Deloitte.

Switzerland | Cyber Risk Services | January 2016

General Data Protection Regulation
EU agrees on new Privacy 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.

Changing the privacy landscape for businesses

With the new Regulation, the EU intends to strengthen citizens' control over the use of their personal data, while simplifying the regulatory landscape for business. A **"one-stop-shop" mechanism** will allow individuals to make complaints about the misuse of their data with the Data Protection Authority (DPA) in their home country, rather than where the company is

based. Individuals will also be able to join in class action suits through representative organisations (such as consumer protection organisations), who if allowed by national law, may also act on their own initiative.

Companies will be obliged to **notify data breaches** to the competent supervisory authority without undue delay and not later than 72 hours after discovering it. One way to avoid infringements is to implement appropriate technical measures (e.g. pseudonymisation) prior and at the time of processing to ensure compliance with data protection principles (**Privacy by Design**, described below). In the event of non-compliance with the law or infringements of individuals' rights, **companies can expect administrative fines of up to 20 million euro or 4% of their total global annual revenue**. All DPAs will get the power to issue such enforcement actions, either directly or through national courts.

Public authorities and bodies that process personal data; organisations whose core activities require regular and systematic large-scale monitoring of individuals; and organisations where large-scale sensitive personal data processing takes place, will now have to appoint a **Data Protection Officer (DPO)**. In addition, national law may require other organisations to appoint a DPO. A DPO's main tasks will consist of monitoring compliance with the privacy principles set by the GDPR, and managing the relationship with both data subjects (employees, customers) and the supervisory authorities.

To ensure that privacy is taken into account throughout the business and at the start of each new process or project that involves the use of personal data, the GDPR introduces the concept of **Privacy by Design**. To ensure that this principle is implemented, the Regulation obliges organisations to carry out **Data Protection Impact Assessments (DPIAs)** before the processing starts, if the processing is considered high-risk for the rights of individuals.

Aside from reaffirming core privacy principles such as purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality; the Regulation shifts the regulators' focus towards **accountability**. This implies that the data controller shall be responsible for, and be able to demonstrate, compliance with the Regulation. Privacy and information security policies and procedures, personal data processing records (such as inventories or data flow mapping), documented training and awareness programmes, Data Protection Impact Assessments and compliance/audit plans will be considered key elements in this respect.

Strengthening citizen's fundamental rights

One of the main 'raisons d'être' for the new Regulation is the EU's aim to restore consumers' trust in how data is processed in an online environment. The law therefore reaffirms that citizens have a **right to be forgotten**, which will require businesses to erase personal data when requested to do so, provided certain conditions are met. In the event a business offers

online services (e.g. e-commerce, social media) to a child, the **age of valid consent** has been set at 16. Individual Member States can however lower this age in their jurisdiction, to as low as 13.

Member State law may still create differences

While the GDPR is intended to streamline data protection laws in the European Union, a complete harmonisation has not been established. The Regulation allows the Member States to go beyond the Regulation in several areas, including to determine in which additional circumstances a DPO must be appointed. DPOs and other privacy compliance officers should therefore continue to monitor changes to national privacy legislation in the Member States as well.

Consequences for Swiss businesses

As Switzerland is not a member of the EU or the EEA, the reform of the European data protection law does not have a direct impact on Swiss businesses. However, the reform will still be relevant from a Swiss business perspective as follows:

The new EU data protection regime will be directly relevant 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

Ultimately, all three new European provisions follow the same principles. 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.

Independent from the FDPA revision, the new EU data protection regime will be directly relevant for many 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. **It will also be key for all Swiss companies to familiarise themselves with the new GDPR and its requirements, to already begin assessing if they are affected by the new rules and to initiate 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.

What's next?

While negotiators of the European Council and the European Parliament reached an agreement on the final text of the Regulation, both institutions still have to formally adopt it.

The responsible Parliament Committee has passed the GDPR with 48 votes for and 4 against on 17 December 2015, which means the Regulation will be presented to the full plenary session of the Parliament in the first months of 2016. In addition, the heads of state of the EU Member States are scheduled to meet in February 2016, and are likely to vote on the Regulation then.

As soon as both the Parliament and the Council have formally adopted the final text and the GDPR is published, 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.

Date	Legislative step
25 Jan 2012	European Commission proposes a new GDPR
12 Mar 2014	European Parliament approves amended draft
15 Jun 2015	Council of the European Union amends draft further
16 Jun - 15 Dec 2015	Trilogue discussions between Parliament, Council and Commission
15 Dec 2015	Trilogue agreement on the GDPR reached
17 Dec 2015	European Parliament LIBE Committee adopts the GDPR
18 – 19 Feb 2016	European Council expected to formally adopt the GDPR
Mar - Apr 2016	European Parliament plenary expected to formally adopt the GDPR
Q2 2016	Expected publication of the GDPR in the Official Journal of the European Communities
Q2 2018	Formal entry into force of new GDPR

Detailed analysis to follow

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. At Deloitte we'll take the time to thoroughly analyse it and its impact on Swiss-based data controllers and data processors, and we encourage you to do the same. A more in-depth analysis of issues raised will be published in due course.

Our team is in constant contact with the leaders of the Global Deloitte Privacy Practice and the Data Protection Authorities regarding the GDPR's emerging impact and consequences, to ensure we can advise global clients on the next steps to take. As privacy requires a legal, technical and organisational approach, our multidisciplinary privacy team consists of specialists in a number of disciplines who together provide comprehensive, all-round solutions.

In the meantime, if 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'll be happy to provide you with tailored insights and updates.

For more information, please contact:

Mark Carter
Partner | Cyber Risk Services
Email: markjcarter@deloitte.ch

Klaus Julisch
Director | Cyber Risk Services
E-mail: kjulisch@deloitte.ch

Deloitte AG
General-Guisan-Quai 38
8022 Zurich
Switzerland