

# Privacy & Data Protection

Volume 18, Issue 2

December 2017

## Headlines

- UK government seeks views on updates to communications regime, p.17
- Lords want to see an ethics code of practice for data controllers, p.19
- Tech companies want the ICO on EU data protection board following Brexit, p.20

## Contents

<i>Expert comment</i>	2
<i>E-privacy in Europe — changes afoot</i>	4
<i>IDTs— transparency, adequacy and GDPR derogations</i>	8
<i>Group actions for data breaches — the case of Morrisons supermarket</i>	10
<i>GDPR series: International data transfers — a high level review</i>	14
<i>News &amp; Views</i>	17

## EU DPAs to go after Uber

The Article 29 Working Party has established a taskforce to coordinate the multiple national investigations into Uber’s 2016 data breach that affected approximately 57 million users worldwide.

According to the latest figures, approximately 2.7 million UK user accounts were among those affected, and compromised details included names, mobile phone numbers and email addresses. Uber had initially kept the breach a secret, paying hackers £75,000 to delete the data. The taxi company did not provide any information about the hacker or how he was paid. It has now emerged that the hacking may have

been the work of a 20-year-old Florida man, who was paid by the ride-hailing company to destroy the information through Uber’s bug bounty programme.

The taskforce, which includes representatives from the DPAs in the UK, France, Italy, Germany, Belgium and Spain, is being led by the regulator in the Netherlands where Uber is headquartered. It will not have the power to impose joint sanctions on the company and investigations will still be conducted at national level. The maximum fine that may be imposed in the UK is £500,000. In the Netherlands, where concealing a breach is illegal,

the maximum fine is €820,000. And in Italy, the only EU country to have announced a full-blown investigation into the Uber incident, the fine may be more than \$1 million, with the amount being related to the number of Italians who were affected.

Previous examples of coordinated actions by the EU’s privacy regulators include the tackling of Google over its unified privacy policy—an action that forced Google to give clearer information to users across the world—and a recently-formed taskforce that’s looking into Facebook’s promise-breaking absorption of

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

## Working Party threatens to take legal action over Privacy Shield

Data protection authorities in the EU have threatened to initiate a legal challenge against the European Commission’s decision to endorse the EU-US Privacy Shield unless their ‘prioritised concerns’ about the framework are not addressed by 25th May 2018.

In a newly published Opinion on the Shield, the Article 29 Working Party, which consists of the head of each Member State’s

DPA, outlined its concerns and called upon the Commission and the US competent authorities to restart discussions.

“An action plan has to be set up immediately in order to demonstrate that all these concerns will be addressed”, said the Working Party. “In case no remedy is brought to the concerns of the Working Party in the given time frames, members will take appro-

priate action, including bringing the Privacy Shield adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling,” it added.

A copy of the Working Party’s Opinion is available at: [www.pdpjournals.com/docs/887846](http://www.pdpjournals.com/docs/887846)

The Shield was discussed

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