www.privacydataprotection.com

ISSN 1473-3498

Privacy & Data Protection

Volume 6, Issue 3

January / February 2006

Headlines:

- Data risks of 'rich lists,' p.14
- Guidance on employee references, p.14
- Private detective fined, p.15

Inside this issue:

Call for stricter approach to foreign data transfers

The EU Data Protection Working Party has called for greater consistency in application of the EU's data export laws and for a stricter interpretation of the derogations from the export ban.

It has also indicated that only very rarely will 'consent' and 'contractual necessity' be available to legitimise data exports.

Citing a lack of harmonisation between Member States and a lack of understanding by data controllers of the restrictions on transferring data overseas, the Working Party stated that it would "like to ensure that the scope and meaning of Article 26(1) are well understood by all those concerned to avoid the use by controllers of the derogations in inappropriate cases. This requires a clear and common interpretation of Article 26(1) itself, and of its position in the Directive as a whole."

Article 26(1) of the Directive allows data transfers to countries that do not have adequate data protection laws (i.e. most non-EU countries).

According to the Working Party, the derogations in Article 26(1) are used by controllers too frequently and should be considered only where the three legitimising methods of binding corporate rules, contractual clauses and safe harbor (Article 26(2) methods) have been found virtually impossible to utilise.

Only if those are truly not feasible should the data controller consider using the derogations of Article 26(1), namely:

- Consent
- Contractual necessity
- Public interest and legal claims
- Vital interests of the individual
- Information on a public register

The Working Party recommends that "the deroga-

(Continued on page 14)

De Vere hotel in data blunder

Thousands of documents revealing the credit card numbers, addresses, phone numbers and signatures of guests were dumped in an open skip by one of Britain's best-known hotels.

The owner of the Grand Hotel in Brighton was forced to apologise after staff threw out registration forms and credit card slips of thousands of guests, including those of several MPs.

The Information Commissioner's Office said it believed the hotel had breached the Data Protection Act, while several MPs said they would be asking questions in parliament to determine if consumers needed further safeguards to protect them from negligent companies.

Brighton residents walking past the city centre hotel in early January were amazed to see a skip full of registration cards of guests who stayed at the hotel between 1998 and 2000. Each one listed the name, company, home address and credit card number in full. Most included a home phone number, and in the case of some foreign guests, passport numbers.

After sitting in the street for 24 hours, open to any passerby, the skip was removed.

Although in most cases the credit cards have expired, many of the guests will still possess cards bearing the same number. Many will be living at the same addresses.

One fraud expert observed that the information in the wrong hands could be very dangerous. Although the credit card numbers in themselves are not hugely damaging, combined with

(Continued on page 14)