

December 2008

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

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 Toolkit on Binding Corporate Rules

On October 1, 2008, the Article 29 Working Party issued a toolkit on Binding Corporate Rules (BCRs) aimed at promoting them as a mechanism for transferring data to countries without an adequate level of data protection. The toolkit includes: (1) a table highlighting the elements and principles to be found in BCRs (WP 153); (2) a document setting up a framework for the structure of BCRs (WP 154); and (3) a revised version of the FAQs on BCRs (WP 155). The toolkit also announced the creation of a mutual recognition procedure between nine national data protection authorities. More information is available [here](#).

EU: Council Adopts Data Protection Framework for Police and Judicial Cooperation

On November 27, 2008, the Council of the European Union adopted a framework decision on the protection of personal data in the field of Police and Judicial Cooperation in Criminal Matters. EU Member States have two years to implement the decision, and are free to adopt stronger requirements. The text is available (in French) [here](#). The European Data Protection Supervisor (EDPS) has criticized the framework decision. More information is available [here](#).

EU: Council Reaches Political Agreement on Review of e-Privacy Directive

On November 27, 2008, the Council of the European Union reached a political agreement on the review of the EU telecoms package (regulatory framework for electronic communications networks and services), including the e-Privacy Directive (Directive 2002/58/EC). The Council now has to adopt a common position which will serve as a basis for the second reading by the European Parliament. The second reading should not be expected before late March 2009.

Therefore, the review is not yet final and changes are still anticipated. The revised directive should enter into force on December 31, 2009, but will still have to be implemented into the national law of the individual Member States. The latest version of the proposal can be found [here](#). More information about the legislative process is available [here](#).

EU: ECJ Advocate General Issues Opinion on Legality of Data Retention Directive

On October 14, 2008, Advocate General Yves Bot issued an opinion finding that the legal basis for the Data Retention Directive (2006/24/EC) was correct. The case was brought by Ireland in 2006, which claimed that the Directive should

have been adopted based on the third pillar (Police and Judicial Cooperation in Criminal Matters) rather than the first pillar (European Community). The Advocate General advised the Court to dismiss the case, taking the view that the Data Retention Directive was correctly adopted on the basis of the first pillar. The full text of the Advocate General's opinion is available [here](#).

EU: ECJ Interprets Article 5 of the e-Commerce Directive

On October 16, 2008, the European Court of Justice (ECJ), interpreting Article 5 of the e-Commerce Directive (Directive 2000/31/EC), ruled that information society service providers must provide their clients with an alternative means of communication beside electronic mail prior to the conclusion of a contract. However, the listing of a telephone number on the company's website is not necessarily required. The ECJ stated that this alternative means of communication can take the form of electronic enquiry templates through which the client can contact the service provider via the internet. Nevertheless, the service provider must also provide non-electronic means of communication in cases where the client specifically requests offline communication because he has no access to an electronic network. The full text of the Court's ruling is available [here](#).

ECHR Rules against UK in DNA Retention Case

On December 4, 2008, the European Court of Human Rights (ECHR) delivered a Grand Chamber judgment

in the case *S. and Marper v. the United Kingdom*. This case concerns the ability of law enforcement authorities to store fingerprints and DNA samples collected from suspects in the context of unsuccessful criminal proceedings. The Court unanimously held that there had been a violation of Article 8 of the European Convention on Human Rights (Right to Privacy), and that by setting up the database, UK legislation had failed to strike a fair balance between competing public and private interests. The full text of the case is available [here](#).

BE: Belgian Supreme Court Introduces Concept of Reasonable Expectation of Privacy

On September 9, 2008, the Belgian Supreme Court (Court de Cassation), ruling in a criminal case, interpreted the secrecy of electronic communications in light of Article 8 of the European Convention on Human Rights and Article 17 of UN International Covenant on Civil and Political Rights (Right to Privacy). The Supreme Court stated that the recording of a private communication by one party to the communication without the other party's notification or prior authorization does not systematically breach the right to privacy.

However, the Supreme Court concluded that use of the recording may be illegal. The legality of the use must be analyzed in light of the "reasonable expectation of privacy" of the parties to the communication. This new concept of "reasonable expectation of privacy" depends on the facts, in particular the content of the communication and the circumstances surrounding the

conversation. Consequently, in certain circumstances, evidence previously dismissed by courts could become admissible. It is now up to the Court of Appeal to apply this new concept to the specific facts of the case. The text of the case is available (in Dutch) [here](#).

Germany: Cabinet adopts amendments to Federal Data Protection Act

On December 11, 2008, the German Federal Government adopted a number of amendments to the Federal Data Protection Act which have far-reaching consequences for businesses. The amendments were developed in response to a number of data breaches in Germany in recent months.

The proposed changes can be summarized as follows: (1) abolishment of the so-called "list privilege" and introduction of an "opt-in" requirement for the sharing of personal data in the context of address selling, advertising and market research, with some exemptions, e.g. opt-in does not apply for a company's own customers, and, there is a 3-year grace period; (2) creation of a security breach notification requirement applying to certain categories of personal data; (3) a proposed comprehensive Data Protection Audit Act, according to which data controllers and providers of data processing systems and software could voluntarily undergo an audit in order to have their data protection concept and technical facilities assessed and evaluated; (4) an increase of fines from € 25,000 up to € 50,000 for violation of certain provisions and from € 250,000 to € 300,000 in case of serious

legal violations and the possibility of forfeiture of profits. The bill still needs to pass the federal council and federal parliament. The first reading in the council is scheduled for February 13, 2009. The amendments are expected to enter into force on July 1, 2009.

France: Consumers' Consent is Required prior to Sending of Bluetooth Commercials

On November 12, 2008, the French Data Protection Authority (CNIL) announced that the sending of commercial messages via Bluetooth requires the consumer's prior consent. This opinion was issued in reaction to plans of installing billboards which would transmit commercial messages to a passerby's cellular phone in public areas, such as subways, shops and discotheques. According to the CNIL, the "MAC address" of a portable device and the Bluetooth identification number are personal data. Therefore, sending commercials to passersby, without obtaining their prior consent is illegal. Additional information is available (in French) [here](#).

France: Paris Court Rules that a Family Name Alone is Not Necessarily Personal Data

On September 22, 2008, the Paris Court of First Instance ruled, following a summary proceeding (*juge des référés*), that the use of an individual's family name to sell products on a genealogy web site did not constitute a breach of the individual's right to privacy because the individual could not be directly or indirectly identified through his family name alone. However, the conclusion of the Court should be

limited to the specific facts of the case (complaint about the selling of products with family names on a genealogy web site). The full text of the Court decision is available (in French) [here](#).

France: CNIL Conducts Inspections on Human Resource Management Systems and Issues Guidance for Employers and Employees

In recent months, the French Data Protection Authority (CNIL) has examined the extent to which Human Resource management systems comply with French data protection laws in some fifty companies. In particular, the inspections revealed the following: (1) insufficient knowledge and information of employees concerning their legal rights; (2) issues relating to international data transfers; (3) the absence of compliant data retention policies; and (4) non-respect of the notification requirements regarding whistleblowing hotlines. The CNIL press release is available (in French) [here](#).

On November 17, 2008, the CNIL also published a guide advising employers in connection with data protection compliance issues and informing employees of their legal rights regarding issues such as the electronic processing of personal data, video-surveillance systems, cyber surveillance and access controls based on biometric data. The full text of the guide is available (in French) [here](#).

France: Senate Adopts "Creation and Internet" Bill

On October 23, 2008, the French Senate adopted a new legal framework for copyright infringements on the

Internet. The framework provides for the creation of a "warning and sanctioning" system (graduated response) to be carried out by a new government agency (the High Authority for the Circulation of Works and the Protection of Rights on the Internet). If the legislation is adopted, the new High Authority would be empowered to suspend a web user's internet connection for illegal downloading of files, provided that several letters of notification have previously been served on the web user. The bill is scheduled to be discussed in the French Parliament in December 2008. Further information is available (in French) [here](#).

Spain: AEPD Publishes Guide on Data Security

On November 3, 2008, the Spanish Data Protection Agency (AEPD) issued a guide on security measures required by Spanish data protection law, along with implementation strategies. The guide contains: (1) an explanation of the different security levels and their corresponding security measures; (2) a template for the drafting of compulsory internal security documents; and (3) a questionnaire to automatically evaluate applicable security levels and their level of compliance. The guide is available (in Spanish) [here](#).

Spain: AEPD Releases Legal Report on Obtaining Consent through Web Sites

Following a public consultation, the Spanish Data Protection Agency (AEPD) has issued a report on how to obtain consent online. In its report, the AEPD reiterated that data controllers have the burden to prove that data

subjects have been well informed before providing their “specific and unequivocal” consent. Subsequently, when collecting data through web sites, consent has to be requested in a way that makes it impossible for the data subject to provide personal data unless he has read all the necessary information related to the processing. The full text of the report is available (in Spanish) [here](#).

The Netherlands: Processing of IP Addresses to Create a Black List of Visitors on a Website is Illegal
.....

On September 23, 2008, the Dutch Data Protection Authority (DPA) published an infringement decision regarding the web site “Geencommentaar.nl” (“No Comment”),

a news web-blog. The web site was accused of secretly registering the IP addresses of visitors in order to create a list of undesirable users. The list was then made available to interested third parties in the form of a “black list”. The black list allowed web site owners to detect and subsequently deter certain users from taking part in discussion fora or in other forms of interactive communications. The DPA concluded that this practice was in breach of data protection law. In particular, the DPA concluded that: (1) IP addresses are regarded as personal data; (2) the Dutch web site had processed the IP addresses without a legitimate legal basis; and (3) it had violated its obligation to notify the user of the data collection.

However, since the web site ultimately removed the application and destroyed the database, the DPA waived further disciplinary actions. Additional information is available (in Dutch) [here](#).

The Netherlands: Adoption of New “Notice and Takedown” Code of Conduct
.....

On October 9, 2008, a voluntary Notice and Takedown Code of Conduct was agreed upon and formally approved by the Ministry of Economic Affairs. The new code outlines a series of procedure for public telecommunication service providers on the Internet (in the Netherlands), and is designed to speed up the removal of illegal or unlawful Internet content. The full text of the code is available (in Dutch) [here](#).

© 2008 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.