HUNTON& WILLIAMS

EUROPEAN PRIVACY & E-COMMERCE ALERT

June 2009

Contacts

Brussels Office
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
P: +32 (0)2 643 58 00
F: +32 (0)2 643 58 22

Christopher Kuner
+32 (0)2 643 58 56
ckuner@hunton.com

Dr. Jörg Hladjk
+32 (0)2 643 58 28
jhladjk@hunton.com

Cédric Burton
+32 (0)2 643 58 29
cburton@hunton.com

Olivier Proust
+32 (0)2 643 58 33
oproust@hunton.com

London Office
30 St Mary Axe
London EC3A 8EP
United Kingdom
P: +44 (0)20 7220 5700
F: +44 (0)20 7220 5772

Bridget C. Treacy
+44 (0)20 7220 5731
btreacy@hunton.com

EU: European Parliament Adopts Amendments to E-Privacy Directive

On May 6, 2009, The European Parliament adopted in second reading all proposed amendments to the e-Privacy Directive (Directive 2002/58/EC). These include a new data breach notification requirement. However, since the e-Privacy Directive is part of the broader Telecom Package, which is undergoing a conciliation procedure, the amendments will likely be delayed. Further analysis is available here, and the European Parliament's press release here.

EU: Commission Issues Recommendation on RFID, Privacy and Data Protection

On May 12, 2009, the European Commission issued a non-binding recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (RFID). It advocates data protection measures, including opt-in policies, notification of consumers on the use of their personal data, and development of a common European sign for products with implemented smart chips. Recommendation C(2009) 3200 final is available here, and the FAQs on RFID here.

EU: New FAQs on Binding Corporate Rules

On April 27, 2009, the Article 29 Working Party issued a new working document (WP 155 rev.04) on frequently asked questions (FAQs) relating to binding corporate rules (BCRs). Two new FAQs were adopted: (1) FAQ 10 deals with the relationship between EEA data protection laws and BCRs; and (2) FAQ 11 relates to the reversal of the burden of proof in the context of BCRs. The Working Party reiterated that, although BCRs may offer an adequate level of protection to personal data being transferred within the same company, they do not exempt multinationals from complying with national data protection laws and taking local compliance steps. The Working Document is available here.

Belgium: Prosecutor's Office Blocks Website Access

On April 22, 2009, the Belgian Public Prosecutor ordered 17 Internet service providers (ISPs) to block access to a Dutch website (www.kinderporno.nl) that was disclosing the names and locations of individuals suspected of pedophile crimes. The order was based on a violation of the prohibition of processing sensitive data, in particular judicial data, on the violation of an individual's right to be forgotten, and on the risk of invasion of the victims' privacy. Interestingly, privacy and data protection concerns seem to have prevailed over

other fundamental rights such as freedom of expression. The DPA press release is available (in French) here.

Germany: Publication of First German Study on Costs of Data Breaches

In February 2009, the Ponemon Institute published the results of its inaugural study "Germany — 2008 Annual Study: Cost of a Data Breach." The study is the first such research study undertaken in Germany, using data from actual incidents to estimate the costs of dealing with data breaches by German companies. It examined the experience of 18 German organizations that had suffered a breach. The case studies ranged in size from an incident involving less than 3,750 records to an incident involving more than 90,000 records. The reported breaches occurred across ten industry sectors. According to the study, the average cost of a data breach in Germany is €112 per compromised record. The total cost of handling the breaches ranged from €267,000 to €6.75 million, the average being over €2.41 million. To access the study, click here.

Germany: German Government Introduces €50,000 Penalty for Unsolicited Calls

On May 15, 2009, the German Federal Council adopted the "Act against unsolicited commercial phone calls and improvement of consumer protection." Pursuant to the Act, violations of the existing prohibition on unsolicited commercial phone calls can now be sanctioned with a fine of up to €50,000. In addition, the Act clarifies that a commercial phone call is only lawful if the recipient has given his or her prior explicit consent to receiving the call. The provision is intended to prevent the caller's reliance on consent that may have been given by the recipient in a totally different context or after the call was placed. Further, those placing commercial phone calls may not suppress their phone number or identity. Violations of this prohibition may be sanctioned with a fine of up to €10,000. The Act will enter into force after publication in the official Federal Gazette. The full text of the Act (in German) can be found here.

Germany: Federal Labor Court Rejects Overheard Telephone Conversation as Evidence

On April 23, 2009, the German Federal Labor Court (Bundesarbeitsgericht) decided (Az.: 6 AZR 189/08) that a party involved in a telephone conversation who intentionally allows a third party to overhear that conversation (e.g., by switching to loudspeaker on the telephone set or by holding the receiver away from his ear) violates the telephone counterpart's general personality right. As a result, and pursuant to the case law of the German Federal Constitutional Court, the third party may not give evidence on the content of the telephone conversation. However, this scenario must be distinguished from a situation where a third party happens to overhear a telephone conversation without the first party's facilitation of this. In this instance, the evidence prohibition does not apply. The Court press release (in German) is available here.

Ireland: Data Protection Commissioner Issues Interim Breach Notification Guidance

On April 14, 2009, the Irish Data Protection Commissioner published interim guidelines for private sector organizations, recommending the notification of all data breaches to the Commissioner's office, "regardless of the amount or quality of the personal data at issue." A working group established in October 2008 by the Minister of Justice, called Equality and Law Reform, is currently examining the introduction of mandatory data breach notifications into Irish data protection legislation. The interim guidelines are available here.

Lithuania: Data Subjects to Be Informed of CCTV Surveillance Use

On April 17, 2009, the Lithuanian Data Protection Agency (ADA) issued recommendations on video surveillance, specifying that the use of CCTV should be notified by data controllers, irrespective of whether or not the images collected are recorded in a file. According to Article 20(1) of the Lithuanian Data Protection Act, data controllers must ensure that information on CCTV and the data controller's contact details are clearly and properly provided to the data subjects before they enter the premises placed under CCTV surveillance. Further information is available via the ADA's website, available here.

Spain: Spanish DPA Issues Internet User Privacy Recommendations

On May 13, 2009, the Spanish Data Protection Authority (AEPD) issued extensive guidance with online privacy and security recommendations. It

highlights twelve key areas in which Internet users can be exposed to risks such as P2P networks, search engines, or social networking sites, and provides recommendations so as to alleviate these risks. It also provides security precautions such as avoiding spyware, erasing cookies and ensuring secure online banking, as well as encouraging responsible online behavior. The 68-page guide, "Recommendations to Internet Users," is available (in Spanish) via the AEPD's website here.

UK: ICO Issues RAND Report on Strengths and Weaknesses of EU Data Protection Directive

On May 12, 2009, the UK Information Commissioner's Office published a study commissioned from RAND Europe, setting out the strengths and weaknesses of the European Data Protection Directive (Directive 95/46/EC). Amongst the Directive's strengths, the Report lists: (a) the flexibility of the Directive's application; (b) the Directive's "technology-neutral" approach; (c) the role the Directive has played in harmonizing data protection rules across the EU; and (d) the provision of a good reference model to other countries. However, the Report notes the Directive's failure to evolve alongside technological and regulatory developments, and formulates nine recommendations for stimulating a much-needed debate surrounding future developments on EU data protection law. Further comments on the Report are available here, and the full RAND Report here.

UK: EC Launches Infringement Proceedings against UK for Failure to Enforce EU Privacy Laws

On April 14, 2009, the European Commission (EC) launched infringement proceedings against the UK government by issuing an infringement notice for alleged breaches of EU data protection laws. The proceedings were prompted by complaints from Internet users about the use of a behavioral advertising technology by Internet advertising company *Phorm Inc.* *Phorm's* tracker technology enables Internet service providers (ISPs) to analyze users' online behavior in order to build up user profiles and deliver targeted advertising. The EC proposes a range of amendments to the UK's legislation, including prohibiting unlawful interception and surveillance techniques, without first seeking the user's prior consent ("opt-in" principles). The UK has two months to respond to the notice. Further information is available here.

UK: ICO Approves Companies' BCRs

On May 1, 2009, the Information Commissioner's Office (ICO) authorized the transfer of personal information from the UK by the Accenture and Atmel groups of companies to other entities within their own corporate groups. In each case, the ICO granted authorization for the data transfers based on the strict rules and procedures put in place by the binding corporate rules (BCRs), which provide adequate levels of protection for individuals' rights in relation to the processing of personal data across the groups. This is the first set of BCRs to be approved by a European DPA relying on the mutual recognition procedure. The ICO's press release is available here.