Deloitte.

Switzerland | Cyber Risk Services | Issue 1, January 2016

Privacy Flash
Privacy at your fingertips

Privacy today

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 is to provide regular updates on global regulatory developments, as well as relevant news and information on upcoming events in the field of data protection and privacy.

Previous issues are available on our website.

For additional information, to suggest improvements to the Privacy Flash or to subscribe/unsubscribe, please email us at deloitte.ch.news@deloitte.ch.

Issue 1, January 2016

GDPR: EU agrees on new General Data Protection Regulation

On Tuesday, 15 December 2015, the European institutions (EU Council, European Parliament and European Commission) agreed on the final text for the new General Data Protection Regulation (GDPR). The GDPR - originally proposed by the European Commission in 2012 - will replace the former EU Data Protection Directive and create a unified data protection law that will apply directly across all 28 EU Member States from 2018.

Consequences for Swiss businesses

As Switzerland is not a member of the EU or the EEA, the reform does not have a direct impact on Swiss businesses. However, the reform will still be relevant from a Swiss business perspective for any data processing undertaken by group entities located in the EU and Swiss-based companies, if they conduct business activities within the EU area and have access to personal data from their EU customers, suppliers and EU employed staff. In this context there are a few significant new requirements such as (to name only a few):

- Data breach notification within 72 hours
- Data protection officer requirements
- Sanctions of up to 4% of total annual worldwide turnover or up to EUR 20,000,000
- Unambiguous or explicit consent

Secondly, the pending **Federal Data Protection Act (FDPA) revision** will be strongly influenced by:

- The modernisation of the "Convention ratified by Switzerland for the protection of individuals with regard to automatic processing of personal data" by the Council of Europe
- The new GDPR (personal data of individuals)
- The new Data Protection Directive for the police and criminal justice sector

Although the core principles of the FDPA are expected to remain the same, and only minor adjustments of the current FDPA are required, Swiss law makers may copy large parts of the final GDPR in its revised FDPA to maintain the harmonisation of the economic area.

It will be key for all Swiss companies to familiarise themselves with the new GDPR and its requirements, to already begin assessing whether they are affected by the new rules and to start with the preparatory work (e.g. review client facing materials to ensure compliance with the new consent and transparency requirements, review and amend contracts with data processors where required) so that all necessary adjustments are made in time to comply with the new data protection requirements in the EU and Switzerland.

Next steps

While the final GDPR text has been agreed upon, the EU Parliament and EU Council still have to formally adopt it at the beginning of 2016. Following the publication of the final text of the GDPR, a two-year period will commence in which organisations and regulators will have the time to prepare for the **formal entry into force of the Regulation in Q2 2018**. This two-year transition period will be shorter in countries that choose to incorporate the GDPR in their respective country law more quickly.

Deloitte's recommendation

The final draft GDPR as published is over 200 pages in length. As with any new law, it will take time to read and understand all recitals and articles thoroughly, and see how it differs from current legislation. It is also important to remember that, while many previous official and leaked versions have been available, this is now the only version that counts. On our website we provide a first look at the main changes that the Regulation brings. We will take the time to thoroughly analyse it and its impact on Swiss-based data controllers and data processors, and we will share with you a more in-depth analysis of issues raised in due course. If, in the meantime you have any questions on the GDPR, privacy or data protection within your organisation, please get in touch with us. We understand that requirements will differ by organisation and we will be happy to provide you with tailored insights and updates.

For further information please see:

- The official European Parliament press release
- The official European Commission press release
- The official European Council press release
- The joint press conference of 21 December 2015

Agreement reached on new Network Information Security Directive (NIS)

Aside from GDPR, another important piece of legislation in the area of information security moved one step closer to becoming law. The European Parliament and Council reached an informal agreement on 7 December 2015 on the proposed Network Information Security Directive (NIS), which aims to increase cooperation between Member States and lay down security obligations for operators of digital service providers (online marketplaces, search engines and cloud computing services) and so-called “essential services”.

This scope puts public and private entities in the financial services, energy, transport, health, water and digital infrastructure sectors with more than 50 employees within the remit of the law as well.

Most importantly from a privacy perspective, the NIS Directive will introduce a security incident notification requirement that extends beyond the personal data breach notification requirements of the GDPR. While GDPR obliges organisations to report a breach only when the risk for the privacy of the data subjects is high, the NIS Directive requires operators to notify the authorities whenever a security incident (any event having an actual adverse effect on the security of networks and information systems) has a substantial impact on the provision of their services.

As with the GDPR, the NIS Directive still has to be formally adopted by both law-making institutions of the EU, the Parliament and the Council. This is expected to happen in Spring 2016, according to the European Council's press release. After the formal adoption of the Directive, the Member States will have 21 months to transpose its provisions into national law.

Provisional agreement on EU Passenger Name Record proposal (PNR)

On 10 December, the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament approved the provisional deal reached with the Council on an EU Directive that would regulate the use of Passenger Name Records (PNR) data for purposes related to terrorism and serious crime.

The Directive is not without controversy. A first proposal, which was presented to the Parliament and Council in February 2011, was rejected by the EP's LIBE Committee after intense discussions about whether the data protection principles of necessity and proportionality were met, and about the data retention period foreseen in the Directive.

The current proposal as it will be presented to the plenary session of the Parliament would oblige air carriers that operate flights between a third country and an EU Member State to hand over the PNR data to the competent Member State authorities. The Member States would then share alerts created based on PNR data and have the right to request PNR data from one another in support of specific investigations. Once formally adopted, the Member States would have two years to transpose the Directive into national law.

US passes Cybersecurity Information Sharing Act; delays Judicial Redress Act; Safe Harbour 2.0 negotiations

On the other side of the Atlantic, the US House of Representatives on 18 December 2015 passed the Cybersecurity Information Sharing Act of 2015 (CISA), a law that is being viewed by privacy advocates as a "backdoor surveillance" bill. The full text of the law was included in a 2000-page Omnibus bill that was passed to avert a government shutdown and ensure continued federal government funding.

Meanwhile, the Senate's Judiciary Committee has moved discussions on the Judicial Redress Act into the new year. The Act would extend privacy rights enjoyed by US citizens to the citizens of some of the US' most prominent allies (including the EU). Extending EU citizens in particular a right to redress would go some way towards addressing the concerns that the EU's highest court expressed in its October judgement on the EU-US Safe Harbour Framework.

Negotiations between the EU and the US on a successor for the Safe Harbour Framework are reportedly still underway. The responsible European Commissioner Vera Jourová has reiterated during a press conference on GDPR that reaching an agreement before the announced deadline of 31 January 2016 is still "realistic". Mrs. Jourová however did not specifically comment on whether the approval of the Cybersecurity Information Sharing Act (CISA) would have a negative influence on the negotiations.

Belgian court ordered Facebook to stop tracking internet users who do not have a Facebook account

On 9 November 2015, a Belgian court ordered Facebook to stop the processing of personal data of internet users from Belgium who do not have a Facebook account. The court case was launched by the Belgian DPA, the Privacy Commission, in response to the findings of a study that it had commissioned, which found that Facebook tracked internet users without a Facebook account through so-called "datr"-cookies. The court ordered Facebook to stop this practice before 14 December 2015, placing a penalty of €250,000 per day for non-compliance after that date.

Facebook responded to the order by making its public pages unavailable to visitors who are not logged in on the social media platform. It argued in a post on its website that the datr-cookie is

necessary to keep the website secure, and that security for Facebook and its Belgian members cannot be guaranteed without using the datr-cookie. Facebook also stated that it would go into appeal.

In response to this move, the Belgian, French, Spanish, Dutch and Hamburg DPAs issued a common statement, urging Facebook to take measures to comply with the court ruling across the EU as soon as possible.

Dutch DPA issues guidelines on data breach notification

As reported in the Belgian Privacy Flash issue 5, the Dutch government has opted not to await the entry into force of the General Data Protection Regulation and has already moved ahead with introducing a data breach notification requirement by amending its existing privacy law. The requirement will enter into force on 1 January 2016 and will be subject to fines up to €820,000. To help organisations in the Netherlands prepare for the new requirements, the CBP has published guidelines detailing the scope of the notification duty and answering frequently asked questions (in Dutch).

Recent breaches and enforcement actions

- A large health insurance provider settled for $3.5 million with the US Department of Health and Human Services, which had initiated investigations into the company's compliance with HIPAA rules.
- In the UK, a broadsheet newspaper was fined £30,000 by the ICO for infringing direct marketing rules. The newspaper had urged readers who had opted out of direct marketing messages to vote Conservative in the run-up to the May 2015 elections.
- The US regulator in charge of privacy, the Federal Trade Commission (FTC), has agreed to its largest settlement ever, with a company that provides identity theft protection. The FTC alleged that the company amongst others falsely advertised that it protected customers' data with the same high-level safeguards as financial institutions.

Privacy events around the globe

Computers, Privacy & Data Protection International Conference

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.

General Data Protection Regulation: Where are the Teeth of the Tiger?

Deloitte Academy, Zurich, Switzerland, 3 February 2016
IAPP Knowledge Net - GDPR

The International Association of Privacy Professionals (IAPP) and Deloitte Switzerland invite for an interactive panel discussion with data privacy experts from Belgium and Switzerland, offering a practical, hands-on overview of the new General EU Data Protection Regulation (GDPR) and its impacts on the Swiss business landscape.

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 sessions of the European Privacy Academy are listed below:
DPO Course – January 2016: 18 – 21 January 2016 & 15 April 2016

For further information or an individual consultation on how our Cyber Risk Services experts can help you, please do not hesitate to contact us.

Mark Carter
Managing Partner, Risk Advisory
markjcarter@deloitte.ch

Dr. Klaus Julisch
Director, Cyber Risk Services
kjulisch@deloitte.ch

Deloitte AG
General-Guisan-Quai 38
8022 Zurich
Switzerland