

Privacy & Data Protection

Volume 15, Issue 5

April / May 2015

Headlines

- Australia: controversial metadata law passed and Commissioner enforces new data retention rules, p.17
- Amazon cloud contract terms meet EU standards on data transfers, p.19
- FTC signs MoU with Dutch regulator, p.20

Contents

<i>Expert comment</i>	2
<i>The EU cookie compliance sweep — lessons to be learned</i>	3
<i>Sensitive personal data — current and future</i>	6
<i>Avoiding and dealing with Monetary Penalty Notices</i>	8
<i>PDP Resource — updated list of fines</i>	11
<i>Data privacy and cyber risk in M&As — are you prepared?</i>	13
<i>News & Views</i>	17

CNIL makes it easier for company groups to transfer data abroad

The French data protection regulator has changed the process by which it grants approvals for Binding Corporate Rules, making it significantly easier for companies to obtain authorisation for intragroup data transfers.

The regulator has said that for each group that has adopted BCRs, it will define and provide content for 'single authorisations', which all companies within a group can then rely on for their transfers.

Once contacted by the CNIL, the group entity is required to complete

a 'compliance commitment' form on CNIL's website declaring that its international data flows framed by the BCR comply with the single authorisation granted to the group.

Following that, the organisation's data controller is required to maintain an up-to-date list of each transfer, to be communicated to CNIL upon request, containing the following:

- general purpose of each transfer;
- categories of data subjects affected by the data transfer;
- categories of personal

data transferred;

- information on each data recipient, including company name, company group to which it belongs and type of BCR adopted; and;
- country of establishment, categories of recipients and nature of the processing operated by the recipient.

The time it takes for the first single authorisation to be granted will depend on how long the organisation takes to respond to the CNIL, and they may contact the CNIL by telephone if necessary.

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

Google decision leaves data controllers 'exposed and vulnerable'

In a landmark decision, the UK Court of Appeal has ruled (in *Google Inc. v Vidal-Hall and Others*) that there is a tort of 'misuse of private information' and that any company breaching it is liable to pay damages without claimants having to show 'harm'.

The decision potentially has huge implications on the ability for data sub-

jects to take direct action against companies for misusing their data.

The case came to the Court following the collection by Google of 'browser generated information' or 'BGI' — used by the company to more effectively target advertising. Apple Safari users had not given their consent to the collection of their BGI data.

The Claimants brought claims for misuse of private information, breach of confidence and breach of the UK Data Protection Act, seeking damages under section 13.

The Court (which was considering the case prior to the full trial) was asked to look at whether misuse

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