Deloitte.

International Privacy Day
Global Privacy - 2016, the Year of Reform

Global Privacy – 2016, the year of further reform

by Candice Holland
Director, Deloitte Legal

Happy New Year!

With the 28th of January 2016 being International Privacy Day and the pending European data protection reform eminent, we would like to take this opportunity to introduce our new quarterly privacy publication with a roundup of the most influential events in global privacy over the last year.

Despite the South African privacy legislation currently on hold pending further Parliamentary discussions, organisations in South Africa, particularly those with an international footprint should not put their privacy compliance efforts on hold, as privacy has become a hot topic particularly with the recent judgments against organisations who have breached their privacy obligations. You can read more about the Protection of Personal Information Act 4 of 2013 ("POPI") as well as global privacy news and judgments in our newsletter below.

Our team of leading privacy experts will keep you updated on developments in the privacy space, leveraging the Deloitte Legal global footprint and our relationship with the International Association for Privacy Professionals (the largest and most comprehensive global information privacy community aimed at helping practitioners and organisations manage and protect their data) to do so. In addition, our IAPP certified trainers and subject matter experts in data privacy compliance regularly provide compliance

assessment services and training in accordance with global standards to simplify and implement client privacy initiatives.

You can read more about Deloitte Legal and in particular, the privacy team here.

Here's to a prosperous and rewarding 2016!

South Africa - POPI promulgation delayed

The appointment of a regulator in terms of the Protection of Personal Information Act 4 of 2013 ("POPI") has been postponed, pending a workshop at Portfolio Committee level.

In December 2015, press reports indicated that on 11 November 2015, a meeting was held by the Portfolio Committee on Justice and Correctional Services to discuss the appointment of the information regulator during which it was requested that further workshops be held to further discuss the appointment of the information regulator, as well as the application of the POPI and its interaction with other legislation such as the Promotion of Access to Information Act 2 of 2000 and the Protection of State Information Bill.

Organisations should not slow down their efforts to become POPI compliant despite the delay in the promulgation of POPI, as privacy has a global, competitive impact. Globally, privacy has been a contentious topic internationally leading to the reform of the European Union Data Protection Regulations, the Safe Harbor privacy principles being declared invalid and new legislation pertaining to cyber security being promulgated in the United States of America.

Europe - Safe Harbor Declared Invalid

One of the largest upheavals in the world of privacy took place in October 2015 with the European Court of Justice ("ECJ") (in Schrems v Data Protection Commissioner (C-362/14)) declaring that the Safe Harbor agreement and privacy principles were invalid – which brought the transfer of personal information from EU member states to the United States to a standstill.

The European Data Protection Directive 95/46/EC ("Directive") prohibits the transfer of personal information of EU citizens to jurisdictions outside of the EU unless the jurisdiction to which the personal information is to be transferred, offers an "adequate level of protection" in respect of that personal information. Decision 2000/520 ("Safe Harbor decision") allowed the transfer of personal information from the EU to the US despite the fact that US was not considered to automatically provide an adequate level of protection of personal information.

Mr Schrems, an Austrian citizen, lodged a complaint with the Irish Data Protection Commissioner ("Commissioner") requesting that the Commissioner prohibit Facebook Ireland from transferring the personal information of European users of the social media application to its holding company, Facebook, Inc. which is located in the US.

Schrem put forward that the US does not offer the adequate level of protection required by the Directive due to the allegations made by Edward Snowden in 2012 that US public authorities such as the National Security Agency ("NSA") and its monitoring of electronic communications within the US.

Schrem's complaint was rejected by the Commissioner prompting Schrem to take his complaint to the Irish High Court which then referred the following two questions to the ECJ:

- was the European Commission's ("Commission") assessment as to the adequacy of the level of protection offered by the US as decided in the Safe Harbor decision of 2000 absolutely binding on national data protection authorities within the EU member states; or
- may the national data protection authority conduct its own investigation?

The ECJ held that a decision adopted by the Commission such as the Safe Harbor decision, does not prevent a supervisory body within a member state from examining the claim of a person concerning the protection of his or her rights and freedoms, particularly with respect to the processing or transfer of his or her personal information.

Further, the ECJ held that the Directive requires the third party country to which the personal information is to be transferred, to provide an adequate level of protection by means of its domestic law or international commitments. Due to the fact that the Commission did not state in its Safe Harbor decision that the US actually ensures an adequate level of protection by reason of its domestic law or international commitments, the Safe Harbor agreement was declared invalid and thus no longer in effect.

The declaration of the ECJ has disrupted all transfers of personal information from the EU to the US. There are currently plans in place to create a new version of the Safe Harbor agreement and process could be published with the new European Data Protection Regulations.

Developments in respect of the Safe Harbor agreement will be published in our next Privacy Newsletter.

Europe - Data Protection Laws Reformed

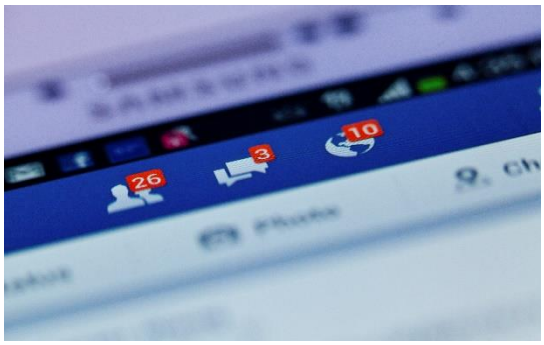
Following four years of deliberation, the European Parliament and Council have agreed to the new General Data Protection Regulation ("GDPR"), including a new Data Protection Directive ("DPD") put forward by the Commission in 2012. The new GDRP will replace the Directive which was 20 years old in favour of a new regime which is more modernised and increases efforts to protect personal information belonging to European citizens by imposing fines of up to four percent of an organisation's global revenue in the event of a breach of the GDPR's.

The GDPR's will provide new obligations in respect of various aspects of the collection and processing of personal information including the consent obtained, data anonymisation, breach notifications, trans-border transfers of personal information and the appointment of data protection officers.

Organisations with a global, and particularly a European, footprint must ensure that they are compliant with the new GDPR's as non-compliance could result in extensive penalties imposed, as well as reputational damage which has impacted many companies to date.

So what's next in respect of the reform of Europe's GDPR? EU member states must approve the new regulations, and the GDPR is expected to be formally adopted by the EU by May 2016, following which member states will have two years to adopt the GDPR into their national legislation.

Facebook fined over privacy breaches



In a judgement by the Dutch-speaking Court of First Instance, Brussels on 9 November 2015, Facebook (which includes Facebook Inc., Facebook Ireland Limited and Facebook Belgium SPRL) has been compelled to cease registering via cookies and social plug-in's, which websites internet users from Belgium (who do not have a Facebook account) visit. Facebook will therefore, no longer install the cookie file for users who are not signed in or do not have Facebook accounts in Belgium. -Facebook continues to use the data cookie outside Belgium and now the legislation recently approved by the European Commission will also give more power to national data-protection authorities to police of more internet companies.

The order remains in force, even if Facebook appeals the judgement. What this means, is that organisations can no longer use technology to follow what users do on the internet, without informing them that this tracking is being done. What makes the judgement interesting, is that the IP-address (the address-number assigned to the computer when visiting the internet) was used to monitor sites visited. The argument for and against is whether an IP-address is considered personal information – per definition, personal information is that information which is considered reasonably identifiable.

Facebook processes, amongst other things, the IP address and a "unique identifier" contained in Facebook's cookie. POPI in South Africa, specifically includes an "online identifier" as personal information and thus the tracking of an IP address would be restricted in South Africa too.

The Facebook incident in Belgium does not relate to the fundamental right of one single individual but of an enormous group of people. Similarly, in POPI, the regulator would evaluate the number of data subjects (those individuals whose personal information was collected or processed) in determining the appropriate fine.

The court in Belgium further ruled that:

- Facebook had not obtained their consent to do so;
- Facebook cannot invoke an agreement with people who do not have a Facebook-account;
- Facebook cannot invoke a legal obligation to do so; and
- the security interest pursued by Facebook is overridden by the fundamental right to privacy of people who do not have a Facebook account.

The defences in South Africa are similar (consent, legally entitled, public interest) and individuals or organisations who process or track IP-addresses would need to meet these criteria in order not to become guilty of an offense.

In the Belgium case, the Court imposed a penalty upon Facebook of €250,000 per day should it not comply with the order. In 2014 Facebook realised a turnover of $12.4 billion and a profit of $2.9 billion and is one of the most financially capable companies in the world, thus the court noted that the amount of €250,000 is a sufficient deterrent.

Contravention of the provisions of POPI may result in penalties such as fines of up to R10 million and/or imprisonment for up to 10 years. Although this has not been sufficiently tested in South African courts, one has to question, whether, like in Belgium, these penalties would apply per contravention, such as per user, and/or per day?

The gravity of the sanction imposed by the Belgian courts necessitate South African businesses to ask whether they are compliant with South African (which primarily consists of POPI) and possibly international privacy laws.

Like Belgium, should a South African business process a user's IP address (which can be used to identify a person), it would constitute the processing of a user's "personal information", and therefore the express consent of the user to do so will also be required. If so, the consequences of non-compliance with POPI may be grave indeed.

For more information, contact:

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Tel: +27 11 806 5159
Email: dechivers@deloitte.co.za

Candice Holland
Director: Risk Advisory Southern Africa
Tel: +27 11 209 8598
Email: caholland@deloitte.co.za

Mimi le Roux
Associate Director: Risk Advisory Southern Africa
Tel: +27 11 806 5456
Email: mleroux@deloitte.co.za

Samantha Buchler
Manager: Risk Advisory Southern Africa
Tel: +27 11 209 6793
Email: sbuchler@deloitte.co.za