

August 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: EDPS Policy Paper on Research and Technology Highlights “Privacy by Design” Principle

On April 28, 2008, the European Data Protection Supervisor Peter Hustinx released a policy paper entitled “The EDPS and EU Research and Technological Development”, according to which privacy and data protection requirements should be introduced as soon as possible in the life cycle of new technological developments. Hustinx stated that the principle of “privacy by design” should represent an inherent part of the European Commission’s 7th Framework Program. The EDPS plans to assist the Commission in the evaluation of data protection issues of project proposals, promote the education of managers and designers, contribute to research advisory boards, and advise companies in order to ensure that privacy and data protection issues are included at an early stage in technology research and development projects.

The policy paper is available at: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28\\_PP\\_RTD\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf).

## EU: Commission Declares the Bailiwick of Jersey to be “Adequate”

On May 8, 2008, following consultation with the European data protection supervisory authorities, the European Commission published its decision recognizing the Bailiwick of Jersey as providing an “adequate level of data protection”. This means that personal data can freely be transferred from the European Union to Jersey. Jersey is a Crown dependency with independent status; as such, it is not part of the European Union and thus considered as a third country under the EU Data Protection Directive.

The Commission’s full press release is available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/news/docs/pr\\_08\\_05\\_08\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_08_05_08_en.pdf).

## Belgium: New Guidance on Direct Marketing

On May 28, 2008, the Belgian DPA issued updated guidance analyzing each of the requirements that must be met by direct marketing activities in order to ensure compliance with Belgian data protection law.

The full text of the report (in French only) is available at: <http://www.privacycommission.be/fr/static/pdf/direct-marketing/20080605-nota-direct-marketing-fr-version-finale.pdf>.

## France: Two Companies Fined €15,000 for Transmission of Ethnic Data

A complaint concerning the receipt of commercial mailings advertising insurance services for foreigners led the French data protection authority (CNIL) to impose a €15,000 fine on two companies. Impact Net had created a database with addresses of foreigners, and this was used by FAC International to advertise visa insurances and assistance and repatriation services. Both companies had thus violated the prohibition on processing sensitive data without the explicit consent of the data subject.

The CNIL press release (in French) is available at: [http://www.cnil.fr/index.php?id=2483&news\[uid\]=565&cHash=124d8c10e4](http://www.cnil.fr/index.php?id=2483&news[uid]=565&cHash=124d8c10e4).

## Ireland: Irish Data Protection Commissioner Investigates Bank of Ireland Laptop Thefts

On April 18, 2008, the Office of the Irish Data Protection Commissioner, Billy Hawkes, was informed about the theft of four laptops belonging to the Bank of Ireland. Although the laptops, which contained personal data of up to 31,500 customers, went missing in the course of last year, the bank's management had not been informed until February. The Commissioner's Office will now conduct an investigation into (i) the reasons why the personal data, including sensitive medical data, had been stored on the laptops; (ii) the security measures used by the bank; and (iii) the reasons for the delay in reporting the loss.

The Irish Data Protection Commissioner's press release is available at: <http://www.dataprotection.ie/viewdoc.asp?Docid=718&Catid=75&StartDate=1+January+2008&m=n>.

## Italy: Supermarket Chain Fined for Unlawful Use of Customer Data

On May 20, 2008, the Italian data protection authority (Garante) imposed on the Italian supermarket chain GS a €54,000 fine for its unlawful use of customer data. GS, which had obtained the data for the purpose of distributing fidelity cards, was fined for using the same data for targeted advertising without the data subjects' consent. The Garante ordered the supermarket chain to correct the use of data and provide its customers with an unambiguous method which would allow them to refuse its use for targeted advertising.

The Garante's official press release (in Italian) can be found at: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1522432>.

## Norway: Governmental Authorities to Access Credit and Debit Card Information

On May 15, 2008, the Norwegian government proposed to grant governmental authorities access to foreign-issued credit and debit card information. The government announced the proposal as part of its current budget, voicing concerns that Norwegians increasingly use foreign bank accounts to avoid taxes.

The press release on the Norwegian revised national budget is available

(in English) at: <http://www.regjeringen.no/en/dep/fin/Press-Center/Press-releases/2008/revised-national-budget-2008-sound-fisca.html?id=511405>.

## Spain: AEPD Rules "Refer-a-Friend" Viral Marketing Illegal

On February 20, 2008, the Spanish Data Protection Authority (AEPD) imposed a fine on the company *Iniciativas Virtuales* for using viral marketing through its website. The AEPD considered that the company had used this "refer-a-friend" tool to send commercial communication and thus violated the requirements of the Spanish Act on Information Society Services and Electronic Commerce (LSSIE). The marketing strategy therefore also violated the "opt-in" principle as set by Directive 2002/58/EC, transposed into Spanish law by the General Telecommunications Act (LGT). Since it concerned merely one e-mail, the infringement was considered "light" according to Article 38 of LSSIE, and was sanctioned with a fine of €600.

The full text of the ruling is available (in Spanish) at: [https://www.agpd.es/portalweb/resoluciones/procedimientos\\_sancionadores/ps\\_2008/common/pdfs/PS-00323-2007\\_Resolucion-defecha-20-02-2008\\_Art-ii-culo-21-LSSI.pdf](https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00323-2007_Resolucion-defecha-20-02-2008_Art-ii-culo-21-LSSI.pdf).

## Spain: AEPD Publishes Guide for Children and Parents to Promote Personal Data Protection

On June 2, 2008, the Spanish Data Protection Authority (AEPD) published its guide "Rights of Boys and Girls and

Duties of Fathers and Mothers”, in order to inform minors of their data protection rights online, at school and in their immediate surroundings. Using simple language, the guide also reminds parents of their children’s right to data protection.

Earlier this year, on April 19, Royal Decree 1720/2007 took effect, developing and clarifying the terms laid out in Spanish data protection law. It requires parental consent before soliciting or handling personal data of children under 14 and ban the collection of information concerning family members from the child.

The AEPD guide is available (in Spanish) at: <https://www.agpd.es/>

[portalweb/canal\\_joven/common/pdfs/recomendaciones\\_menores\\_2008.pdf](portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf).

### **UK: Retailers Using Database on Dismissed Staff Must Inform Employees**

According to the Information Commissioner’s Office (ICO), employers must notify their employees if they intend to access the newly created National Staff Dismissal Register. The database, which holds information on employees who have previously been dismissed on the grounds of theft or fraud, operates as part of an initiative by the Action Against Business Crime (AABC) in an attempt to reduce industry’s losses incurred from staff theft or fraud. Organizations must

inform employees before checking the database as well as before entering an employee’s details, which can also include details of ongoing investigations. Although the database has been criticized, the ICO assured that data protection concerns have adequately been addressed in order to prevent misuse of the data contained in the register.

Further information is available under the ICO’s Data Protections FAQs at: [http://www.ico.gov.uk/Global/faqs/data\\_protection\\_for\\_the\\_public.aspx#f4B62C0B5-ADAE-45F3-84FC-B8B2585FA38A](http://www.ico.gov.uk/Global/faqs/data_protection_for_the_public.aspx#f4B62C0B5-ADAE-45F3-84FC-B8B2585FA38A).

© 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.