

# Privacy & Data Protection

Volume 17, Issue 7

July / August 2017

## Headlines

- Industry group issues guidance on GDPR legitimate interests, p.18
- Australia to get RIPA style law later this year, p.19
- UK government approves major changes in use of health data, p.20

## Contents

<i>Expert comment</i>	2
<i>GDPR series: Data security and response planning</i>	3
<i>PDP Resource: List of monetary penalties levied by UK Information Commissioner</i>	8
<i>China's new Cybersecurity Law: what you need to know</i>	14
<i>News &amp; Views</i>	17

## Brexit plans need work, says Committee

The UK government's plans for sharing data with the EU following Brexit are significantly lacking in detail, according to a new report from the House of Lords EU Select Committee. The report says that much more thought is needed to prevent a breakdown in business and security communications.

The UK government has indicated its intention to secure 'unhindered' and 'uninterrupted' flows of data between UK and EU after Brexit. But peers are 'struck by the lack of detail in the government's assurances thus far'.

One of the Committee's concerns is the UK's ability to tackle crime. It said that any friction around data transfers after Britain leaves the EU 'could hinder police and security co-operation', and law enforcement bodies could lose access to information and intelligence mechanisms. Such mechanisms are currently guaranteed through the UK's membership of Eurojust and Europol.

The report also warned that haziness governing the legitimacy of transfers will affect the UK's competitive status in interna-

tional trade. Peers said being able to move data is especially important given the UK economy's dependence on the services sector — around half of Britain's trade in services is 'enabled by digital technologies and the associated data flows', and three-quarters of all UK data shared across borders is with EU countries.

Michael Jay, the peer who chairs the Committee said: "The government says the right things but we have had no evidence yet that it sees the potential seriousness of Brexit

[\(Continued on page 17\)](#)

## Clampdown on social media job snoops

Employers need a legal ground to justify vetting potential job candidates on the basis of their Facebook and Twitter profiles, the EU regulators have said.

The Article 29 Working Party gave the view in its recently released Opinion on data processing at work, which aims to provide guidance on balancing employee privacy expectations in the work-

place with employers' legitimate interests in processing employee data.

The Opinion (which like other opinions isn't legally binding) is applicable to all types of employees and not just those under an employment contract. It is to be read in conjunction with the Working Party's previous Opinion 08/2001 on the processing of

personal data in the employment context and Working document on the surveillance of electronic communications in the workplace.

Page 11 of the Opinion deals with the recruitment process. It states that employers should not assume that merely because an individual's social media profile is

[\(Continued on page 17\)](#)