HUNTON& WILLIAMS

EUROPEAN PRIVACY & E-COMMERCE ALERT

February 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

ECHR Rules on Disclosure of Web Users' Identity

On December 2, 2008, the European Court of Human Rights (ECHR) ruled in *K.U. v. Finland* that Article 8 of the European Convention on Human Rights requires national laws to protect individuals from serious online privacy infringements, but also that the national legal framework must allow for the identification and prosecution of offenders. This case involved an advertisement of a sexual nature, which was placed on an Internet dating site on behalf of the applicant, who was twelve years old at the time, without his knowledge. The applicant's father could not identify the individual(s) responsible for the advertisement because the Internet service provider (ISP) refused to disclose any identity, arguing that it was bound by the secrecy of telecommunications. The Court concluded that the Finnish legislation violated the applicant's privacy because it did not authorize the ISP to disclose the identity of the person(s) behind the advertisement. The national legislation should have balanced the right to privacy of the Internet advertiser with the right to privacy of the infringed individual. The full text of the ECHR's judgment is available here.

ECJ Rules against Central Register of Foreign Nationals

On December 15, 2008, the European Court of Justice (ECJ) ruled in Case C-524/06 *Heinz Huber v. Bundesrepublik Deutschland*, which involved the legality of a database (Central Register of Foreign Nationals) maintained by the German Federal Government containing residence information about European Union citizens who are not German citizens. The ECJ concluded that such database is incompatible with the EU Data Protection Directive, unless: (a) it contains only the data necessary for the application by public residence authorities of the legislation relating to the right of residence; and (b) the centralized nature of the database enables a more effective application of that legislation. The ECJ further stated that the storage and processing of personal data in the Central Register of Foreign Nationals for statistical purposes cannot be considered to be necessary within the meaning of the EU Data Protection Directive. The full text of the judgment is available here.

EU: First Meeting of EU Data Protection Expert Group

On December 4, 2008, the new Data Protection Expert Group of the European Commission (GEX PD) met for the first time. Christopher Kuner of Hunton & Williams is among the five appointed members of the group. Further information is available here.

Austria: DPA Approves SOX Whistleblowing Hotline with Limitations

On December 5, 2008, the Austrian data protection authority (DPA) issued its first decision on the implementation of a whistleblowing hotline as required by the Sarbanes-Oxley Act (SOX), to be

administered by the Austrian subsidiary of a US-based company. The DPA partly approved the data transfers from the Austrian entity to the US entity for the purpose of enabling it to prosecute "serious incidents" caused by the behaviour of executive managers. The DPA ordered the Austrian subsidiary to implement a contract guarantying data subjects the ability to exercise their rights through the service provider managing the hotline. The DPA did not consider SOX to provide a legal basis for the transfer, but rather found that the legal basis was provided by the legitimate interests of the Austrian subsidiary, as conveyed by instructions of the employer, admissible in the context of an employment relationship, including a Code of Conduct. The conditions placed on the hotline are based on the recommendations issued by the Article 29 Working Party in its Working Paper 117. The full text of the decision (in German) is available here.

Belgium: Belgian Privacy Commission Publishes Decision on "SWIFT Case"

On December 9, 2008, following an extensive two-year review of SWIFT's messaging service, the Belgian Privacy Commission (DPA) concluded that SWIFT had fully complied with Belgian data protection law. While the Article 29 Working Party and the DPA had previously determined that SWIFT was acting as a co-controller, the DPA, introducing a new concept in data protection law, decided that SWIFT is mainly acting as a mandate (délégué de fait) for the financial community. The financial community and the banks are therefore the data controllers and are liable for compliance with most data protection rules. The DPA consider SWIFT as a data controller for the processing of data for extraction and anonymization of non-identifying data for statistical and analytical purposes. In addition, the DPA decided that Belgian law applies when assessing the data transfers and the level of data protection of the country to which the data is transferred. However, further processing of data physically located in the US (e.g., onward transfer of data to the UST) is subject to only US law. Finally, a series of voluntary measures taken by SWIFT to improve the protection of personal data were also decisive. The full text of the Belgian DPA's decision (in French) is available here.

France: CNIL Sanctions Online Merchant for Breach of Security Measures

On November 17, 2008, the CNIL issued a press release regarding its previous public warning against a French website ("entreparticuliers.com") which specializes in connecting real estate owners with real estate agents and potential buyers. Following an investigation on the premises of the data controller, the CNIL found that a failure in the web platform's security system made it possible for anyone to access the personal space of advertisers, access their personal data, and change the content of the advertisements. The CNIL found that there had been additional breaches of the Data Protection Act, the absence of specific data retention periods, insufficient information of the data subjects, and the carrying out of marketing campaigns via email and SMS without the prior consent of the data subjects. More information is available (in French) here.

France: Court Finds Company Online Privacy Terms and Conditions Unlawful

On October 28, 2008, the Paris Court of First Instance ruled that the general terms and conditions of Amazon.fr relating to the sharing of customers' personal data and third-party marketing were unlawful under the French Consumer Code and subsequently ordered the removal of 18 unlawful clauses from the terms and conditions. The Court ruled that the provisions imposing data sharing for marketing purposes on customers created disproportionate obligations for the consumers. Furthermore, it found that the clauses did not mention the purposes for which customer data was being collected. It ordered Amazon.fr to pay €30,000 in damages to the Union Fédérale des Consommateurs Que Choisir, the French consumer association which had launched the proceedings. The full court judgement is available (in French) here.

Germany: Transfer of Patient Data for Invoicing Purposes is Unlawful

On December 10, 2008, the German Federal Social Court (Bundessozialgericht: Az.: B 6 KA 37/07 R) issued a ground-breaking decision in the health insurance sector. The Court ruled on the scope of protection of patient data in the context of statutory health insurance. It concluded that hospitals or contract doctors are not allowed to transfer patient data to private service providers for invoicing purposes. According to the Court, this also applies when patients have signed consent declarations. The press release (in German) is available here.

Ireland: Spammers Face Record Fines under New Regulations

On December 13, 2008, new stricter Irish regulations (Statutory Instrument No. 526 of 2008) came into force in connection with unsolicited electronic communications and direct marketing. The Irish Data Protection Commissioner welcomed the new regulations, which

impose greater penalties for non-compliance. Amongst the changes introduced by the new regulations are: (1) maximum fines of up to €250,000; (2) the creation of an indictable offence for breaches relating to unsolicited communications; (3) provisions for the prosecution of individual officers of a corporate organization, regardless of whether or not proceedings are brought against the organization itself; and (4) the sender of the electronic communication will have to prove that the subscriber gave prior consent (shifting of the burden of proof). The Regulations are available here.

Spain: Telefonica Moviles Sanctioned over Contracts with Underage Children

On December 9, 2008, the Spanish Data Protection Agency (AEPD) imposed on mobile operator Telefonica Moviles a fine of approximately €230,000 for signing service provision contracts with three underage children in Spain and using their data unlawfully. Under the Spanish Data Protection Act, no one is permitted to use data from children under 14 years of age without the prior consent of their parents or legal guardians. Further information is available here.

Spain: Attendees at Barcelona Meeting Discuss Global Privacy Standards

On January 12, 2009, national and international data protection experts met in Barcelona under the auspices of the Catalonian data protection agency to consider the adoption of international privacy standards. This high-level meeting brought together experts from both the public and private sectors. International privacy standards will be discussed further at the 31st International Conference of Data Protection and Privacy Commissioners that will be hosted in Madrid in November 2009.

Switzerland: Swiss-US Safe Harbor Framework Signed

On December 9, 2008, an exchange of letters was signed by the Swiss Federal Data Protection and Information Commissioner (FDPIC) on the creation of a "Swiss-US Safe Harbor Framework", which is comparable to the "EU-US Safe Harbor Framework". The Swiss-US Safe Harbor Framework is intended to simplify the transfer of personal data by Swiss companies to American companies certified by the US Department of Commerce. US companies that are self-certified with the US Department of Commerce and bound by the data protection principles contained in the Framework will be automatically considered as providing an adequate level of data protection under Swiss law. More information is available here.

The Netherlands: Dutch DPA Takes Position on Tell-a-Friend Systems

On December 3, 2008, the Dutch DPA (CBP) and the Dutch Telecom Regulator (OPTA) published a joint decision relating to web-based "Tell-a-Friend" systems. Tell-a-Friend systems are viral marketing mechanisms whereby an Internet content provider requests its readers and consumers to circulate prepared commercials to their friends and contacts using their e-mail. The decision discussed specific mechanisms whereby an Internet user (the sender) provides the email addresses of third parties (the recipients) to the Internet content provider (the data controller) via a form on its website. The data controller subsequently sends emails to the addresses provided. In their decision, CBP and OPTA state that Tell-a-Friend mechanisms may be legitimate if the following requirements are met: (1) it is up to the sender to decide whether or not to send a message; (2) the message must unambiguously indicate who is sending the message; (3) the sender must receive unambiguous and complete information about the message to be sent in order to take full responsibility for its contents; and (4) the data controller cannot use or keep the provided contact details for purposes other than the sending of a message on behalf of the sender. Any other email sent to these contact details will be considered as spam. The decision is available (in Dutch) here.

United Kingdom: ICO Consults on Draft Code of Practice for Privacy Notices

On January 12, 2009, the Information Commissioner's Office (ICO) launched a consultation on a new draft code of practice for privacy notices. The code is designed to help organizations provide more user-friendly privacy notices. The draft code of practice contains examples of good and bad privacy notices. The consultation closes on April 3, 2009. The ICO's press release is available here.