



Privacy & Data Protection

Volume 5, Issue 3

January / February 2005

Headlines:

- Marketing emails breach the ASA's code, p.13
- Canada safe for airline data, p.14
- Tesco's—boycott over privacy issues p.15

Inside this issue:

- The alternative model clauses—pragmatism at heart 3
- Implementing codes of conduct 5
- The data protection implications of data rooms—Part II 8
- US privacy update 11
- News & Views 13

New 'model contract' approved for data exports

In an attempt to promote greater use of 'model contractual clauses,' the European Commission has approved a new contract for the transfer of personal data to countries outside the European Union.

Model clauses are one method of circumnavigating the export ban contained in the 8th Data Protection Principle, which provides that,

Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory has an adequate level of protection for the rights and freedoms of data subjects.

The new set of clauses, which apply only to exports to 'data controllers,' and,

therefore, do not cover outsourcing arrangements, were formed after pressure was brought on the Commission by a coalition of organisations including the International Chamber of Commerce and the Japan Business Council in Europe.

According to Eduardo Ustaran, data protection lawyer at Field Fisher Waterhouse, "from a commercial perspective, the new clauses make a lot more sense than the original ones. My prediction is that they will prove very popular. What we need now is a similar set dealing with transfers to data processors such as offshore service providers."

The new clauses do away with joint and several liability—the main sticking point in the previous set. Instead,

they make the data exporter and data importer liable to individual data subjects for their own breaches of the export contract.

Further, the data exporter must check that the importer is able to fulfil its obligations under the contract—in so doing, it can either carry out an audit at the importer's premises, or it can request evidence from the importer of sufficient financial resources to meet any relevant liability that it may face.

David Griffiths, of Clifford Chance, told *Privacy & Data Protection* that, "companies will welcome the new liability regime. Under the new clauses, data exporting companies are not jointly and severally liable for

(Continued on page 13)

Enforcement to be beefed up

Pressure to bring data protection enforcement actions is being brought to bear on European countries.

The influential Article 29 Working Party, the body responsible for the harmonisation of data protection laws in the EU Member States, has stated that it intends to "further develop the enforcement of national data protection legislation ... in order to enhance harmonised compliance."

In a Declaration adopted in late 2004, the Working Party commits itself to developing

"proactive enforcement strategies" and "increasing enforcement actions."

The move will be interpreted as the Working Party running out of patience with those Member States that do not have an active and publicly visible enforcement regime.

In previous reports, the European Commission has noted three undesirable and related phenomena:

- very patchy compliance by data controllers who perceive the risks of get-

ting caught for poor compliance to be very low

- national data protection authorities that give low priority to enforcement action; and
- a low level of knowledge by data subjects of their data protection rights.

The Working Party states in its Declaration that, in order to achieve compliance with data protection law, the imposition of sanctions at a national level could now be necessary.

(Continued on page 13)