

Data Protection Ireland

Volume 10, Issue 4

July / August 2017

Headlines

- AG supports student in 8 year battle over exam scripts, p.18
- Most Irish business unprepared for new rules, p.19
- New powers for EU law enforcement to access data, p.20

Contents

<i>Expert comment</i>	2
<i>GDPR series: Data security and response planning</i>	4
<i>GDPR series: demystifying DPIAs</i>	9
<i>US broadband privacy rules — troubling times ahead</i>	12
<i>China's new cyber-security law: what you need to know</i>	14
<i>News & Views</i>	17

Resolve urgent deficiencies with Shield, says Committee

“Deficiencies must be urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses”, said the European Parliament’s Civil Liberties, Justice and Home Affairs Committee (LIBE), which recently met the US administration responsible for administering the EU-US Privacy Shield.

The MEPs met with the US Departments of State, Justice, Treasury, Homeland Security and Commerce, as well as the Federal Trade Commission, Congressional representatives, academics and representatives of

civil society. Both sides reiterated their continued commitment to make the agreement work, but MEPs highlighted various issues to be addressed:

“As already emphasized by the European Parliament in April, several key positions still need to be filled under the new US administration in order to meet the conditions of the adequacy decision. These would include some of the necessary functions of the Federal Trade Commission, the Privacy and Civil Liberties Oversight Board that is currently lacking four of its five commissioners

and the Ombudsperson, who is currently only in an acting capacity,” said Claude Moraes, Chair of the Committee.

MEPs also drew attention to open questions on the commercial aspects of the Privacy Shield, as well as the ongoing review of Section 702 of the Foreign Intelligence Surveillance Act, Presidential Policy Directive 28 and law enforcement issues — all essential components of the US commitments.

The MEPs said that its

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

EU DPAs tell employers: ‘stop snooping on employees’

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 workplace 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 publicly available, they are then allowed to

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