THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP/US
December 2012 • Volume 12 • Number 10

Global Privacy Dispatches

## BELGIUM—Time to Comply with the Amended Telecom Act


By Jan Dhont and David Dumont

The amendments to the Belgian Act on Electronic Communications (Telecom Act) entered into force on October 1, 2012. Amongst other things, the amended Telecom Act introduces a requirement for opt-in consent for cookies and a data breach notification obligation for telecommunications providers.

**Opt-in Consent for Cookies**

Many companies use cookies on their websites for a variety of purposes. Previously, placing cookies was allowed if the user was informed about the cookie prior to its installation and if the user was granted the opportunity to object. Now, the Telecom Act requires companies to obtain the user's opt-in consent, unless the cookie is strictly necessary to transmit a communication over an electronic communication network or to provide services explicitly requested by the user. Furthermore, users must always have the opportunity to withdraw their consent easily and free of charge. In practice, this implies that companies using cookies will have to redesign their websites in a way that the user's consent can be obtained prior to installing any cookie—where the cookie use does not fall within one of the abovementioned exemptions. This may be done, for example, by implementing a banner or pop-up message requiring users to tick a box to indicate their consent to the use of cookies. Furthermore, a practical procedure needs to be implemented for users who want to withdraw their consent.

**Data Breach Notification Obligation for Telecom Providers**

The amended Telecom Act introduces a data breach notification obligation for providers of public electronic communication services (i.e. services that mainly consist of transferring signals over an electronic communication network). This implies that these providers are now required to immediately report any kind of security breach effecting personal data to the Belgian Institute for Postal Services and Telecommunications (BIPT). Furthermore, if the data breach is likely to negatively affect personal data and the privacy of clients or other individuals, these individuals should also be informed without delay, unless the company can demonstrate to the BIPT that the affected personal data is protected by information security measures, which render the data incomprehensible for unauthorized third parties (e.g. encryption techniques). Data breach notices to individuals should contain

information on the nature of the data breach, the persons or services that individuals can contact for more information, as well as the measures which individuals can take to mitigate the negative effects of the data breach. In addition, the data breach notification to the BIPT should contain a description of the consequences of the data breach and the actions which the company intends to take or has already taken to address the data breach. In practice, companies subject to the data breach notification obligations should anticipate potential data breaches, for example by preparing operating procedures and notification templates which are ready to use, since the BIPT and the concerned individuals should be notified without delay. Furthermore, it is also required to keep a register of the data breaches that contains information on the facts of the data breach, the consequences and the measures taken to address the incident.

***Jan Dhont*** *heads the Data Privacy Practice at Lorenz. He can be reached at j.dhont@lorenz-law.com.*

***David Dumont*** *is an associate with Lorenz Brussels specializing in privacy and data protection of commercial law.*