

ENSURING INTERNATIONAL PERSONNEL DATABASES COMPLY WITH NATIONAL LAWS

Will a contract between a company and its employees ensure that data protection principles are observed in the development and use of an international personnel database? More generally, what are the advantages and disadvantages of this approach in the regulation of transborder data flows?

Professor Brian Napier addressed these issues at the Council of Europe/European Community Conference in Luxembourg 27-28th March (PL&B December '89 p.3) and at the June 14th Privacy Laws & Business conference on the impact of the Council of Europe Recommendation on Employment Data. Dr. Ken Cooke skillfully summarises Professor Napier's main points.

The problem of trans-border flows of personal data is one which arises not only in relation to employment but also to many other areas. It has proved difficult to regulate international data flows through domestic legislation and the view that between ratifying countries "problems should not arise in practice" is over-optimistic. (Paragraph 62, Council of Europe Recommendation on the Protection of Personal Data used for Employment Purposes). Problems arise even where the data exporting and importing countries have ratified the Recommendation, but where this has not been done the position is even more difficult.

1. Powers of the UK Data Protection Registrar

The Registrar has power under section 12 of the Data Protection Act to prohibit the export of data but has never done so to date. By contrast, the exporting of personal data has frequently been prohibited in Scandinavia and France by its Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL).

In France, the CNIL has pressed the case for trans-national flows to be governed by a contract between the importer and exporter in the absence of which the Registrar in the exporting country should (or may) disallow the transfer. Does the UK Registrar have powers to intervene where a contract exists between the importer and exporter? Arguably he does not and, in any event, he is likely to be strongly influenced by the existence of a contract which incorporates sufficient guarantees protecting the interest of the data subject.

2. Contractual Guarantees

Even where such guarantees are incorporated into contracts for the import and export of data, how can such guarantees be enforced by the data subjects who are not parties to them? One answer would be to argue that when the data exporter enters into a contract it does so as the data subject's agent. Even so, in the absence of any form of statutory assistance with legal costs, it would be very difficult for an individual data subject to enforce any rights he or she may have.

3. An Alternative Solution

It may be possible to circumvent the difficulties which arise in attempting to regulate data flows contractually by the creation of administrative controls. One suggestion would be the establishment of an adjudicatory body drawn from the national data protection authorities whose function would be to decide whether there had been misuse following a trans-border data flow. This procedure would follow the well established system of adjudication in international contracts by the International Chamber of Commerce. The advantage would be to take adjudication out of the courts.

Professor Brian Napier is Head of the Information Technology Law Unit, at the Centre for Commercial Law Studies, Queen Mary and Westfield College, University of London. He prepared a 39 page paper for the Luxembourg conference covering the above issues. Its title is "Contractual Solutions to the Problem of Equivalent Data Protection in Transborder Data Flows." This paper is available from the PL&B office.

Dr. K. R. Cooke is a member of the Intellectual Property Department of Dibb Lupton Broomhead & Prior, Solicitors, Leeds, England.

The papers from the Privacy Laws & Business June conference on Employment are also available from PL & B.