that in some examples of the export of data “there is usually and necessarily a substantial reduction in the control that an agency has over how the service is provided on a day-to-day basis.”.

III. The contract for the transfer of data and the settling of disputes

As with all international contracts, clauses relating to disputes have some degree of importance. They also have their weaknesses.

The commonly used models contain clauses specifying the governing law, the competent tribunal and, often, an arbitration and mediation procedure.

Such provisions are effective in relations between the parties (A), but have only a very limited relevance to relations with third parties (B), who are, nevertheless, at the heart of the clause.

A. Disputes between the parties

In relations between the parties, namely the data exporter and data importer, it is desirable to prescribe the governing law and the competent tribunal. An alternative is to submit to arbitration

It has already been emphasised that as far as the governing law is concerned, it would be wise to choose that of the country of origin of the data, that is to say, of a European country, as this will provide an adequate level of data protection (see above, under Introduction).

It should nevertheless be observed that it does not appear admissible, having regard to the rules of procedure and in particular the rules governing the right of defence, for there to be included in a model contract, as contemplated by the Preliminary draft of a Commission decision on standard clauses for the transfer of personal data to third countries, December 2000, a clause under which the data importer agrees to abide by the decisions of the data protection authority or a tribunal in the country of origin of the data (instrument cited above, Article 9 (2)).

It has been observed too that if the contract provides for a possible re-exportation by the data importer to another third country, this poses a further problem in determining the governing law for the new transfer and that it would be desirable to submit the whole contractual arrangement to a single jurisdiction: that of the first country of origin of the data (see Part II above).

However, it is not in relations between the parties that litigation poses the greatest threat.

B. Disputes with third parties

In relations with third parties, dispute clauses are likely to be of very limited effect. Third parties, in fact, are not bound by the undertakings assumed by the parties in regard to them. The determination of the governing law, or of the competent tribunal, will therefore be difficult to impose on data subjects, for example, in the event of a dispute.

It could, of course, be argued that data subjects would not be able to take advantage of the clause in the contract conferring rights on a third party while at the same time repudiating the clause governing the settlement of disputes. However, a third party who has fallen victim to a malfunctioning of data protection could easily challenge that argument by saying that his case was brought not under the law of contract, but as the result of the breach of the duty of care owed towards him under the law of torts.

The same argument would apply to arbitration clauses. They cannot bind third parties, and in particular data subjects. And if recourse is to be had to this method of settling disputes, it will have to be done on the basis of a compromise between the data controllers and the victim after the action has been brought.

General conclusions

This analysis of the possibilities of harnessing the phenomenon of the international transfer of personal data by contractual clauses, in particular in the context of contract law, has brought to light a number of weaknesses within the system.

On the one hand, it has been seen that even if the undertakings usually included in model contracts make it possible to give some assurance with regard to data security and the respecting a number of principles (given purpose, access, rectification….), the concept of the clause conferring rights on a third party, which is indispensable in enabling data subjects to exert their rights, contains weaknesses inasmuch as legal systems do not always accept it without restriction, and in the event of a re-exportation of data to a second third country the need to reiterate the clause conferring rights on a third party renders the system somewhat complex.

On the other hand, and above all, it has been shown that the contract mechanism is rather badly adapted to safeguarding the efficiency of regulations that mainly derive from police law, and consequently should be enforceable by data protection authorities able to investigate and penalise, whereas under contract law, the penalty for acts of bad faith on the part of data controllers mainly consists of the right of data subjects, in the event of their suffering loss or damage, to obtain reparation through the award of damages.

Jérôme HUET
Professor of Law
21 January 2001