AN AMERICAN SOLUTION TO TBDF PERSONAL DATA CONTRACTUAL PROBLEMS

A group of experts under the auspices of the Council of Europe and the European Commission has examined contractual solutions to the problem of safeguarding transborder data flows of personal data and maintaining data subject rights when the data has arrived at the country (or countries) to which it has been transferred. The group has circulated for comment a draft agreement to ensure "equivalent" data protection for personal information (see PL&B October '91, p.6). We asked for your commments. Joel R Reidenberg, Associate Professor, Fordham University School of Law, New York, has responded with a United States perspective.

Among the resolved points, three sets of critical issues have been identified:

1. The enforceability of data subject rights
2. The dissuasive cost of private litigation
3. The spectre of foreign litigation

For these issues, American contract law may offer a few solutions that could be incorporated in the model agreement.

The contractual approach however, appears unworkable to ensure "equivalence" for transborder data flows occurring on global information networks. The model agreement is likely to be viable only for simple point-to-point transfers.

Data Subject Rights

The contractual approach contemplates an agreement between the entity transferring personal information and the recipient. Data subjects are third party beneficiaries; the agreement creates obligations for their benefit, but they are not signatories. Because some countries may not allow third party beneficiaries to seek legal redress, data subjects may be unable either to enforce the contractual provisions on data protection or sue for damages in the event of breach.

Under prevailing American contract law, however, third parties may sue when they are "intended" beneficiaries of the contract. Consequently, provisions between the transferor and the recipient of personal information can grant the data subject enforceable rights. Although the model agreement does not specifically provide in Article 1 that the information processing obligations protect data subjects, the purpose of the contract is to make them the intended beneficiaries of data protection rights. As a drafting matter, the model agreement could clearly state in Article 1 that the data protection principles are for the benefit of data subjects.

Notification of Data Subject

For data subject rights to vest fully and not be modifiable by the contracting parties, US contract law requires that data subjects be notified of the agreement. The model agreement could satisfy this concern with a provision requiring notification of data subjects.

Choice of Law

In order to use the American legal doctrine, US contract law must be able to govern the agreement between the transferor and recipient. The relationship between the data transfer and the United States as well as the willingness of Data Protection Authorities to accept a choice of foreign law will, thus, be critical for the viability of this solution. If US law can be applied to the contract, the model agreement would need a choice of law provision in addition to the existing arbitration clause in Article 5.

Using a DPA as a party to the contract

If use of US law is not possible, another solution might be to include the national Data Protection Authority as a party to the contract. As a signatory to the contract, the DPA would represent the interests of data subjects. In its capacity as a direct party, the DPA might then be able to safeguard the data subject rights.

Dissuasive Costs - a Contractual Solution

The fear that a data subject may be dissuaded from enforcing privacy rights because of expensive legal fees and the difficulty of establishing monetary damages can be resolved contractually. The addition of two provisions in the model agreement would significantly reduce these cost disincentives:

1. **Attorney's Fee Clause:** In contract litigation, American courts are reluctant to award legal fees to the winner. Yet, if the contract makes a specific provision for attorney's fees, these same courts generally will enforce the agreed allocation of legal expenses. Thus, the model agreement can stipulate that the victorious data subject recovers legal fees, thereby eliminating the cost of litigation for the meritorious claim.
2. **Liquidated Damages Clause:** Under appropriate circumstances, American courts will recognise contractual provisions that stipulate a fixed sum of money to be paid in the event of breach. Because the courts refuse to enforce contractual penalties, three conditions must be met for a "liquidated damages" clause to be valid:

- the actual damages resulting from breach are uncertain or difficult to prove.
- the parties intended to identify the damages in advance.
- the amount stipulated is reasonable and not disproportionate to the injury.

These conditions can be met for infringements of data protection obligations.

The model agreement already contains a clause in Article 6 awarding a specific sum of money if the recipient fails to destroy the data upon termination of the contract. This clause could be expanded to spell out liquidated damages for data subjects in the event of a recipient's breach of the data protection obligations.

Foreign Enforcement - Role for DPA's

Under the model agreement, local data subjects may also face the practical difficulty of foreign litigation or arbitration. This may be avoided by an additional "choice of forum" clause in the model agreement that permits suit or arbitration in the exporting jurisdiction. If the Data Protection Authority were a party to the contract representing data subject rights, then foreign enforcement or arbitration would be less problematic and a forum stipulation would not be critical.

Privacy "Equivalence" Problematical for International Networks

Even though these critical issues may be addressed in the agreement, the contractual approach focusses on simple cross-border data transfers such as the Fiat scenario or similar back-office consolidations. For sophisticated data processing arrangements, the contractual approach does not appear viable.

Simple Data Transfers

The model agreement assumes that data processing arrangements involve only three parties: the data transferor, the data recipient and the data subject. The model text, for example, does not refer at all to the possibility of "subtransferring."

Complex Data Transfers

An international data transfer is likely to pass through various intermediate data processing entities such as telecommunications service providers. These intermediate service providers may also make subtransfers of personal information. For the contractual approach to be viable in these circumstances, a vertical chain of agreements would be required. Each intermediate and sub-entity would need to execute agreements either directly or in an unbroken chain with the transferor or the recipient.

The mechanics of arranging a series of subtransfer agreements are likely to be onerous both in terms of cost and business policy, particularly if businesses will be required to

disclose various corporate alliances either to other companies involved in the data transfer or to Data Protection Authorities.

In the context of global information networks where multiple parties may share information and may also in turn subcontract data processing (e.g. computer reservation systems or cash machine networks), the contractual approach seems rather unwieldly. Under the model approach, each member of the network would be required to sign a contract with every other member of the network and every subcontractor.

A Model "Network Agreement"

An alternative might be a model "network agreement." Yet, one can imagine a host of difficulties demarcating information processing responsibility, identifying violations of data protection and settling disputes. In the end, some of the perceived difficulties with the contractual approach might be resolved by the model agreement. But, the approach itself appears to be a limited starting point for TBDF equivalence.

Joel R Reidenberg, Associate Professor of Law, Fordham University, New York, USA

DATA COMMISSIONERS SET PRE-CONDITIONS FOR POLICE USE OF INTERNATIONAL DATA

The Data Protection Commissioners of Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom have demanded adequate national data protection arrangements as a pre-condition before the Schengen Agreement enters into force. These decisions resulted from their meeting on international police cooperation held in The Hague on November 28/29.

The Commissioners' Conference gave special attention to the Convention applying the Schengen Agreement, as this Convention is an important precedent for similar developments regarding the free movement of peple within the framework of the 12 EC countries forming the Single European Market.

The establishment of a Schengen Information System, and a variety of other arrangements concerning data transmission for police use, as provided for in the Convention, will result in a considerable increase of personal data flowing across national borders.

Pre-Conditions for Police Use of Data from other Countries

As a result, a coherent system of data protection provisions has been created which have to be met before the Convention enters into force, expected on March 1, 1993.

The transmission of personal data, through the Schengen Information System or according to other arrangements in the Convention, may take place only when each Contracting Party has taken, when the Convention enters into force at the latest, the necessary measures to achieve a level of personal data protection at least equal to that resulting from the principles of the *Council of Europe Data Protection Convention*. In particular, the Commissioners state that these national arrangements have to be in compliance with the *Council of Europe Recommendation* R (87) 15 of 17 September 1987 *regulating the use of personal data in the police sector.* (Both these documents are available from the PL&B office).

The Convention also provides for the designation of independent national supervisory authorities for the national sections of the Schengen Information System, and for a joint supervisory authority for the central technical support function.

Conference decisions

The Conference, noting that these developments are taking place and that not all of the Convention's Contracting Parties have yet fulfilled the relevant data protection conditions, stressed the need for:

1. *adequate national arrangements on data protection as an absolute condition* before the Convention enters into force.
2. *adequate data protection arrangements in relation to the development of essential parts of the Schengen Information System* before the Convention enters into force.

In addition, the *Data Protection Commissioners of the Contracting Parties* (Belgium, France, Germany, Luxembourg and the Netherlands) have decided to establish an *ad-hoc working group* - before the Convention enters into force - in order to facilitate the necessary consultation between them with regard to the relevant parts of the Convention as well as on all organisational matters related to its operation.

This edited report was submitted by Alexander Singewald, Information Manager, the Registratiekamer, the Netherlands Data Protection Authority.