

## **MSc in Information Security and Cyberspace Law**

**Name: Vasco Paulo Branco dos Santos**

**Title: The General Data Protection Regulation on the Insurance activity**

**Advisor: Prof. Doutor Eduardo Vera Cruz**

**Co-advisor: Prof. Doutor Carlos Manuel Costa Lourenço Caleiro**

**Date: December 2020**

### **Extended Abstract**

Nowadays, cyberspace is an essential space for economic and social interaction. The growing number of transactions involving people, organizations and equipment, connected through digital networks on a global scale, results in the generation of an unprecedented amount of data.

From the organizations' point of view, particularly companies, this large amount of data is an extremely relevant and valuable resource as it allows companies to adapt products or services to customers' preferences, create a new offer based on potential customers' data or evaluate the potential of a new market based on information regarding the individuals that make it up, among others. Based on this information, it is possible to design strategies with greater probability of success and consequent financial return.

This companies' appetite for personal data brought to the public agenda the importance of personal data and personal data protection concepts. It was within this context that the General Data Protection Regulation (GDPR) emerged and came into force on May 25 2018, in all European Union countries.

The entry into force of the GDPR implied changes in the activity of all companies. Among these, insurance companies were particularly affected since the collection, processing and storage of personal data, particularly sensitive data, are the "raw material" of health and life insurance.

The dissertation has a twofold goal. Firstly, it intends to analyze the origins and development of the concept of protection of personal data until today. Also covered in this analysis are the concepts of privacy and sensitive data since they are closely related to the former concept. Secondly, we aim to understand the effects of the implementation of the GDPR on the Insurance activity. We will focus on two dimensions of the activity: the resources used, and the results achieved.

To accomplish the first goal outlined, we used a literature review and the second goal is achieved by an exploratory study, conducted through a case study. The company Alfa, the study case, operates in the insurance sector in Portugal and provides services in all market segments, to individuals and companies. The data were collected from semi-structured interviews and documental analysis. Ten interviews with an average length of 50 minutes were conducted and several internal company documents were analyzed, including the document describing the personal data protection policy and the document containing the guidelines in force for the management of personal data breaches.

This dissertation is structured as follows. Chapter 1 presents an overview of the technological evolution felt since the first “computer” (in 2000 BC) until the emergence of the internet. This chapter objective is, on the one hand, to demonstrate the technological evolution and, on the other hand, to make evident, in contrast to the pre-internet era, the current need for access and use of personal data regulation.

Chapter 2 presents the central concepts of this dissertation - privacy, data protection and personal data protection - and fits them in European legislation.

Chapter 3 focuses on Portuguese data protection legislation. It starts with a summary of existing legislation before the GDPR comes into force and details GDPR.

Chapter 4 is dedicated to the specific case of the implementation of the GDPR in the insurance activity. Firstly, some relevant concepts of the insurance contract are presented and, secondly, a brief theoretical framework of the business activity resources and results is made. Finally, the case study of an Insurance company is described and analyzed in order to understand the effects of GDPR on the Insurance activity. The dissertation ends with the presentation, in conclusion, of some reflections on the GDPR consequences in the insurance activity. Conclusions are now summarized.

The analysis of the origins and development of the data protection concept and framework up to nowadays was what we sought to do throughout the work. This analysis also covered the privacy and sensitive data concepts. From this analysis, it was clear that the concern with data protection and data privacy existed even before the current “merging of the physical world with the virtual world” that we live in. However, the effort made, especially from the European Union, to constantly adapt the regulations to the social and economic reality is notorious. This effort was reinforced in recent years, with the entry into force of the GDPR.

The GDPR brought a great deal of uncertainty to the Insurance sector regarding the lawfulness of the personal insurance contracts data processing. We can say that this lack of definition did not arise with the entry into force of the GDPR since it was already present with the Personal Data Protection Act of 1998. However, this lack of definition has not been clarified by the GDPR nor by additional national legislation. This is the main missing clarification found. Has the legislator forgotten this issue?

Another unanswered question is what should be done with the insurance contracts that insurance companies have in their portfolio and which were still in force on May 25, 2018 and for which the insurance companies do not have any consent given according to the GDPR criteria.

Finally, we also analyzed, based on the company Alfa case study, what are the main effects on the activity resulting from the entry into force of the GDPR. Alfa is an insurance company. It is concluded that the changes imposed by the regulation had, effectively, effects both in the resources used and in the results of the activity. In terms of resources, it was observed that the group of resources most affected was organizational resources, especially organizational processes as the GDPR caused significant and transversal changes in the company's processes. Regarding the impact on the activity results, it was observed that the changes implemented due to the GDPR had negative implications on some operational indicators, such as the response time to customers and the number of complaints received from customers.