Osborne Clarke is one of Europe's most respected law firms and a UK leader in advising marketers on the legal issues affecting them. The firm's blog, MarketingLaw.co.uk, has provided marketers with authoritative legal insights for over 15 years. Please send any queries regarding this column to Stephen Groom (Stephen.groom@osborneclarke.com)

Legal and Regulatory Update

World privacy authorities warn leading Appstores

Daisy Jones

Journal of Direct, Data and Digital Marketing Practice (2015) **16**, 225–226. doi:10.1057/dddmp.2015.9

Who: Twenty-three National Data Protection Authorities (DPAs) involved in the Global Privacy Enforcement Network, including the DPAs for Australia, Canada, France, various German DPAs, Israel and South Korea.

Apple, Google, Samsung, Microsoft, Nokia, Blackberry and Amazon.com (the 'Appstores')

Where: Worldwide

When: 9 December 2014

Law stated as at: 12 January 2015

What happened

On 9 December 2014, the Data Protection Authorities (DPAs) sent an open letter to the Appstores, the largest global app marketplaces, asking them to make it mandatory on their marketplaces for app users to be given access to the app's privacy policy. The DPAs pointed out that the Appstores already facilitate communication on numerous issues, such as the age rating, size and version of the app. They argue that privacy policies should form part of this discussion and that privacy information should be displayed on the app marketplace to allow consumers to make an informed decision.

App users struggling with privacy

This recommendation follows the publication of the second annual Global Privacy Enforcement Network Privacy Sweep in September 2014, which showed that users of 59 per cent of the 1,211 mobile apps surveyed struggled to find basic privacy information. The letter argues that consumers are therefore unable to make a meaningful decision about the collection and use of their data by the app.

Why this matters

The UK Information Commissioner's Office (the 'ICO') has published guidance, 'Privacy in mobile apps', to help app developers collect and use personal data correctly in the United Kingdom. The ICO commissioned research to support the launch of its guidance showing that 49 per cent of app users have decided not to download an app based on privacy concerns. This clearly indicates that, as well as the DPAs, the average consumer is concerned about the lack of privacy policies.

Threat of action?

It is therefore important that app developers and sellers take action to ensure that the relevant privacy policies are in place and that these are clearly communicated to consumers on the Appstore as well as within the

app. Theoretically, the ICO is able to fine companies up to £500,000 for breaches of the relevant legislation, although this power has yet to be used against mobile app developers. However, the threat of action will surely motivate app developers and Appstores alike in this area.

Daisy Jones, Associate, Osborne Clarke, London

German privacy regulator imposes €1,300,000 fine on insurance giant Debeka

Flemming Moos

Journal of Direct, Data and Digital Marketing Practice (2015) **16**, 226–227. doi:10.1057/dddmp.2015.10

Who: Data Protection Authority of Rhineland-Palatinate

Where: Germany

When: 29 December 2014

What happened

The regional German Data Protection Authority (DPA) of Rhineland-Palatinate imposed a record fine of €1,300,000 on insurance giant Debeka after its sales staff allegedly sought address data of business customers' employees in order to offer them Debeka's consumer products. The case did not only attract the attention of the DPA. The Public Prosecutor initiated investigations against five employees because of an alleged incitement of civil servants to violate secrecy obligations and data protection laws by disclosing details on other officials in order for Debeka to market their services to them. On top of this, Germany's insurance regulator, the Federal Financial Supervisory Authority (BaFin), conducted an investigation and required various improvements of the company's data protection organization.

Why this matters

At first glance, the case is all about proper marketing use of data. It reminds businesses that data must generally be collected directly from the affected individual; otherwise the individual must have clearly consented to the forwarding of his details to a third party. In particular, the call by BaFin for genuine improvements to Debeka's business organization through the strengthening of the internal data protection framework shows, however, that it has a much more fundamental impact.

Further, BaFin required the company to:

- fully document the origin of all data on potential new customers;
- install a proper data protection organization, for example, by entrusting specific employees with the oversight of the proper collection and use of personal data;