pdp JOURNALS

ISSN 1473-3498

Privacy & Data Protection

Volume 12, Issue 8 September 2012

Headlines

- Body fined £250,000 for failing to have data processor contract, p.17
- Campaign group calls for schools to come clean about toilet CCTV, p.18
- Swiss watchdog in row about workers' privacy, p.19

Contents

EU privacy chief erupts over asylum seekers database

A row between the European Commission and the European Data Protection Supervisor has broken out over plans to give police access to biometric data from the fingerprints of asylum seekers.

The controversy centres on the role of EURODAC, the EU-wide fingerprint database. The database was originally created in 2000 to prevent multiple claims for asylum being lodged in different Member States, with no country taking responsibility for the application. The establishment of the database was accompanied by specific safeguards that data are not used for other purposes.

In May 2012, the Commission adopted a proposal concerning a recast of the EURODAC Regulation, allowing national law enforcement authorities and the European police service, Europol, to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences.

The change would have the result that, if a fingerprint is found at a crime scene, asylum seekers could potentially be identified through EURODAC data while other individuals could not because of a lack of availability of similar data on all other groups of society.

In his 20 page report, Peter Hustinx accused the European Commission of failing to provide sufficient evidence and justification for the plans, stating that the Commission should prepare a fresh impact assessment "in which solid evidence and reliable statistics are provided and which includes a fundamental rights assessment."

The EDPS said "just

(Continued on page 17)

Compliance can be suspended for data put 'beyond use'

The UK regulator has produced new guidance on data deletion which is important for all organisations doing business in the UK.

The guidance sets out how organisations can ensure compliance with the Fifth Data Protection Principle (to do with data retention) in UK law when archiving or deleting personal information. It also explains what the Information Commissioner's Office means by deletion, archiving and putting personal data 'beyond use'.

The guidance acknowledges that information can be put 'beyond use' without actually being deleted. In those circumstances, data protection compliance may be 'suspended' where certain safeguards are met.

The ICO gives specific examples of where putting information 'beyond use' would be an acceptable alternative to 'deletion'. For example, it may arise where, for technical reasons, it is not possible to delete the information without also deleting other information

(Continued on page 17)