

February 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

#### [Isabelle Chatelier](#)

+32 (0)2 643 58 33  
ichatelier@hunton.com

#### [Cedric Burton](#)

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

### London Office

30 St Mary Axe  
London EC3A 8EP  
+44 (0)20 7220 5700 Phone  
+44 (0)20 7220 5772 Fax

#### [Bridget C. Treacy](#)

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

## EU: Adequacy Decision Rendered for Jersey and Faroe Islands

On October 9, 2007, in Opinion 8/2007 and Opinion 9/2007 respectively, the Article 29 Working Party assessed the adequacy of data protection law in Jersey and in the Faroe Islands in light of the criteria set out in its document on the transfer of personal data. With respect to the Faroe Islands, the Article 29 Working Party determined that, except for a missing provision regarding automated individual decisions, the Faroese law complies with most of the EU data protection principles. Taking the view that adequacy does not mean complete equivalence with the level of protection set by the Data Protection Directive, the Working Party concluded that the Faroe Islands ensure an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC. Regarding Jersey, the law of which is an embodiment of UK law, the Article 29 Working Party found that a number of provisions differ substantially from the Directive, in particular the definition of personal data, unnecessary restrictions to the transparency principle, or the powers of the Data Protection Commissioner. The Article 29 Working Party considered however that these differences were not significant in relation to the protection provided for personal data transferred from EU Member States to Jersey, and concluded that Jersey ensures an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC.

Opinion 8/2007 for Jersey is available (in English) at: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp141\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp141_en.pdf)

Opinion 9/2007 for the Faroe Islands is available (in English) at: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp142\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp142_en.pdf)

## EU: Article 29 Working Party and EDPS Concerned about Commission's Proposal for European PNR Regime

In a press release dated December 6, 2007, the Article 29 Working Party expressed serious concerns over the Commission's proposal for a European PNR regime. In its view, the legislative proposal is still in its early stage and far from fulfilling data protection requirements. It will nonetheless be submitted to the European Council for implementation. In particular, the Working Party highlights the following shortcomings: (1) the proposal does not substantiate any legitimate basis for the collection of passenger data; (2) the amount of personal data collected is unreasonable; and (3) the retention period of 13 years seems to be excessive. Additional shortcomings include inadequate filtering mechanisms and possible third-country transfers.

The press release is available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/news/docs/pr\\_05\\_12\\_07\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_05_12_07_en.pdf)

The European Data Protection Supervisor (EDPS) was consulted by the European Commission regarding this new proposal, and issued an opinion critical of the follow-

ing elements: (1) insufficient justification of the legitimacy of the measures in view of the purpose of combating terrorism; (2) serious lack of legal certainty; (3) lack of clarity about the identification of the data recipients; and (4) potential data transfers to third countries.

The full Opinion is available (in English) at: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20\\_EU\\_PNR\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf)

### **EU: CFI Rules on Right of Access to Names of Individuals Attending European Commission Meetings**

---

On November 8, 2007, the Court of First Instance (CFI) ruled in Case T-194/04 (*Bavarian Lager v. Commission*) that disclosing the names of individuals attending a European Commission meeting is vital to preserve transparency and the rule of law. The right of access to EU documents overrides privacy rights under data protection laws in the European Union. The CFI added that objection by individuals against disclosure of their names should not hinder the right of access. Consequently, the CFI overruled the Commission decision refusing to disclose lobbyists' names. The Court based its reasoning on Article 255 EC according to which any EU citizen and any natural or legal person residing in a Member State has a right of access to documents of the Community institutions. This right of access is subject to restrictions under Regulation No. 1049/2001/EC, which provides that "certain public and private interests should be protected by way of exceptions where necessary to safeguard their ability to carry out their tasks. In assessing the exceptions, the institutions should take account of the principles under Community legislation concerning the protection of personal

data, in all areas of Union activities. The right to public access to documents under Regulation No. 1049/2001 is generally unrestricted and therefore the person making the request is not normally obliged to state reasons justifying it."

The judgment is available at: <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Rechercher&alldocs=alldocs&docj=docj&docop=docop&docor=docor&docjo=docjo&numaff=T-194/04&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100>

### **EU: EDPS Publishes Opinion on Commission's RFID Communication**

---

On December 20, 2007, the European Data Protection Supervisor (EDPS) issued an opinion in response to European Commission Communication COM (2007) 96 on Radio Frequency Identification (RFID) adopted on March 15, 2007. First, the EDPS stresses the significant impact of RFID technology on our society and its potential risks to privacy and data protection. It insists that the focus must be on the whole RFID system and not on RFID tags only. Second, it states that the current data protection framework applies to RFID if personal data is processed. The EDPS, however, recommends adding a new regulation to the current legal framework. This regulation could be a mix of regulatory tools. For example, the EDPS favors the use of self-regulatory mechanisms and close cooperation with the RFID Expert Group. If this combination (current legal framework and self-regulatory mechanisms) fails, the EDPS recommends the adoption of additional, sector-specific legislation regulating RFID technology. Regardless of the solution chosen, the EDPS calls for an opt-in principle "at the point of sale", whereby the individual would

consent to the RFID device remaining activated past the cashier.

The Opinion is available at: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20\\_RFID\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf)

### **France: Fine Imposed on Google for Faulty Data Retention and IP Violation**

---

On December 12, 2007, the Paris Court of Appeal ruled that web-hosting services must be able to fully identify the editors and operators of blogs and other personal sites and may not rely on Internet Protocol addresses as their principal personal identifier. In mid-2006, Benetton had asked Google to block access to blogs on their hosting services that Benetton accused of violating the company's trademark. Google refused to do so. On March 1, 2007, the Paris Court of First Instance ordered Google to forward to Benetton personal data on the identity of the individual behind the fraudulent website. Google responded by forwarding an e-mail address and two IP addresses. The Paris Court of First Instance considered this response unsatisfactory and issued an emergency injunction demanding an immediate ban on the blog. Despite Google's appeal, the Paris Court of Appeal upheld this decision and ordered Google to pay to Benetton €36,000 (over US\$50,000) in damages for failing to comply with French rules on web-hosting firms.

The Court's opinion is available (in French) at: [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=2116](http://www.legalis.net/jurisprudence-decision.php3?id_article=2116)

### **Germany: New Data Retention Law Challenged before Federal Constitutional Court**

In late 2007, Germany adopted the proposed Act implementing Directive 2006/24/EC of the European Parliament and of the Council of March 16, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Under the Act, the data retention provisions are implemented into the Telecommunications Act. The Act places data retention obligations on telecommunications and Internet service providers who provide publicly accessible services to retain data for six months. The Act applies to various types of communications, including e-mail and Internet access services, telecommunications via fixed lines, and mobile telecommunications. The providers will also be required to store traffic data. However, the use of traffic data is limited to law enforcement purposes. The law has been adopted by both the lower and upper house of the German federal Parliament (Bundestag and Bundesrat). The Act came into force for telecommunications providers (with few exemptions) on January 1, 2008 and will enter into force for ISPs on January 1, 2009.

On December 31, 2007, a constitutional complaint prepared on behalf of 30,000 citizens was ready to be filed with the Federal Constitutional Court. It is claimed that the Act violates the German constitution.

The text and commentary to the Data Retention Law is available (in German) at: <http://www.bgblportal.de/BGBl/bgbl1f/bgbl107s3198.pdf>

### **Netherlands: Telecommunications Regulator Imposes Record Fine for Distribution of Unsolicited Software**

On December 18, 2007, the Dutch independent authority regulating postal and electronic communications services (Onafhankelijke Post en Telecommunicatie Autoriteit — OPTA) imposed a fine totaling one million euros on three Dutch companies operating under the name DollarRevenue. These small businesses had surreptitiously installed spy- and adware on over 22 million computers belonging to Internet users in the Netherlands and elsewhere. This practice allowed them to spy on consumers' online behavior and triggered pop-up windows with advertising material. This is the first time that OPTA has imposed a fine on the distributors of undesirable software and this action was welcomed by EU Telecoms and Media Commissioner Viviane Reding in a press release on December 19, 2007.

For additional information, please consult these press releases (in English) at: <http://www.opta.nl/asp/en/newsand-publications/pressreleases/document.asp?id=2459>

### **Spain: DPA Reviews Privacy Policies of Internet Search Engines**

On December 12, 2007, the Spanish Data Protection Agency (AEPD) published a report analyzing the privacy policies of major Internet search engines and requested limits on search data storage and e-mail filters. The report, entitled "Declaration on Internet Search Engines", is the result of information provided by Google, Microsoft and Yahoo!. It reveals significant privacy policy differences between companies and lack of information to the consumers on how their personal data is being used. Moreover, the report states that although companies may not store personal data for longer

than necessary to provide the intended services or for limited functions such as service improvement, they currently retain search data between 13 and 18 months. Additionally, the AEPD criticized e-mail services that scan mail to offer personalized advertising, when scanning is only permitted to filter spam and viruses. The Declaration also targeted the registration data required of consumers in order for them to create blogs or use other Internet services. Therefore, the Agency asked the search engine companies to develop new information mechanisms providing clear and visible information to customers on how their data is used, and giving them the right to cancel, correct, or challenge it.

The Declaration on Internet Search Engines is available (in Spanish) at: [https://www.agpd.es/upload/Canal\\_Documentacion/Recomendaciones/declaracion\\_aepd\\_buscadores.pdf](https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores.pdf)

### **Sweden: DPA Denies to US Subsidiary Exemption to Process Employee Criminal Records**

The Swedish DPA refused to authorize Standard & Poor's AB, a Swedish subsidiary of a US company, to process employee criminal records. The law restricts the processing of this type of data to public authorities, unless prior authorization is obtained from the Swedish DPA. The Swedish entity was asked to obtain employees' past criminal records by its US parent company so that it could become a member of a "Nationally Recognized Statistical Rating Organisation (NRSRO)" in the US. The Swedish DPA took into consideration the International Labor Organization (ILO) recommendations whereby employers should not seek to obtain employees' past criminal records in the course of the employment relationship, unless the request is directly

connected or relevant to the company's undertaking.

The DPA decision is available (in Swedish only) at: <http://www.datainspektionen.se/pdf/beslut/20071218-standard-poor.pdf>

#### **UK: ICO to Be Granted Additional Powers**

---

On November 21, 2007, the British Prime Minister announced that he would grant new powers to the UK Data Protection Office (ICO), which will allow for the conducting of unannounced spot checks of government privacy and security procedures. This statement followed the disclosure by the British government of an unprecedented data breach, involving the loss of two computer discs containing the personal data of some 25 million people. ICO will work with the Ministry of Justice to confirm the details of the new powers. Information Commissioner Richard Thomas said he

would like the UK data protection law changed to make security breaches of the scope of this data loss a "criminal offense". Additionally, this would enable the ICO to prosecute organizations in case of serious breaches, which is not the case currently.

The British Prime Minister press briefing from November 21, 2007 is available (in English) at: <http://www.number10.gov.uk/output/page13818.asp>

Richard Thomas's statement is available (in English) at: [http://www.ico.gov.uk/upload/documents/pressreleases/2007/personal\\_details\\_lost\\_by\\_hmrc\\_201107003.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2007/personal_details_lost_by_hmrc_201107003.pdf)

#### **UK: Large Fine Imposed on Norwich Union Life for Failure to Protect Confidential Information**

---

On December 17, 2007, the UK Financial Services Authority (FSA) fined Norwich Union Life — the largest

UK insurance company offering instant online insurance — GBP 1.26 million (approx. €1.7 million or US\$ 2.5 million) for neglecting to put in place effective systems and controls to protect customers' confidential information. Because of the weakness of the Norwich Union Life system, fraudsters were able to use publicly available information such as names and birthdates to impersonate customers and obtain sensitive customer details from its call centers. The FSA found out that the insurance company had failed to properly assess the risks of financial crime and therefore its customers were more likely to fall victim to such crimes. Norwich Union settled at the early stage of the investigation and also reinstated its policies in full.

The full text of the notice about a financial penalty is available (in English) at: [http://www.fsa.gov.uk/pubs/final/Norwich\\_Union\\_Life.pdf](http://www.fsa.gov.uk/pubs/final/Norwich_Union_Life.pdf)

© 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.