pdp® JOURNALS

Data Protection Ireland

Volume 6, Issue 5 September / October 2013

Headlines

- 2 million customers affected by Vodafone Germany hack, p.17
- Global Internet Sweep identifies best practice for online companies, p.18
- Reworked DNA Bill published, p.19

Contents

Working Party asks — is 'Safe Harbor' still safe?

EU data regulators have voiced concerns about whether EU privacy rules have been breached by secret US surveillance programmes, raising questions as to whether the US/EU Safe Harbor agreement is still effectual.

In a letter to EU Justice Commissioner, Viviane Reding, Jacob Kohnstamm, Chairman of the Article 29 Working Party, questioned how organisations could comply with information requests issued under the USA Patriot Act, the FISA Amendment Act, and Executive Order 1233, while still fulfilling the conditions for the transfer of personal data to third countries. He stated: "The Safe Harbor Principles indeed do allow for a limitation of adherence to the Principles 'to the extent necessary to meet national security...requirements'.

"However, the WP29 has doubts whether the seemingly large-scale and structural surveillance of personal data that has now emerged can still be considered an exception strictly limited to the extent necessary".

Kohnstamm noted that competent authorities in Member States may suspend data flows under Article 3.1 (b) of the Commission Decision on the Safe Harbor principles "in cases where there is a substantial likelihood that the [Safe Harbor] Principles are being violated and where the continuing transfer would create an imminent risk of grave harm to data subjects".

The concerns are the latest in a growing group of voices in the EU to question whether Safe Harbor is working.

(Continued on page 17)

New breach reporting rules for ISPs and telecoms — now in force

New European Union Regulations requiring telecoms operators and internet service providers ('ISPs') to notify national authorities within 24 hours of detection if there has been any theft, loss or unauthorised access to customer data are now (as from 25th August 2013) in force.

The new rules follow the publication on 26th June 2013 in the Official Journal of the European Union of a new Regulation on what telecoms and ISPs should do if their customers' personal data are lost, stolen or otherwise compromised.

Because the technical implementing measures were adopted as a Regulation, they have direct effect in Member States (i.e. they do not require an implementation into the national law).
The rules are separate and distinct from the draft Data Protection Regulation and draft Directive on network and information security. However, they are understood to be a 'foretaste' of what the Commission plans in the reform package.

The purpose of the new rules is to ensure that businesses operating in more than one EU country can take a pan-EU approach in the event of a data breach.

Since 2011, telecoms

(Continued on page 17)