pdp JOURNALS

ISSN 2049-5307

Privacy & Data Protection

Volume 14, Issue 5 April / May 2014

Headlines

- Survey of SMEs reveals compliance motivations, p.18
- New Opinion on breach notification, p.18
- First sites admit to data losses resulting from Heartbleed attacks, p.19

Contents

Uncertainty for EU ISPs as Court declares retention law invalid

The Court of Justice of the European Union has ruled that the European Data Retention Directive 2006 is illegal and invalid, creating uncertainty for ISPs and telecom providers in the EU that have been collecting and storing user data since the 2006 law was enacted.

Directive 2006/24/EC was adopted in the aftermath of terrorist attacks in Madrid and London. The law required telecom providers in EU Member States to hold on to data about their users' traffic and location for two years.

Individual Member States were required to implement the Directive into national legislation.

The law was controversial at the outset, with various Member State governments, including Germany, refusing to implement it on the basis that it was fundamentally incompatible with national law.

The case came to the European Court following requests from Irish and Austrian courts which asked for an examination of the Directive's compatibility with human rights law.

According to the ruling, the law violated fundamental rights to respect for private life and to the protection of personal data, because it does not sufficiently limit the instances in which authorities can access the collected information.

The Court identified five specific failings in the Data Retention Directive:

- it covers all individuals, all means of communication and all traffic data, without limitation;
- it fails to set out the criteria that national law enforcement

(Continued on page 17)

CNIL gets new inspection powers affecting all companies selling goods to French

The French Data Protection Act has been amended to give the data protection regulator, the CNIL, the right to remotely detect and react to data breaches on the internet.

Until now, the CNIL's powers of investigation have extended to the following:

- on-site inspections, during which its agents can visit company facilities and have access to servers, computers, devices and applications that have the capacity to store data;
- document reviews, which allow the CNIL to obtain from a company disclosure of any documents or files, through a written request; and
- hearings, which allow CNIL agents to summon any individual in connection with an investigation.

The new powers enable the CNIL to verify all data that are made freely available on the internet, without any restriction.

The powers do not allow the CNIL to override or break companies' security to gain entry into their information systems.

(Continued on page 17)