White Paper

GDPR: A Right and A Duty

Fabienne Lens, Director, Regulatory Compliance, CTG Europe

Reliability Matters

The **General Data Protection Regulation (GDPR)** became effective on May 24, 2016. This new European law aims to protect the personal data of individuals in the EU. Although it is a European law, the impact is global: any organization that processes personal data of EU citizens and visitors must comply with GDPR.

Why Was This Law Established?

Quite simply, Europe was not ready to protect its citizens in our rapidly evolving globalized economy. First, a European directive was translated into a national legislation for each member country of the EU. The initial scope of this regulation allowed too much flexibility for EU members to determine how they would apply certain rules, which led to a lot of differences in interpretation and considerably limited the growth of the digital market worldwide.

What Are the Advantages of GDPR?

By harmonizing the rules for all member countries, the EU hopes to enable more freedom of movement of personal data and to simplify international commerce. The new legislation scope simplifies the ability of companies to process personal data across borders. This will undoubtedly contribute to more honest competition within Europe. Moreover, international players will now need to communicate with only one supervisory authority. Previously, the translation of the directive differed per country. Under GDPR, this has been replaced by one unified legislation. Today, organizations must abide by the supervisory authority of the country where either their main establishment or representative in the EU is located. The EU calculated a global saving of 2.3 billion euro for companies!

The GDPR clearly defines the rights of EU citizens with regard to their own personal data. This new legislation is very much in support of the citizen versus the business community. Studies demonstrated just how urgently this legislation was needed—only 15 percent of the investigated population felt that they had control of their online identity. Under GDPR, individuals now have many more rights. Not only is this law focused on improving the protection of their personal data, but also on stricter control over the processing of this data. From now on, companies are obligated to ask explicit permission with regard to disposal of an individual's data. Additionally, full data transparency is now required and the citizen has the right to "be forgotten" or to have his/her data transferred to another party. Minors have also been granted extra protection under GDPR statutes.

Is Two Years Enough Time to Implement GDPR?

This significant new legislation only granted affected companies two years to get things organized. Organizations that collect the personal data of individuals in the EU must meet the requirements of this regulation by May 25, 2018. This legislation represents the first time that such a sweeping a law has been so uniformly enforced on a European level. Never before has a law had the impact that GDPR will: it will affect all departments of an organization.

Organizations that employ a big work force, work with highly sensitive information (e.g., patient or health data), or deal with large amounts of personal data are facing the biggest challenge.

For organizations that are already active in highly regulated environments, there may be less work to be done. These organizations are already used to meeting strict rules and remaining in compliance. For others, however, many things remain unclear regarding the exact consequences of this new regulation and the exact measures they are expected to take. Supervisory authorities, like the Belgian Privacy Commission, have developed plans that describe the steps organizations must take in order to be compliant. These step-by-step plans have been beneficial guidelines, however, the need for substantial advice and guidance around the execution of GDPR compliance projects remains necessary. Each organization will have its own unique needs when it comes to achieving full GDPR compliance.

Haven't Started Yet? What Now?

There is only one message for anyone who has neglected GDPR until now: time's up! The only solution at hand consists of developing a thorough assessment of the present situation. Which personal data does the company process? Where are these filed? Who has access to this data? Is the level of data protection sufficient? Briefly, what does the data flow look like and what are the risks involved?

The analysis should also reveal the regulatory requirements that have not been met yet and where improvements can be made. A solid plan will help formulate a solution for areas that need to be addressed and solidify priorities, actions, and deadlines with regard to remediation of possible obstacles in all departments involved. If you already have a detailed view, you are certainly in an excellent position to start.

As each situation is different, companies are encouraged to seek assistance from an expert who is both knowledgeable in this legislation and has the necessary understanding of IT to translate the regulatory requirements to their specific needs. Furthermore, it is important that everyone within the company receives training, whether it is an awareness training or a training with regard to the execution of specific actions in case of a data breach.

It goes without saying that both appointing the person responsible for this as well as the allocating the required budgets require priority.

Does Each Organization Need to Employ a DPO?

Companies or organizations that frequently process sensitive data or the analysis of personal data will be obligated to appoint a Data Protection Officer (DPO) under GDPR. Government institutions must do so by default, regardless of their activities.

The job of the DPO consists of supporting companies, organizations, or government institutions with GDPR compliance. The DPO must have the required knowledge and expertise to implement the GDPR correctly, train the staff, provide GDPR compliance advice, and work with the organization to deal with compliance issues and maintain overall compliance. The DPO also acts as a champion of this new regulation within their organization. Ideal candidates for this job include those with a legal background or with thorough compliance experience, but equally important—a healthy affinity for IT. However, most important is the deep rooted eagerness of a DPO to take on GDPR compliance.

A DPO must also remain independent in their work and judgement. For this reason, many organizations have found benefits in utilizing external parties to fill these roles.

Sanctions or Scaremongering?

Not abiding to this law certainly is not an option: the penalties are very high. If you are not compliant with GDPR, you will find yourself in one of the following sanction categories, depending on the nature of the breach:

- A fine of 10 million euros or two percent of the global annual revenue
- A fine of 20 million, i.e., four percent of the global annual revenue

In both cases, the highest possible sanction will be issued.

The Belgian Privacy Commission will most likely not use these big penalties right away. It is also important to note that the Commission recently acquired a set of new responsibilities as well. In addition to their initial role as advisors, they will now also perform audits and issue sanctions as necessary. Thus, faced with their own workload challenges, they understand that becoming compliant takes time, effort, and money. However, make no mistake, companies must work diligently to get everything under control. If you can provide a solid plan and demonstrate that it is being followed accurately, this will certainly be a big advantage in the case of complaints.

Published by Computer Task Group, Inc.

Backed by more than 50 years of experience, CTG (NASDAQ: CTG) has a proven track record of reliably delivering high-value, industry-specific staffing services and solutions to its clients, including IT staffing, application management outsourcing, consulting, and software development and integration solutions. CTG combines in-depth understanding of our clients' businesses with a full range of integrated services and proprietary ISO 9001:2000-certified service methodologies. CTG has operations in North America, Western Europe, and India. The company regularly posts news and other important information online at www.ctg.com.

 Rev. 05/18