ISSUE
02

European Privacy Reporter

An Update on Legal Developments in European Privacy and Data Protection

November 2012

In This Issue

Here is the second issue of our Privacy Reporter. We have made a selection of topics on national, European and international data privacy. We hope you find it interesting.

Jan Dhont
Partner
Lorenz | International Lawyers

Direct phone +32 (0) 2 239 2008
Email j.dhont@lorenz-law.com

Time to Comply with the Amended Telecom Act

The amendments to the Belgian Act on Electronic Communications ("Telecom Act") entered into force on October 1st, 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. 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 affecting 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.

Belgian DPA Clarifies Policy on Workplace Cyber-surveillance

On May 2, 2012, the Belgian Data Protection Authority ("DPA") issued its long-awaited recommendation on cyber-surveillance in the workplace (Recommendation nr. 08/2012). This non-binding recommendation strives among other things to clarify the Belgian rules governing access to content of e-communications at work.

Accessing content of e-mails (and other e-communications) has historically been risky in Belgium. The Belgian 2005 Act on Electronic Communications requires a specific legal basis or a prior consent of all the parties involved to access private electronic communications (typically e-mails). Belgian case-law is rather polarized as to whether employers may access electronic communications, often taking the view that there are no sufficient clear legal grounds to access the content of e-communications and that an employee is not in a position to provide free consent to its employer.

In its game-changing recommendation, the DPA opines that the current legal framework provides a sufficient legal basis to access e-communication content in certain cases taking the view that accessing such content is legally authorized by the employer's general authority set forth in the 1978 Employment Contract Act. The DPA considers employee's consent to be unreliable as it may not be "freely" given.

However, the DPA highlights that such access is only allowed if it is conducted in compliance with three principles: finality, transparency, and proportionality ("Principles"). Practically, it means that the employer must pursue a legitimate and predefine purpose such as the prevention of illegal or defamatory acts, while accessing emails; employees must be

informed of the monitoring practices of the employer; the employer cannot systematically access all e-communications of its employees. Additional procedural rules (such as notice requirements, works council consultation and monitoring methodology) are specified in a Collective Labor Agreement ("CBA No. 81") and should of course be observed.

The DPA further proposes practical measures to comply with the Principles, such as:

- Consider limiting employees' use of professional email account for business related purposes in their computer use to mitigate the risk that the employer interferes with private e-communication. In this case, the employer may presume that all emails are professional and may be opened provided that the Principles and the CBA 81 have been respected. This implies, for example, that an employer can access the email account of an employee who is sick or on leave to follow up on an urgent matter, or in the context of a targeted control of compliance with the provisions of the employment contract. However, the DPA is of the opinion that the employer should allow employees to use another email address for private purposes.
- If employees are allowed to use their professional email account for business and private related purposes, additional measures should be taken to mitigate the risks that the employer interferes with private e-communications of its employees. This implies among other things that an employer should in a first phase monitor traffic data of emails, and access the content of private emails of their employees only if irregularities show up.

Overall, the recommendation signals the commitment of the DPA to confront in a practical way the challenges that arise for businesses and it is foreseeable that courts will welcome

this initiative. Therefore, it is recommended that employers draft carefully their computer use policy in a clear and transparent way.

The full text of the recommendation is available here.

Australian Privacy Reforms Under Scrutiny

Australia is set to pass reforms to its Privacy Act in 2012 granting broader supervisory and enforcement powers to the Privacy Commissioner, consolidating the obligations of the public and private sectors into a set of 'Australian Privacy Principles', and extending the extraterritorial application of privacy law. The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 has passed the lower house and is currently being debated in the Senate, where it is encountering objections from Opposition Senators.

Opposition Senators have vowed to try to soften the proposed law, taking on board industry fears that the reforms will restrict transfers of data abroad, inhibit cloud computing, prevent social media companies from sharing data with third parties, and impose unduly harsh penalties for serious breaches. Added to this are concerns that the Bill is too complex and confusing, leading Opposition sources to describe it as a dog's breakfast. At the other end of the spectrum privacy advocates have called for the Bill to be scrapped because it does not go far enough in protecting individual privacy. While all parties are eager to pass the Bill which has already been seven years in the making, it is not yet clear how long it will take to finalize the amendments and send it back to the lower house.

Other major aspects of reforms recommended by the

Australian Law Reform Commission in 2008 are to be dealt with in a second round of amendments, which are yet to be scheduled. In October the Attorney General released a discussion paper on potential mandatory data breach notifications, one of the Law Reform Commission's recommendations, which is currently only regulated in Australia by the Privacy Commissioner's voluntary guidelines. While Australians are increasingly concerned about online privacy and government retention of data, it will inevitably be some years before regulation of privacy and data protection matches the depth and breadth of European laws.

European Cloud Initiative

On September 27, 2012, the European Commission (EC) announced its intention to roll out a new strategy for uniform rules for cloud computing within the European Union (EU). The strategy is introduced in a communication from the Commission entitled "Unleashing the Potential of Cloud Computing" (Communication).

Drawing on the Momentum of Cloud Development

In its Communication, the EC points out the extensive benefits of cloud computing. As cloud computing is at early stage of development, the EC would like to take prompt action to take advantage of the timing and vanguard its future development. The EC would also like to aim at enabling and facilitating fast adoption of cloud services in all sectors of the economy. Building on the analysis laid out in the framework for the "Digital Single Market" , the EC calls on all stakeholders to participate in the development of cloud computing with a larger view to the EC Digital Agenda.

Key Action Items

The EC identifies the following three key issues where action is necessary:

- Fragmentation of the Digital Single Market due to different national legal frameworks and uncertainty on applicable law, content and the location of data.
- Issues with contracts, specifically on access, portability of data, change of control and data ownership.
- Confusion about standards due to the mass generation of standards and, conversely, a lack of certainty about which standards provide sufficient coverage for data protection, portability and data security.

A key area of concern is data protection, as there were 27 different national legislative frameworks, making it cumbersome to provide cost effective cloud solutions. Furthermore, given the global character of the cloud, there is concern about how international transfers would be regulated. The EC highlights that this concern will be addressed in the new proposed Regulation , specifically on applicable law. It reiterates that the Regulation will provide a 'level playing field' for businesses and provide a reduced administrative burden and compliance costs and give individuals a high level of protection and more control over their data. This new legal framework will also provide the foundations for the adoption of standards, codes of conduct, certification schemes for IT security and safeguards for data transfers.

The EC identifies the following three actions to deliver results with respect to cloud services within Europe:

- Standardization for cloud computing.
- Development of "safe and fair" contractual framework.
- The establishment of a "European Cloud Partnership"

to push forward cloud services in the public sector.

Standards for the Cloud

The EC envisages broad standards, certification schemes and the public support of both by regulatory authorities in order to push forward the use of cloud services within EU. Therefore, the EC will task the European Telecommunications Standards Institute (ETSI) with coordinating with stakeholders to identify (by 2013) a "detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility)". Further, the EC will work with ENISA and other organizations to develop voluntary cloud certification schemes for data protection and create a list of these schemes by 2014.

Safe and Fair Contracts

The EC desires to change the current status of the contractual legal framework for cloud services. The proposed data protection Regulation will assist in this. On top of this, the EC will:

- develop model terms for cloud SLAs between cloud providers and professional users,
- propose model contract terms for consumers and users (i.e. SMEs),
- task an expert group, including industry, to identify safe and fair contract terms for consumers and small firms,
- revise the Standard Contractual Clauses for transfers of personal data to third countries and adapt them (if necessary) for cloud scenarios and
- work jointly with industry to establish a code of conduct for cloud providers.

Cloud Services for the Public Sector and the European Cloud

Partnership

There remains fragmentation and low public sector use of cloud services, therefore the EC will set up the European Cloud Partnership (ECP) to provide for "an umbrella" at the EU member state level. The Communication states that the ECP will, together under the direction of a steering board, implement a pre-commercial procurement action to:

- identify public sector cloud requirements and
- boost joint procurement of cloud services by public bodies.

Additionally, the EC will investigate other steps for stimulating cloud services, including the establishment of a "Digital Service Infrastructures" under the proposed Connecting Europe Facility in 2014 for EU-wide cloud-based public services (e.g. business establishment, cross-border procurement, ehealth services).

The full text of the Communication can be found here.

Lorenz | International Lawyers
Boulevard du Régent 37-40 Regentlaan
1000 Brussels

Phone +32 (0)2 239 2000 | Fax +32 (0)2 239 2002 | E-mail info@lorenz-law.com |