Time for EU Corporates to Act on Data Protection

Edith Rigler, gtnews Freelance Consultant - 3 March 2015

Given the recent epidemic of data breaches, a proposed new Data Protection Regulation from the European Union (EU) is underway. Data protection is an underestimated topic and corporates that haven't already started preparing themselves for the new rules need to move quickly.

Mention the phrase "data protection" to someone and you are likely to receive a big yawn. Add the fact that 28 January was European Data Protection Day and you're just as likely to get a puzzled reaction. You will hear the comment that data protection is a dry subject, which is neither of great relevance or interest. At most, the subject is seen to be relevant to banks - after all, they hold financial data on their customers such as account numbers, balance information, risk and investment preferences, as well as personal information such as names, postal and email addresses and telephone numbers. But data protection as a subject of interest to corporates?

Yet data protection and security should concern everyone, be it an individual, a business, a bank or a public authority.

Data Breaches: The New Normal

Consider the recent news about data breaches - 2014 has been called *the* year of major data breaches. They happened everywhere and no-one was exempt: public authorities, corporates and banks were all targets.

The impact of data breaches is significant, not only for individuals - who may lose money or may have to spend much time trying to retrieve their data - but above all for corporates. Surveys have found that the scale and cost of data breaches have nearly doubled in recent years. First, there is the direct cost such as having to as having to notify your customers of a data breach, followed by investigating and controlling the breach, potential litigation (dealing with lawsuits arising from customers), and last but not least regulatory fines.

However, the intangible costs may be even more significant. They include damage to the corporate brand, potential loss of customers, lost business opportunities and a decline in share value. Research reveals that reputation and the loss of customer loyalty does the most damage to the corporate bottom line.

Corporates are at risk if hackers attempt not only to steal their customer data, but also destroy company systems, complete with all the data. Following such a breach, a corporate may no longer be able to operate. There is also the risk that corporates´ proprietary information such as product designs, finance and strategic plans may be stolen.

Corporates´ Dilemma

Corporates find themselves in a dilemma: for one, data is essential for their economic activities. Companies collect data, aggregate it and analyse it. Understanding data about

their customers and their activities and preferences is important for businesses of all types and sizes to be able to develop better and more targeted products.

The conclusion is of course that corporates must protect the data which they hold on their customers, and that is not a new thought. Across the EU, everyone has the right to the protection of personal data concerning him or her, as laid down in Article 8 of the 2000 EU Charter of Fundamental Rights. Consumers have benefited from data protection laws in the form of an EU Directive since 1995, but over the subsequent 20 years there have been tremendous changes in terms of technology and consumer behaviour. No wonder that the 1995 Directive can no longer represent the digital age.

The EU's new General Data Protection Regulation (GDPR) has therefore been proposed in response, and appears likely to be finalised later this year. Who is impacted, what are its goals, who benefits and what will it mean for corporates?

Corporates Stand to Gain from the new Regulation

The regulation will apply to any company holding personal data on customers/consumers residing in the EU, where 'personal data' could be names, email addresses, payment details, social networking posts, medical information and/or internet protocol (IP) addresses. It will therefore have a major impact on many industries - from technology, media and telecommunications companies, to retailers, e-commerce and payment services providers.

There are three key elements which will benefit corporates:

1. The first is colloquially referred to as "one continent, one law", which means that there will be one set of data protection rules for all of the EU's member states rather than 28 different ones. Companies wishing to enter a new market will find it easier to do so. Those already operating in multiple jurisdictions will no longer have to deal with multiple rules and regulations.
2. The second key element is referred to as "one-stop-shop for data protection". For businesses, this means having to deal with one single data protection authority rather than 28 different ones, thus cutting red tape and costs.
3. The third element refers to "same rules for all companies". Today, European companies have to adhere to stricter standards than their competitors established outside the EU but who also do business in the single market. With the new regulation, companies based outside of Europe will have to apply the same rules as those within the EU. This eliminates the competitive advantage of corporates outside the EU.

What Will Corporates have to do?

There are several key activities corporates need to undertake to prepare for the proposed GDPR:

- First, establishing a "data protection culture" within the company. This entails raising the awareness of internal staff and setting accountability goals. Recent surveys have shown that in many businesses, IT professionals are not aware of the pending regulation. They need to review and bolster their data processing policies and practices now. This is particularly

relevant since the GDPR will carry penalties (fines of up to €100m or 5% of global turnover - whichever is greater) in the case of non-compliance.

- Second, corporates must ensure that they have appropriate internal procedures in place. These will include assessing the data being collected and held by the company; aiming to minimise data processing and data retention; building in safeguards to all data processing activities; and ensuring that processes for data breach notifications to the regulator are in place.
- Third, it will be necessary to communicate with the corporate's customer base. Customers need to be educated in order to understand their rights regarding the data that corporates hold on them.
- Fourth, if corporates operate across borders outside the EU, they must ensure that they have a legitimate basis for transferring personal data to jurisdictions outside the EU that are not recognised as having adequate data protection regulation.

Take Action Now

To summarise, cybercrime and data breaches are on the rise. At the same time public concern over the safety of data has increased - although not yet to the level one might expect in view of the frequency and size of recent incidents.

The good news is that data protection regulation is in the works. This should ensure that more stringent procedures will become mandatory for organisations which hold data on their customers. For corporates, the time to act is now, before the new regulation is adopted.