Deloitte.

Belgium | Audit & Enterprise Risk Services | November 2015

Privacy Flash
Privacy at your fingertips

Privacy is becoming increasingly important to everyday business. Legal developments and regulators' increasing attention to privacy are two of the key drivers behind this. The aim of the Privacy Flash series is to bring to an audience eager to learning more about privacy, selected information on regulation, awareness events and initiatives related to personal data protection, as well as indicative privacy-related topics and current projects taking place.

You can find our previous issues on our website.

We hope that you will find this bi-monthly newsletter interesting. For additional information or suggestions on how to improve the Privacy Flash, or to (no longer) receive the next issue directly via email, please send an email to BEPrivacyFlash@deloitte.com.

Issue 8
November 2015

Safe Harbor invalid

Navigating the storm

Since the Court of Justice of the European Union (CJEU) nullified the EU-US Safe Harbor Framework on 6 October 2015, businesses, regulators and European rule makers have been working hard to put together an appropriate response. Our team has published an article that summarises the events of the past month and assesses the different remaining options for transferring personal data from the EU to the US: Binding Corporate Rules (BCRs), EU Model Contracts, ad-hoc transfer agreements and the derogations in the law.

EU Data Protection Reform

Update

On 9 October 2015, the Ministers in the EU Justice Council announced an overall agreement on the EU's Data Protection Directive for the police and criminal justice sector. The Directive is part of the EU's data protection reform package (together with the General Data Protection Regulation) and would protect citizens' fundamental right to data protection when their personal data is being used by law enforcement authorities. In addition, the Directive contains provisions that provide robust rules with regards to exchanges of personal data between law enforcement authorities at the European and international level.

Trilogue meetings on the Data Protection Directive for the police and criminal justice sector, as well as on the Regulation are now ongoing, with the three institutions (Commission, Council, Parliament) confirming that both negotiations are still on track for completion by the end of 2015.

At the same time, the European Data Protection Supervisor (EDPS) published its recommendations for the recitals of the General Data Protection Regulation (GDPR). Though the recitals have no independent legal value, their importance cannot be underestimated as they can be used when interpreting the scope of the substantive provisions in the text.

News

US House passes Judicial Redress Act of 2015

In a move to appease privacy concerns in Europe following the Safe Harbor ruling in October 2015, the US House of Representatives has passed the Judicial Redress Act of 2015. The Act in effect extends the rights enjoyed by US citizens under the Privacy Act of 1974 to the citizens of US allies who share data on criminal cases with the US, which includes the EU and its member states. The extension of these rights is limited and covers only records shared by the EU and other countries with US law enforcement agencies for the purpose of investigating, detecting or prosecuting criminal offenses. It does not apply to records about EU citizens that those agencies collect on their own.

The EU and the US last month agreed on an Umbrella Agreement, which creates a high-level data protection framework to regulate the exchange of personal data for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism. The passing of the Judicial Redress Act should be viewed in this context, as the EU has made it clear it will not initial the Umbrella Agreement until EU citizens have the right to enforce data protection rights in US courts. The Act will now be introduced in the US Senate.

US Senate approves Cybersecurity Information Sharing Act

On 27 October 2015, the United States Senate voted 74 to 21 to pass a bill to promote information sharing between companies and the government on cybersecurity risks. The Cybersecurity Information Sharing Act or CISA would allow companies to share “any cybersecurity threat” information with the Department of Homeland Security, who could in turn pass it on to the FBI and the NSA.

Many of the largest technology companies, such as Apple and Dropbox criticised the bill stating that they do not support a cybersecurity bill that would allow the intelligence community to collect “upstream data” from the Internet backbone more easily. Privacy advocates see CISA as a backdoor surveillance bill that would only benefit the intelligence community, as it allows companies to monitor users and share their information with the government, while exempting it from legal privacy obligations of any nature.

CISA still faces some hurdles on the way to becoming law. The bill must be conferenced together with three similar bills already passed by the House of Representatives and then voted again in the House. There could still be strong debate over the details of the bill in that process. Next, President Obama could still veto CISA, however this would be unlikely, considering the White House had already expressed its qualified support for the legislation earlier.

Privacy Bridges Report released

Just two weeks after the Court of Justice of the European Union (CJEU) declared the Safe Harbor agreement invalid for failure to protect the fundamental rights of EU citizens, the EU-U.S. Privacy Bridge Initiative released its Privacy Bridges report. The group of nineteen privacy law and technology experts from the EU and the U.S. defined 10 “privacy bridges” that can serve as practical steps towards bridging gaps between the existing approaches to data privacy of the EU and the US.

The goal of these bridges is to create a high level of transatlantic privacy protection without legislative changes on either side of the Atlantic. The Privacy Bridges report’s mission did not seek to define the legal relationships between the U.S. and the EU. Rather, its 10 bridges are meant to result in better-informed, more consistent regulatory cooperation, policy guidance and enforcement activity.

At the 37th International Data Protection and Privacy Commissioners Conference, Commissioner Jourová welcomed many of the ideas in the Privacy Bridges Report and stated “I intend to use the ideas of the Privacy Bridges project and its 10 bridges as inspiration when looking for practical ways of supporting the implementing of our own data protection rules”.

California adopts new strict Digital Privacy Law

In the US State of California, Governor Jerry Brown signed the California Electronic Communications Privacy Act on 8 October 1015, after the legislation was passed by both State legislatures in September. The law has been heralded by civil liberties groups and tech companies as the nation’s strictest privacy law, possibly setting a new standard for data protection in the US.

It requires law enforcement authorities to get a warrant from a judge to be able to access digital information from customers held by phone and internet companies. Emails, digital documents, text messages, geo-location data as well as metadata such as time-stamp, addressee and sender information are protected under the law.

Recent breaches and enforcement actions

- The French Data Protection Authority, CNIL, has fined a distributor of optical products €50,000 for violations related to the security and confidentiality of customer data.
- UK regulator the ICO has fined an online pharmacy £130,000 for selling customer details through an online marketing list company. More than 100,000 customer details were affected.

- The US Federal Communications Commission has reached a $595,000 settlement with a cable company, after it found that the company failed to properly protect personal information following a data breach last year.

Forthcoming interesting events

IAPP Europe Data Protection Congress

Brussels, Belgium, 30 November – 3 December 2015
https://iapp.org/conference/iapp-europe-data-protection-congress-2015/

Training and Workshops: 30 November – 1 December 2015
Conference: 2-3 December 2015

6th Annual Data Protection & Privacy Conference

Brussels, Belgium, 10 December 2015
http://eu-ems.com/summary.asp?event_id=266&page_id=2397

The 6th edition of a well-attended annual data protection conference. Special focus this year will be placed on the GDPR, the Safe Harbor ruling and the EU-US Umbrella Agreement.

Computers, Privacy & Data Protection (CPDP)

Brussels, Belgium, 27 January – 29 January 2016
http://www.cpdpconferences.org/

The annual Computers, Privacy & Data Protection (CPDP) conference brings together academics, lawyers, practitioners, policymakers, industry and civil society to discuss legal as well as technological developments in data protection and privacy.

IAAP GDPR Comprehensive 2016

Brussels, Belgium, 22 February – 23 February 2016
https://iapp.org/conference/gdpr-comprehensive

The International Association of Privacy Professionals (IAPP) offers an intensive two-day training course, offering a practical, hands-on view of the fundamentals of the new General EU Data Protection Regulation (GDPR).

European Privacy Academy

http://www.europeanprivacyacademy.com/

The European Privacy Academy is a unique training, knowledge and networking centre focused on the actual day-to-day management of the privacy challenge. It provides both an on-campus data protection officer course and on-campus or in-house department-specific data protection trainings during which attendees learn to efficiently manage privacy and security in a risk based and integrated manner.

The next session of the European Privacy Academy is listed below:

DPO Course – January 2016: 18 – 21 January 2016 & 15 April 2016