ISSUE
01

European Privacy Reporter

An Update on Legal Developments in European Privacy and Data Protection

July 2012

In This Issue

Welcome to the European Privacy Reporter

We are happy to announce the first issue of the Lorenz European Privacy Reporter, a quarterly publication focusing on a selection of the European privacy and data protection topics. Our aim is to keep you informed of significant legal developments which affect businesses trying to comply

with the ever changing regulatory landscape of European data privacy law. We hope that you will find the publication useful.

Enjoy!

Lorenz

Jan Dhont
Partner
Lorenz | International Lawyers

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

Toolbox for Processor BCRs

On June 6, 2012, the Article 29 Working Party issued a working document on Binding Corporate Rules for data processors ("Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", hereinafter "Toolbox"). Taking initiative in the context of transfers to processors in non-adequate jurisdictions, the Working Party strives for the working document to serve as a toolbox for the requisite conditions for Binding Corporate Rules (BCRs) for processors. Although, BCRs for processors do not exist in the current legal framework, this possibility is stipulated in the new proposed Data Protection Regulation.

The Toolbox stipulates the elements that must be present in the BCR and in the application forms – it is unclear how these application forms will work in

practice, however it is safe to assume that the process would mirror closely the application process for controller BCRs. The Working Party also lists the specific commitments which must be present in the contractual relationship that must be established between a controller and processors (as stipulated by Article 17.3 of Directive 95/46/EC).

A summary of the requirements from the Toolbox for processor BCRs are summarized in the attached chart, which can be accessed here.

The Toolbox emphasizes that the contractual relationship between the processor and controller should be in the form of a service agreement (SLA). The SLA should be unambiguously linked to the BCR. First, the SLA must include that the BCR will be binding through specific reference (or as annex). Second, when transferring sensitive data, the controller must ensure that the data subjects have been informed (or will be) about the possible transfer of their data to non-adequate countries. Third, the controller should provide notice, generally, about the existence of processors outside the EU and the BCR (including availability of BCR and SLA). Fourth, as required for most contracts with processors, the SLA must include a clear description of the confidentiality and security measures. Fifth, a clear description of the instructions and the data processing should also be included. Finally, the SLA must stipulate if data may be sub-processed inside or outside the group and whether the prior approval of the controller is granted in general for such sub-processing or if approval needs to sought for each instance.

Overall, the Toolbox signals the commitment of the Working Party and the EU Data Protection Authorities

(DPAs) to confronting the challenges that arise for businesses utilizing external and non-EU based processors. Nevertheless, how quickly this will catch on with companies and businesses remains to be seen.

The full text of the Toolbox is available here.

Jan Dhont, Lead Data Privacy Practice (j.dhont@lorenz-law.com) and Katherine Woodcock (k.woodcock@lorenz-law.com).

Australia's Privacy Law Reform: A Step Closer to EU Adequacy?

Australian Privacy Regime

Australia's Privacy Act 1988 ('the Privacy Act') governs the federal privacy regime in Australia, along with other legislation relating to telecommunications, health care, government data-matching, and criminal records. Each state and territory in Australia also regulates its government agencies by way of separate legislation (apart from the Australian Capital Territory which is covered by the federal laws). The Privacy Act is overseen by the Office of the Australian Information Commissioner which is also responsible for freedom of information and information policy issues. Since 2001 the Privacy Act has also covered the private sector, however there are exemptions for most small businesses with an annual turnover under $3 million (AUD), which covers around 90% of Australian businesses. In 2012 the Australian Parliament will implement reforms to

the Privacy Act which grant more powers to the Information Commissioner and streamline some of the public and private sector obligations relating to privacy.

EU Adequacy

Under Article 25(6) of the EU Directive on data protection (95/46/EC), the European Commission can determine whether a third country ensures an adequate level of protection of personal data. A determination of adequacy is important because it enables the free flow of information between EU member states and third states, aiding business transactions and trade. Negotiations between the EU and Australia on adequacy led to the 2000 amendments to the Privacy Act which extended application to the private sector. However, in March 2001 the EU's Article 29 Working Party released an opinion expressing concern about the exclusion of small businesses and employee records from the privacy regime.

Moving closer to EU requirements, 2004 amendments to the Privacy Act introduced three main provisions:

- a clear statement that National Privacy Principle 9 (transborder data flows) applies to the personal information of non-Australians as well as Australians;
- the removal of nationality and residency limitations on the Commissioner's power to investigate complaints about the correction of personal information; and
- allowance for organizations to draft approved privacy codes which include exempt acts or

practices.

Since that time, however, the drive to obtain an EU adequacy determination seems to have faded. In 2005, in a review of the private sector provisions of the Privacy Act, the Office of the Privacy Commissioner (predecessor to the Office of the Australian Information Commissioner) reported that there was no evidence of a broad business push for adequacy, and that very few stakeholders claimed that trade was inhibited by the lack of adequacy determination. The Australian government has said it will continue working with the EU on adequacy but amendments which would address EU concerns have not yet been formulated. In a 2010 country study on Australia commissioned by the EU, it was noted that the EU Directive remains as an influential international standard in Australian law, but the small number of adequacy findings by the Commission has caused the issue to lose currency with policy-makers and the media.

First Stage of the 2012 Reforms

While they do not address all of the EU's concerns, the 2012 amendments to the Privacy Act provide more robust privacy protection and take a stronger approach to enforcement. These reforms are a partial implementation of the Australian Law Reform Commission's recommendations in a 2008 report on privacy. Due to the number of recommendations the government decided to address them in two stages of legislation. The first stage is currently before Parliament and is expected to pass without significant amendments. Reforms would come into effect 9 months after approval of the new law.

The first stage of reform introduces a number of new powers for the Information Commissioner, who will be able to:

- seek civil penalties for serious or repeated interferences with privacy;
- accept a written undertaking from an organization that they will take or refrain from a specified action. This undertaking will be enforceable in court;
- make a determination following an investigation conducted on the Commissioner's own initiative. Previously, a determination could only be made following the investigation of an individual's complaint;
- conduct performance assessments of private sector organizations handling personal information, previously the Commissioner could only audit government agencies and credit reporting agencies; and
- develop and register binding privacy codes and a credit reporting code that set out how the Act's requirements will be complied with, this power may be exercised where code developers have not complied with a request to develop a code or the Commissioner decides not to register the code that was submitted.

The reforms also introduce one set of Australian Privacy Principles (APPs, Schedule 1) to replace the separate public and private sector principles that previously applied. The APPs introduce new protections including:

- enhanced obligations on agencies and organizations regarding an individual's

access to, and correction of, their personal information;
- requiring entities to publish more comprehensive privacy policies to promote more open and transparent management of personal information;
- introducing a requirement for federal government agencies to accord higher protection to sensitive information;
- ensuring that personal information received by an entity is still protected, even where that information was not solicited by the entity; and
- introducing a new 'Direct Marketing' principle, placing extra limitations on organizations that may use or disclose personal information to promote or sell goods or services directly to individuals.

Other changes to the Privacy Act include:

- The extension of the extra-territorial application of the Act. The Act and registered codes will now apply to information practices outside Australia by any government agency, and by organizations or small businesses with an Australian link (defined in Section 5B);
- and more comprehensive credit reporting, giving credit providers access to more information about credit accounts in an individual's name in order to allow them to make more robust assessments of credit worthiness. These are joined by increased responsibilities on those providers regarding notification, data quality, access and

correction, and complaints.

Second Stage of the 2012 Reforms

A second stage of reform will address other recommendations made by the Australian Law Reform Commission (ALRC) for amending the Privacy Act. No timetable has been set for this second stage of reform, but given that it took four years for the first stage to be brought before Parliament, expectations for a rapid process are low.

Outstanding issues include possible clarification or removal of exemptions from the Act. The ALRC proposed removing exemptions for small businesses, employee records and political parties. It was also recommended to introduce mandatory data breach notifications where there is a real risk of serious harm to the individual. Currently there are only voluntary guidelines for data breaches issued by the Information Commissioner in April 2012. A statutory cause of action for serious invasion of privacy will also be considered in the second phase of amendments.

If the recommendations of the ALRC are implemented, the second stage of reforms will address the major concerns of the EU regarding adequacy and may move Australia towards a positive determination in that regard.

Jan Dhont, Lead Data Privacy Practice (j.dhont@lorenz-law.com) and Emily Hay (e.hay@lorenz-law.com).

Belgian Cookie Regulations Adopted

On June 28, 2012, the Belgian Parliament adopted the amendments to the 2005 Electronic Communications Law (hereinafter: the "Law"). This Law implements the amendments to the E-Privacy Directive 2002/58/EC (stipulated in Directive 2009/136/EC), more than a year after expiration of the implementation deadline. Prior to entering into fore, the Law needs to be ratified by the King and published in the official law journal. Nevertheless, the ratification and publication are expected in the coming weeks.

The Law amends the currently existing requirements for the use of cookies. The most important change introduced is that companies need to obtain the users' opt-in consent after providing them information regarding the purposes of the cookie and prior to the installation or use of cookies. This requirement replaces the current obligation to offer the user the possibility to opt-out (i.e. right to object to the use of cookies). The opt-in requirement does not apply on cookies that are strictly necessary and used exclusively (i) to enable the transmission of a communication over an electronic communication network, or (ii) to provide a service explicitly requested by the user. Moreover, companies installing and using cookies are also required to offer users an easy way to withdraw their consent free of charge.

Although, the initiative of the Belgian Legislator to finally implement the amendments to the E-Privacy Directive is positive, the end result of the long

implementation process is disappointing: the Belgian legislator limited itself to a formal implementation of the E.U. framework, without specifying how companies should obtain the users' opt-in consent (for example by browser settings) or which types of cookies fall within the scope of the above mentioned exemptions. Companies will struggle with these practical questions until the legislator or advisory body (the Belgian Privacy Commission) provides practical guidance on these issues. Meanwhile, companies should consult the advice of the European advisory body, the Article 29 Working Party, for more guidance regarding the practical application of the new cookie requirements (available here).

Jan Dhont, Lead Data Privacy Practice (j.dhont@lorenz-law.com) and David Dumont (d.dumont@lorenz-law.com).

Should you wish to no longer receive this newsletter, please unsubscribe instantly.

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

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