HUNTON& WILLIAMS

EUROPEAN PRIVACY & E-COMMERCE ALERT

March 2010

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: Article 29 Working Party Issues Contribution to Consultation on EU Data Protection Framework

On December 1, 2009, the Article 29 Working Party adopted a contribution (the "Contribution") to the Consultation launched by the European Commission ("EC") on the legal framework for the fundamental right to the protection of personal data (the "Consultation"). The Contribution maintains that the fundamental principles of European data protection law remain valid. However, it also notes that both improvements in implementation and changes to the existing data protection framework should be considered. The EC will now evaluate all the contributions received under the Consultation and examine whether changes to the European Union's data protection framework should be proposed. Further information is available here and view the full text of the Contribution.

EU: Article 29 Working Party States that Israeli and Andorran Data Protection Laws Provide "Adequate Protection"

On January 5, 2010, the Article 29 Working Party published an opinion dated December 1, 2009, stating that Israeli data protection law largely provides an "adequate level of data protection" under the European Union Data Protection Directive 95/46. The European Commission will now take this opinion into account when determining whether to issue an "adequacy decision" for Israel over the coming months. A positive decision from the Commission would provide that data transfers from the EU to Israel are adequately protected, for the purpose of compliance with the EU Data Protection Directive. Similarly, the Article 29 Working Party also adopted the opinion dated December 1, 2009 on the level of protection of personal data in the Principality of Andorra. The Working Party considered that the Principality of Andorra ensures an adequate level of protection within the meaning of Directive 95/46.

EU: Hunton & Williams Prepares Study on Interaction between Data Protection Law and Copyright Enforcement

On February 3, 2010, Christopher Kuner, a partner in Hunton & Williams' Brussels office, presented to the "Stakeholders' Dialogue on Illegal Uploading and Downloading" a study prepared by the Hunton & Williams Brussels team for the European Commission, on the interaction of data protection law and copyright enforcement. The study covers both the legal framework under EU law and the situation in six selected EU Member States (Austria, Belgium, France, Germany, Spain and Sweden). As the study demonstrates, the relationship between data protection law and online copyright enforcement is far from being settled. This issue will certainly be discussed in the coming months during the ongoing debate on the review of the General Data

Protection Directive at the European level, and in the context of the debate around possible graduated response mechanisms at the national level. Further information is available here.

EU: New Standard Contractual Clauses Approved for Transfers to Data Processors

On February 5, 2010, the European Commission adopted a new set of standard contractual clauses ("SCCs") for the transfer of personal data from data controllers in the EU to data processors outside the EU. The clauses were negotiated over several years between the European Commission and a group of business associations led by Brussels-based Hunton & Williams partner Christopher Kuner, who is chair of the International Chamber of Commerce Task Force on Privacy and Data Protection. Despite the growing popularity of other mechanisms, which provide a legal basis for complying with EU requirements on the international transfer of personal data outside the EU (e.g., binding corporate rules), the use of SCCs remains indispensable, since in many situations, they are the only "off the shelf" data transfer solution that can be used and implemented on short notice. Further information is available here and view the full text of the new SCCs.

EU: European Parliament Rejects SWIFT Agreement

On February 11, 2010, the European Parliament rejected by a vote of 378 to 196 the 2009 agreement reached between the EU and the U.S., which allowed U.S. law enforcement authorities access to the payment database of the financial consortium SWIFT. A number of members of the Parliament had expressed concern regarding the level of data protection provided for in the agreement. The rejection of the agreement sends the EU and the U.S. back to the drawing board in order to negotiate a new agreement and with the participation of the Parliament. The vote illustrates the enhanced powers of the Parliament in data protection and privacy matters under the Lisbon Treaty, and the dangers that companies face when caught between U.S. law enforcement requirements and EU data protection restrictions. Further information is available here.

EU: Article 29 Working Party Issues Opinion on Concepts of "Controller" and "Processor"

On February 16, 2010, the Article 29 Working Party adopted an opinion (WP 169, the "Opinion") providing clarification and guidance on the interpretation of the concepts of "data controller" and "data processor" in the context of the EU Data Protection Directive 95/46/EC. Recognizing the difficulties in applying the current definitions, the Working Party has provided some examples from daily experiences taken from data protection authorities. View the full text of the Opinion.

Germany: DPA Fines Drugstore Chain €137,500 for Illegal Collection of Health Data

On January 11, 2010, the data protection authority of the German federal state of Baden-Württemburg issued a press release stating that it had fined the Müller Group €137,500 for illegal retention of health-related data and failure to appoint a data protection officer). In April 2009, the German press had reported that the Müller Group, a drugstore chain comprised of twelve entities and employing some 20,000 workers, had been illegally collecting health data from its employees since 2006. The Müller Group entities had systematically requested that employees returning from sick leave identify the reasons for their sicknesses on a form that was then sent to the group's central human resources department for processing. As of April 2009, approximately 24,000 records containing data on employee illnesses were being stored in Müller's centralized HR files. View Baden-Württemberg DPA's press release.

Germany: Federal Network Agency Imposes €500,000 in Fines for Telemarketing Violations

On January 29, 2010, the German Federal Network Agency (the "Agency") stated in a press release that it had imposed fines for unauthorized telephone advertising in six cases. This brings the total number of fines imposed during the period December 2009–January 2010 to nine, for a total amount of €500,000. It also marks the first time the Agency has imposed sanctions for unauthorized telephone advertising and for breaches of caller ID requirements for telephone marketing. Since amendments to the Law against Unfair Competition and the Telecommunications Act came into force on August 4, 2009, marketing calls made without the consent of the recipient, or made using masked or suppressed numbers, have been considered misdemeanors. Further information is available here and view the Agency's press release (in German).

UK: Fines for Data Breaches Now a Reality

On January 12, 2010, the UK government laid regulations before Parliament to bring into force civil monetary penalties of up to £500,000 ($800,000) for serious data breaches. These penalties are likely to take effect on April 6, 2010. Significantly, the penalties will apply not only to data security breaches but also to all serious breaches of the UK Data Protection Act 1998. Christopher Graham, the UK's information commissioner, has emphasized that he will adopt a pragmatic and proportionate approach to issuing monetary penalties, taking into account the organization's size, financial resources and industry sector, as well as the severity of the breach. The information commissioner's statutory guidance explaining how he proposes to use his power is available on the Commissioner's website. The Ministry of Justice's response to the public consultation is available on the Ministry's website.

Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and information security law updates and analysis.