Chapter 87
Analysis of the US Privacy Model:
Implications of the GDPR in the US

Francisco García Martínez
Illinois Institute of Technology, Chicago, USA

ABSTRACT

The creation of the General Data Protection Regulation (GDPR) constituted an enormous advance in data privacy, empowering the online consumers, who were doomed to the complete loss of control of their personal information. Although it may first seem that it only affects companies within the European Union, the regulation clearly states that every company who has businesses in the EU must be compliant with the GDPR. Other non-EU countries, like the United States, have seen the benefits of the GDPR and are already developing their own privacy laws. In this article, the most important updates introduced by the GDPR concerning US corporations will be discussed, as well as how American companies can become compliant with the regulation. Besides, a comparison between the GDPR and the state of art of privacy in the US will be presented, highlighting similarities and disparities at the national level and in states of particular interest.

INTRODUCTION

Last May 25th, 2018 the General Data Protection Regulation (GDPR), the most shocking privacy law in Europe, and perhaps in the whole globe, became of full application. Although it is commonly wrongly said that last May was the date when the GDPR was enacted by the EU, truth is that it has been already effective for two years, since April 14th, 2016. The regulation had given European companies two entire years to become compliant. Thus, it is from May 25th, 2018 when every enterprise dealing with privacy data of European citizens must be fully compliant with the General Data Protection Regulation. Otherwise, they would have to face thrilling fines.

DOI: 10.4018/978-1-7998-8954-0.ch087

Nonetheless, one of the key things that need to be highlighted from this complex regulation is that not only European companies are affected by this new data protection law, but also foreign companies that do business in the EU. Numerous non-EU companies are now wondering whether they must follow the severe inflictions of the GDPR or if the European regulators are truly going to take serious actions.

What scares the most American companies are the penalties established by this new privacy law, which can go up to the higher of 4% of the company´s worldwide revenue or 20 million euros. However, European regulators recognize what they call good faith. This means that enterprises are not getting fined right away if they do not completely comply the regulation. Instead, the consensus is that EU regulators go slowly at first giving warnings before imposing the striking penalties (Cornock, 2018).

GDPR MOST SIGNIFICANT UPDATES

Apart from the already mentioned increased penalties, the General Data Protection Regulation has included many other updates that directly affect US companies with businesses in Europe. This is, in fact, the most important update: every non-EU organization must be compliant with the regulation when they conduct activities related to the collection and treatment of private data to EU citizens ("Regulation (EU) 2016/679 of the European Parliament and of the Council," 2016).

With the goal of preserving the security and liability of the enterprise, as well as of offering guidance to technology professionals, controllers have to designate a qualified individual called Data Protection Officer (DPO) in the following scenarios ("Regulation (EU) 2016/679 of the European Parliament and of the Council," 2016):

- Processing is carried out by a public authority, except a court acting in the exercise of its judicial function;
- The main activities consist of processing operations which, by reason of their nature, scope and/or purposes, require routine and systematic observation of subjects of large-scale data;
- The main activities consist of the large-scale processing of special categories of personal data and of data relating to convictions and criminal offences.

Another great way of preserving the security and minimizing risks is by performing a Privacy Impact Assessment (PIA). This is basically a risk assessment to better know the potential risks to which an organization is exposed based upon the type of activities that it does with the personal data. Specifically, the GDPR defines that a PIA must be performed, at least, in any of the following cases ("Regulation (EU) 2016/679 of the European Parliament and of the Council", 2016):

- The company's activities involve profile elaboration;
- The company treats large scale sensitive data;
- The organization systematically observes great scale data of public areas.

The General Data Protection Regulation introduces a new principle, called "accountability", that implies a cultural and organizational change in enterprises. Thus, this principle states that companies should have a proactive and preventive attitude, instead of a reactive one, considering security as a part of their business model and demonstrating it. Besides, the regulation defines two key concepts related