COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

EU General Data Protection Regulation: Changes and implications for personal data collecting companies

*Christina Tikkinen-Piri, Anna Rohunen *, Jouni Markkula*

University of Oulu, Finland

Keywords:
General Data Protection Regulation
GDPR
Data Protection Directive
Personal data

A B S T R A C T

The General Data Protection Regulation (GDPR) will come into force in the European Union (EU) in May 2018 to meet current challenges related to personal data protection and to harmonise data protection across the EU. Although the GDPR is anticipated to benefit companies by offering consistency in data protection activities and liabilities across the EU countries and by enabling more integrated EU-wide data protection policies, it poses new challenges to companies. They are not necessarily prepared for the changes and may lack awareness of the upcoming requirements and the GDPR's coercive measures. The implementation of the GDPR requirements demands substantial financial and human resources, as well as training of employees; hence, companies need guidance to support them in this transition. The purposes of this study were to compare the current Data Protection Directive 95/46/EC with the GDPR by systematically analysing their differences and to identify the GDPR's practical implications, specifically for companies that provide services based on personal data. This study aimed to identify and discuss the changes introduced by the GDPR that would have the most practical relevance to these companies and possibly affect their data management and usage practices. Therefore, a review and a thematic analysis and synthesis of the article-level changes were carried out. Through the analysis, the key practical implications of the changes were identified and classified. As a synthesis of the results, a framework was developed, presenting 12 aspects of these implications and the corresponding guidance on how to prepare for the new requirements. These aspects cover business strategies and practices, as well as organisational and technical measures.

1. Introduction

The European Parliament voted on the General Data Protection Regulation (GDPR) in May 2016. The GDPR will come into force and replace the current Data Protection Directive 95/46/EC (hereinafter DIR95) in May 2018. It will improve data subjects' privacy protection and facilitate organisations' and companies' work through its clarified rules, more concretised requirements and even direct instructions on the provisions'

* *Corresponding author.* University of Oulu, Faculty of Information Technology and Electrical Engineering (ITEE), Empirical Software Engineering in Software, Systems and Services (M3S) research unit, P.O. Box 500, FI-90014 Finland.
E-mail address: anna.rohunen@oulu.fi (A. Rohunen).

http://dx.doi.org/10.1016/j.clsr.2017.05.015

implementation. On the other hand, the GDPR's new obligations bring considerable changes to companies' privacy protection implementation. All companies handling EU residents' personal data or monitoring data subjects' behaviour within the EU, regardless of where they are based, will be governed by the GDPR. This indicates that non-EU and international companies will have to comply with both their national legislation and the GDPR. Since its adoption in 1995, DIR95 has been the central legislative, personal data privacy instrument in the European Union (EU). The GDPR has been under development since 2009, and the European Commission officially published a proposal for the data protection reform in early 2012 (de Hert and Papakonstantinou, 2016). In 2018, the GDPR will finally come into force after this multiphase law-making process. The GDPR aims to improve the level of personal data protection and harmonisation across the EU as DIR95 no longer meets the privacy requirements of the present-day digital environment.

Data privacy legislation has been evolving with the development of personal data collection and processing technologies since the rapid progress in electronic data processing began in the 1960s. In Western countries, legislation on personal data privacy was established at that time, in both Europe and the United States (US). The first means of ensuring data privacy were the data protection act passed by the German federal state of Hessen in 1970, the Swedish data protection act adopted in 1973 and the Fair Information Practices (FIPs) formulated by the US government in 1973. Since then, several other initiatives on privacy regulation have been launched. Many of them have applied and further developed FIPs, such as the Organisation for Economic Co-operation and Development (OECD) guidelines, DIR95 and now the GDPR, with the FIP-based Privacy by Design and Privacy by Default (PbD) principles.

Rapid technological development due to the convergence of calculation power progress, increased storage capacity and advanced network technology makes it possible for companies to collect, process and interlink data in an expanded way. They increasingly tend to use these data for various purposes, such as personalised services and marketing. As a result of technological development, along with globalisation, new and increased challenges for personal data protection have emerged (Reding, 2010). Although new technologies and services benefit both businesses and consumers, they also generate serious privacy risks. This situation may decrease people's trust in companies that collect data for their service production. The lack of trust can slow down the development of the innovative use and adoption of new technologies (Reding, 2010), and many new business opportunities may be missed if appropriate data protection practices are not implemented.

The GDPR aims to meet the current challenges related to personal data protection, strengthen online privacy rights and boost Europe's digital economy. It specifically aims to provide individuals with better capabilities for controlling and managing their personal data (Mantelero, 2013), hence striving to reinforce the data subjects' trust in personal data collecting companies. Within the new data protection framework, individual service users may also benefit from the free movement of data if it results in growing businesses with improved and personalised services.

The companies collecting, processing and utilising personal data are required to comply with the data privacy legislation. They should now proactively prepare for the changes that the GDPR brings and adapt to these changes within a given time span. Implementing data privacy in business operations is often challenging as such. For example, PbD rests on a proactive approach to privacy and privacy assurance as the organisation's default mode of operation (Cavoukian, 2009). It promotes embedding privacy into the design of information technology systems and business practices by default in a data-minimising way. The adoption of PbD principles in systems design has proven demanding, although there are specified means for achieving PbD goals (Spiekermann, 2012). Data privacy implementation also deals with a complex whole, covering different aspects, including company-level awareness raising and training, adoption of organisational and technological data protection measures, and documentation of processing operations. In parallel with putting these into practice, personal data utilisation and processing should be enabled in a way that benefits companies. In this light, companies clearly need substantial amounts of time, resources and guidance to implement data privacy.

A major challenge related to the implementation of the GDPR is the companies' lack of awareness and understanding of the forthcoming changes and requirements that the GDPR imposes through its new rules. These requirements have various practical implications for organisational processes and practices, technological system design, as well as personnel training and assignment of new responsibilities in the organisations. Such demands bring out the need to review and revise current data privacy practices and technological data protection measures, as well as possibly plan new ones to ensure compliance with the GDPR. Some companies understand the need for changes, but research indicates that the information about the GDPR and its provisions is not necessarily diffused to them in a timely manner. According to London Economics (2013), Mikkonen (2014) and a TRUSTe survey (TRUSTe, 2015), less than half of the companies were aware of the GDPR changes. Learning about and understanding legislative requirements as such are often cumbersome and time consuming, resulting in difficulties in the implementation of the legislation's provisions. As for the GDPR, a comprehensive reform with coercive measures (such as substantial sanctions for infringements) is expected to take place. This makes the situation even more challenging and requires from companies additional actions and responsibilities to achieve compliance. The implementation of the GDPR necessitates changes that have diverse implications for companies and the usage of their resources. For example, complying with the GDPR will strongly affect information-intensive, small- and medium-sized enterprises (SME) that drive their revenue growth from online advertising (Thüsing and Traut, 2013). These companies also cannot necessarily afford juridical help to comply with the new rules of the GDPR. As non-compliance with the GDPR poses financial, legal and reputational risks to companies, they may want to deal with the GDPR requirements through their risk management policies and risk analyses. In this way, data privacy issues can be managed by means of companies' established risk management procedures.

This paper aims to help with the GDPR implementation by providing information on its changes and their practical implications, specifically for personal data intensive companies.

Please cite this article in press as: Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.015