European Union General Data Protection Regulation

The EU's New & Draconic Privacy Regime is just a few Weeks away

Being compliant with the new legal regime of the GDPR is a major challenge businesses face when using data connected with countries in the EU. Here is a summary of the most important issues.

November 2017, Dr. Jan Tibor Lelley

The Charter of Fundamental Rights of the European Union, Article 8, protects everybody's personal information. Effective May 24, 2016, the EU's **General Data Protection Regulation ("GDPR" or "the Regulation")** began to protect this right in the digital age.

One of the most important new developments from the GDPR is that the same rules apply to all companies, regardless of where they are incorporated. The EU felt that European companies have to adhere to stricter standards than companies established outside the EU, but that are also doing business in the EU. Under the Regulation, companies based outside of Europe will have to apply the same rules when they offer goods or services in the EU market. The EU wants to create a level playing field for all businesses.

The Regulation will be **enforceable** starting **May 25, 2018**. This means that all globally based companies offering goods or services in the EU have to fully comply with the Regulation by that date, at the latest.

What is personal data – scope of enforcement?

The scope of information regarded by the EU as personal data and, therefore, protected by the Regulation is extremely broad. Personal data is any personal information, which can be used to identify an individual, directly or indirectly, such as his/her name, telephone number, email address, place and date of birth, etc.

What personal data do most companies hold?

Under the Regulation, the vast portion of HR data used by employers meets the broad definition of protected personal data:

- Monitoring employees' use of email and social media;
- Conducting investigations and obtaining personnel information and personal data of employees;
- Trans-border data flow;
- Use of police and criminal justice data.

What are international businesses' duties under the Regulation?

The Regulation provides an extensive (it includes 99 articles) and dense legal framework. Companies that have personal data must:

- ensure that the **individual rights of data subjects** are observed (i.e. inform individuals whose data is processed and give access to individual's data);
- … ensure that data is **collected only for** specified, explicit and **legitimate purposes**, kept accurate and up to date, and maintained for no longer than is necessary;
- … ensure that the Regulation's criteria for **making data-processing legitimate** are observed (for example, obtaining an individual's consent for using his/her data);
- … ensure **confidentiality and security** of the data processing;
- … ensure that when a **transfer of data occurs to the US**, an adequate level of protection is guaranteed (for example, by using EU standard contract clauses or by using the EU-U.S. Privacy Shield Program);
- … ensure the **Right to be Forgotten**: if individuals no longer want data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted;
- … ensure **easier access to data**: Individuals can ask for information on how their data is processed and this information should be available in a clear and understandable way;
- … ensure the **right to data portability**: individuals are allowed to transmit personal data more easily between service providers;
- … ensure the **right to know** when **data has been hacked**: Companies must notify the EU Supervisory Authority of data breaches that put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures;
- … ensure **data protection by design and by default**: 'Data protection by design' and 'Data protection by default' are safeguards to be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm (e.g. on social networks or mobile apps).

Stronger enforcement of the rules:

The EU data protection authorities and regulators will be able to **fine companies** that do not comply with EU rules up to **€ 20 Million/$ 21 Million or up to 4%** of their **global annual turnover**.

What is the timeframe by when businesses must be in compliance?

The Regulation went into effect on May 24, 2016, but enforcement begins on **May 25, 2018**. It is expected that the authorities will immediately begin to investigate and fine non-EU businesses to set an early example.

Regulators have already been flexing their muscle with high fines for EU businesses violating privacy rights. In 2015, they fined a German national insurance company € 1.3 Million ($1.4 Million) for more minor privacy violations. Other recent examples are Spain fined € 900,000 ($1.0 Million) and France fined € 150,000 ($168,000).

If you have locations in the EU, now is the time to find out your options for compliance.

Contact:

Dr. Jan Tibor Lelley
E-Mail: lelley@buse.de | Tel: +49 201 1758-0

Web Version: http://buse.de/en/insights/european-union-general-data-protection-regulation/