Journal of Integrated Information Management electronic journal

Implementing GDPR in Greek Companies - The necessary steps for integration

Nikolaos Kareklas [1,2], Zoe Michalopoulou[2], Fani Giannakopoulou[2]
[1] GreenFence, Select Material Recovery, Confidential Data Destruction & Recycling Company
[2] Department of Archival, Library and Information Studies, University of West Attica
nkareklas@uniwa.gr , zoemichalopoulou@gmail.com, fanigiannak@gmail.com

Article Info

Article history:
Received 04 March 2020
Received in revised form 5 May 2020
Accepted 17 May 2010

https://doi.org/10.26265/jiim.v5i1.4424

Abstract:

Purpose - *The purpose of this paper is to examine the application of the European General Data Protection Regulation (GDPR) to Greek companies. The research investigated the positive and negative impact of the implementation of the Regulations, 18 months after the new legislation went active, regarding technological, organizational and legal issues.*

Design/methodology/approach – *For this research first step was the study of existing literature. Then, questionnaires were distributed to companies liable to the GDPR for the collection of quantitative data. Finally, a conduct research was made in a company that offers records management services trying to bring the services in compliance with GDPR.*

Findings – *The above procedures have yielded significant findings regarding the actual implementation of GDPR in the companies and the technological and organizational issues that took place and need to be resolved.*

The most important outcomes from this research is a) that the companies are in need for more guidance from the competent authorities in the field of data protection, b) there is a significant cost required to implement the changes in organizational structures and c) the important role of the Data Protection Officer *(DPO).*

Index Terms — General Data Protection Regulation - GDRP, Records Management, Data Protection Officer - DPO, Protection of Personal data

I. Introduction

With the passage of the new General Data Protection Regulation in 2016, the way European citizens' personal data is processed by both European countries and non-European countries has changed. The need for more stringent legislation with homogeneity in all European countries has led to the revision of Directive 95/46 / EC Regulation **[1]** on a strict legislative framework and heavy fines **[2]**. After the application of the 2018 Regulation, all countries had to comply with all necessary changes regarding the personal data processing.

However, Greece internalized the regulation with a significant delay, as the parliament passed the law 4624/2019 in August 2019 **[3]**. Despite the delay in the integration of the Regulation into Greek legislation system, actions for its implementation has been started since 2018 **[2]**. Specifically, the Hellenic Authority for the Protection of Personal Data carried out inspections and imposed fines exactly as stipulated by the new regulation.

Normally, the application of the Regulation to the public and private sector that process personal data in any form should have been completed before 25 May 2018, something which nevertheless did not occur **[2].**

The purpose of this study was to examine whether or not Greek private-sector enterprises accomplished the implementation of the Regulation and to what extent the technological, organizational and financial requirements (which arise from the implementation) did or did not impact their businesses processes and specifically their records management policies. Another, important part of the research, was to identify the role of the Personal Data Protection Officer and his/her contribution to the application process.

The first part of the paper illustrates the innovations of the Regulation. The second part presents the research results from several Greek companies, while the third part presents the results of the communication through questionnaires with the companies and their DPOs, alongside an interview with an active DPO of a well-established Records Management Company.

II. Terminology

In order to better understand the topic of the present research, it is important to define the basic terms according to Article 4 of the GDPR Regulation:

- **'Personal Data'** means any information relating to an identified or identifiable natural person ('data subject'); the identifiable natural person is that whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier, such as name, identity number, location data, an identifiable identifier or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person' **[2]** .
- "***processing***" is defined as "any act or series of operations carried out with or without the use of automated means on personal data or sets of personal data, such as collection, registration, organization, structure, storage, adaptation or

alteration, recovery, search for information, use, disclosure by transmission, dissemination or any other form of disposal, correlation or combination, restriction, erasure or destruction **[2]** .

"***Data Controller***" means a natural or legal person, public authority, service or other body which, alone or together with others, determines the purposes and methods of processing personal data; where the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State" **[2]** .

- "***Processors"*** shall be defined as a natural or legal person, public authority, agency or other body processing personal data on behalf of the controller" **[2]**.

III. General data protection regulation

A. Key Points

The revision of Directive 95/46/EC **[1]** and the implementation of the Regulation **[2]** was based on the strictest legislative and implementing framework .

The purpose was to create a new culture for personal data processing, through the revision of the basic principles, rights, obligations and fines.

Mainly, the new Regulation revised:

- Principles relating to processing personal data
- Obligations concerning the Data Protection Officer, the Data Controller and the Data Processor
- Rights of the data subject
- Criminal penalties and administrative fines

The European Parliament proceeded to the adoption of Directive 2016/680 **[4]** which analyzes all the articles of Regulation. The extensive and detailed description of the procedures of the Regulation aims to fill possible legal gaps and to avoid a similar application of Directive 95/46/EC **[1]**, where in many cases it was interpreted by the countries at will.

The main provisions of the Regulation focus on the processing of personal data in any form and how they should be carried out to ensure the safety and protection of the data subject. The processing operations concern the basic technological and organizational changes that should be made and maintained by those entities and companies that process and store data for their own purposes.

B. Key Roles

The data processing is carried out through a set of procedures for which the data controller has the responsibility. Processor has a secondary role and is always directed by the controller. In addition to the controller and processor roles, all companies with significant volumes of personal data and complex processing operations are required, by the new regulation, to appoint the data protection officer (DPO) **[2]**.

According to the GDPR, the main responsible for the right processing of personal data is the controller and secondly the processor. The DPO, in case of a data breach is not penalized if all the necessary actions described by the Regulation were applied. On the contrary, according to Greek Law 4624/2019, the data protection officer is accountable to the law if any of the actions constitute unethical behavior and pose a risk to the security and protection of the data of the subjects **[3].**

All obligations and procedures concerning controllers, processors and data protection officers, are analyzed in the fourth chapter of the Regulation and in the articles 24-39 **[2].**

C. Criminal penalties and administrative fines

The key for implementing the changes of the Regulation is through strict fines. According to article 83 of the Regulation, in cases of violation of the provisions, the enterprises are subject to administrative fines and legal penalties **[2]**.

For administrative fines two levels are described:

The first level predicts fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, for obligations:

1. of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
2. of the certification body pursuant to Articles 42 and 43
3. of the monitoring body pursuant to Article 41

The other level of administrative fines is up to 20.000.000 EUR, or in the case of a confirmed data breach, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher for obligations **[2]**:

1. of the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
2. of the data subjects' rights pursuant to Articles 12 to 22;
3. of the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49;
4. of any obligations pursuant to Member State law adopted under Chapter
5. of non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58 or failure to provide access in violation of Article.

It is important to be clarified as characteristically referred to in Article 83 paragraph 9 "…*In any event, the fines imposed shall be effective, proportionate and dissuasive…"* that the purpose of those strict fines is to act as a deterrent to violations of the regulation and as a base to change data processing attitudes **[2].**

D. Policy and privacy

The main concern of the Regulation is the protection of personal data, as it was the fundamental request for the revision of Directive 95/46/EC in Regulation **[1].**

The articles 25 (*Data protection by design and by default*), 32 (*Security of processing*), 33 (*Notification of a personal*

data breach to the supervisory authority), 34 (*Communication of a personal data breach to the data subject*) and 35 (*Data protection impact assessment*) **[5]** aim to strengthen data protection and encourage companies to proceed in revisions at all stages of personal data processing which means structural changes including their records management policies. Moreover, articles 40 and 41 of the Code of Ethics, attempts to create a unified perspective, a single culture on which the articles will find a test basis to be applied consistently and disciplined **[2].**

E. EU institutions and bodies

For the protection of personal data, institutions and authorities are obliged to define key persons responsible to inform and be informed about all developments in the field of data protection. They must also observe global developments in the technological and socio-political sectors in order to prevent the risks that may arise from them and may put in risk the personal data in their institute or organization.

With GDPR, the data protection agencies were also revised. With the article 68 of GDPR **[2]** the European Data Protection Board **[6]** was established, replacing the Group of Article 29 from the Directive 95/46/EC **[7]**. In addition, the duties of European Data Protection Supervisor **[8]** and the responsibilities of the national data protection authorities were revised accordingly **[2].**

In Greece, Hellenic Data Protection Authority represents the country in the European Councils of Data Protection, and it has the responsibility to control and inform legal entities from the private and public sector, as well as governmental agencies and the citizens about the new regulation **[9].**

F. Technological and organizational observations

The basic application of the Regulation is based on the legislative, technological and organizational upgrading of private and public sector. The proposed technologies of Article 25 **[2]** - such as anonymization, pseudonymization, minimization of processing data and implementation of certified security procedures - are difficult to implement, as they require significant investments and high maintenance costs, which companies cannot afford.

The technologies proposed by the Regulation were one of the main questions of the present research regarding their implementation by Greek companies **[10] [11].**

G. Innovative points of the regulation

The ground-breaking aspects of the Regulation are - as mentioned above - the necessary technological and organizational revisions as well as the strict fines. The innovations of the Regulation stand in important areas such as the essential and legislative presence of a data protection officer, the need of a records management policy, the imposition of fines which leads to a new era for the personal data processing.

As it will be presented at the upcoming section, not all type of businesses could manage these changes. The high cost, the lack of expertise and the need for guidance on the implementation of the Regulation are difficult tasks which, as it turns out, are not easy to carry out successfully.

The next chapter presents the findings from the GDPR application and impact on Greek Companies **[10] [11]**

IV. GDPR AND GREEK COMPANIES

A. Research methodology

As mentioned before, the research aimed to highlight the current situation for the implementation of the GDPR in Greek companies. Clearly, this research could not apply to all Greek companies in all levels and industries. Such a task would require a longer and certainly more immediate and interpersonal communication.

The methodology applied, was the case study of the application of the Regulation to a company through interviewing the Data Protection Officer and the distribution of electronic anonymous questionnaires to companies obliged to implement the Regulation.

The dual orientation of the research aimed firstly at the immediate collection of indicative statistics via the questionnaires, and secondly at a deeper understanding of the application process through the interview with the DPO.

B. Interview with a DPO

For the case study on the "implementation of the GDPR and the role of the Data Protection Officer", a leading company in the field of Records Management Services was selected. The criteria of this choice were that the company:

A. followed GDPR prior to the implementation of the Regulation and its establishment

B. already have high technological and organizational level

C. was already certified by official bodies for its services regarding data protection

D. operates in the field of Records Management Services which is about compliance.

For the interview process, the data protection officer was first contacted, and its cooperation and terms were agreed. The information sought to be collected, concerned both the company's procedures for implementing the Regulation and the role of the company's DPO.

Regarding the company's identity, it is a Records Management Services provider whose services concern the organization, storage and safe destruction of data that belong to third party companies - customers. The nature of the work concerns the management of personal data both at the level of the processor and at the level of the controller

The second phase was to study and examine the role of the DPO, the controller and the processor though the eyes of a professional DPO. Based on what the Regulation states about the technological organization the steps of the interview were as follows:

Part 1: Meeting with the Data Protection Officer, discussing her studies and professional experience in the field of data protection, responsibilities within the company in the compliance department and the relevant certifications which are helpful on the role of DPO.

Part 2: Presentation of the business, the nature of its

operations, services and size.

Part 3: The implementation of the Regulation in the company.

For the interview was used sound recording machine.

C. Questionnaires

For the definition of the sample of companies that would participate in the research, the following eligibility criteria were established:

- They had the obligation to implement the Regulation
- Their workflows had to include both processing and storage of personal data
- The companies should be subjected to Greek law.

After the establishment of the criteria, the next step was an online search for private companies that fulfill them. The search aimed to the collection of contact information – so that the questionnaire would be distributed online via e-mail - but also concerned the nature of the operations of the companies, in order to determine whether they were subject to the relevant legislation.

The information of the sample companies was collected and recorded in an excel file including also the type and the size of the company. The target population was about 100 companies and 100 DPOs, respectively. For this purpose, two questionnaires were created. The first was addressing the technological and organizational procedures of the implementation of the Regulation and the second the role of the Data Protection Officer.

Structurally both questionnaires were consisted of closed ended questions. In the DPO's questionnaire the number of questions were 25 and in the business's questionnaire they were 27. Both were required to be completed by the Data Protection Officer or the Head of the Compliance Department. The questionnaires were formulated after a detailed study of the existing bibliography, with the systematic monitoring of the developments in the field of data protection and the data that were exported daily and finally based on the Regulation.

The questionnaires concerning the application of the Regulation on business, were divided into the following four sections:

Part A: General business identity questions (type of business, where it operates, establishment year, number of personnel employed, type of services etc.).

Part B: Specific questions for the implementation of the Regulation regarding technological, organizational and economic challenges that the new regulation brought.

Part C: Specific questions on how the companies were informed and adapted the company of the GDPR.

Part D: Questions related to the impact of the GDPR in the records management policies of the companies, if any.

The questionnaire about Data Protection Officers was also divided into 4 topics which concerned:

Part A: Demographic questions.

Part B: Educational Training of the Data Protection Officer.

Part C: The role of the Data Protection Officer inside the company.

Part D: Records Management Policies after applying GDPR.

The collection period of the samples was initially set from 1st until 15th of October 2019 but since the number of the responses was low, the survey continued until the 10th of November 2019. The answers received within 40 days reached 13 in the DPO questionnaire and 18 in the business questionnaire.

V. RESEARCH RESULTS

This chapter provides a detailed overview of the results of the research conducted through the interview process and the analysis of the questionnaires. In paragraph A the data collected through the DPO interview are presented while in paragraphs B and C the results from the questionnaires. In the final section (VI) the analysis of the results is discussed.

A. Outcomes from DPO's Interview

Regarding the DPO position, the results of the interview showed that while it is an advantage it is not necessary for the DPO to be associated with IT or Legal Studies. What is required for this position is that the DPO should be characterized by observation, flexibility, communication and information insight. Furthermore, must be able to orchestrate the compliance procedures within the company, for the correct application of both GDPR and other security and compliance regulations.

The DPO also highlighted the need of GDPR Groups for the broad interdisciplinary approach of the applications of the Regulation.

Regarding the application of the Regulation in this specific company, DPO refers that the implementation of GDPR had to follow specific and carefully steps such as:

1. Data Mapping
2. Gap Flow Analysis
3. Data Processing Impact Assessment
4. Selection of technologies to fill gaps
5. Training of the staff on new technologies and procedures
6. Cultivating a culture of data protection and Records Management.

In addition to those steps, a key factor in implementing the Regulation is the pre-existing technological and organizational level as well as the company's policy. As it was mentioned by the DPO, the high costs of the proposed technologies are deterrent to a company that does not already have a good technological background as well as specific policies and procedures. The cost of implementing new technologies and reorganizing all compliance procedures and policies for small and medium-sized companies has been a major problem and the main reason for the delay in implementing the Regulation.

In the field of document management, there was an increase of documents, mainly legal and contractual

agreements between the company and customers. New documents were also created and provided for the gap analysis both within the company and in the companies that were potential customers. The most important new document was the Data Protection Impact Assessment (DPIA) both on the controller and on the processor side.

According to the DPO, the main negative of GDPR is the high cost for the companies which were not technologically ready to adopt the Regulation. It is almost impossible to reach 100% percent compliance as there is not only the technological barrier but also the human factor that affects the implementation of the Regulation. The positive aspects of the Regulation are the redefinition of the business policies, the understanding of the use and the value of records management in a company and the new jobs that were created.

B. Outcomes from the DPO's questionnaires

The main purpose of the questionnaire that was referred to DPOs, it was to identify their role, their perspective on the implementation of the Regulation.

Structurally, the questionnaire was divided into 4 sections with 25 questions. The most important outcomes revealed that:

- DPOs are mostly male, over 45 years old, with master's degrees and with experience in the field 1 to 5 years.
- Most of them have obtained certificates related to personal data processing within 2018.
- The certifications and the pre-existing subject experience did not fully serve the needs of the position and additional external assistance was sought.
- The areas in which DPOs are mainly involved are the antitrust assessment, data flow mapping and policy review processes.
- The level of communication between the controller, the processor and the DPO is at satisfactory levels for most of the responders.
- Regarding the citizen's requests to the DPOs, data portability is in great demand alongside with the restriction of their data processing. The prevailing view is that GDPR was a necessary addition and will provide positives long-term results.
- There is an increase of business documents and a difficulty on managing them without proper records management policy and relative document management software.
- As GDPR clearly refers data destruction when the life period of a record is ended, there is a gap in Greek legislation regarding the best way to safely dispose records with personal data.

C. Outcomes from the Companies questionnaires

The companies' questionnaire aimed at gathering information on how the Regulation is being implemented in technological, organizational, legal, economic and finally at policy level.

The most important outcomes were:

- The actions for the implementation of the Regulation were carried out in collaboration with external consultants.
- 17 out of 18 companies consider themselves to be GDPR Compliant.
- 11 out of 18 refers that the cost in order to be GDPR compliant exceeded the 15,000€, while for 7 of them was less.
- Their communication with the Hellenic Data Protection Authority in general is less than 3 times a year and only in case of contact of the Authority with the company and not the other way around.
- The most difficult process were the steps of Minimizing Data Processing and the Data Flow Mapping.
- The preparation of the companies in order to be in compliance with the new Regulation started mainly 12 months before the Regulation come to force on 25 May 2018.
- External legal advisors were used for the creation of the legal documents.
- The impact of the Regulation on businesses was mostly positive despite the difficulties of the implementation.
- There was an increase on records causing companies to identify the use and the value of records management services.
- Regarding document disposal, a large percentage of the companies used confidential destruction without following the relative articles of the Regulation.

VI. CONCLUSION

According to what has been reported, recorded and researched so far, the implementation of the Regulation is an area of great study with multiple perspectives.

The most important result, apart from the need for technological, organizational and legal changes from companies in order to be in compliance with GDPR, is the necessity for people who work with personal data to become more familiar with the new Regulation. This will eventually result to changes in the way people process the personal data of subjects embracing the new regulation.

The application of the Regulation has benefits and disadvantages. On the positive side, data privacy is protected with high fines for anyone who doesn't comply with the new Regulation. On the other hand, there is a significant cost to those who want to integrate and to be compliant with the new Regulation.

It is important for companies and the public sector to understand that training upon data protection and following the developments of the new Regulation should be a continuous process. Technological modernization will help to meet the security needs while Records Management culture will help them to comply efficiently with the new Regulation.

VII. REFERENCES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons against processing of personal data and for the free circulation of this data and the abolition of Directive 95/46 / EC (General Data Protection Regulation). (2016). Official Journal of the European Union. Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons against processing of personal data and for the free circulation of this data and the abolition of Directive 95/46 / EC (General Data Protection Regulation). (2016). Official Journal of the European Union. Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

[3] Law no. 4624 : Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and other provisions. (2019). Government Gazette of the Hellenic republic. Retrieved from https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF

[4] Directive (EU) 2016/680 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. (2016). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680

[5] PIAF: A Privacy Impact Assessment Framework for Data Protection and Privacy Rights. › Research Explorer. (2020). In Cris.vub.be. Retrieved from https://cris.vub.be/en/projects/piaf-a-privacy-impact-assessment-framework-for-data-protection-and-privacy-rights(6f397a97-834e-4ff7-b44e-52df1cf020d2).html)

[6] European data protection board. (2018, April 20). Role of the NSRF - European Data Protection Board. Retrieved July 7, 2019, from European Data Protection Board website: https://edpb.europa.eu/role-edpb_el

[7] Guidelines of Article 29 of the Working Group on Data Protection Officers WP 243 rev.01 Group for the Protection of Persons against the Processing of Personal Data. (2018, January 24). Retrieved from Lawspot website: https://www.lawspot.gr/nomikes-plirofories/loipa-nomika/kateythyntiries-grammes/kateythyntiries-grammes-omadas-ergasias-0

[8] European Data Protection Supervisor (EDPS) | European Union. (2016). European Union. Retrieved from https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el

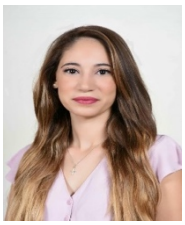
[9] Authority for the protection of personal data. (n.d.-c). Data Protection Officer (DPO). Retrieved from https://www.dpa.gr/portal/page?_pageid=33,211475&_dad=portal&_schema=PORTAL

[10] SAS. (2018). GDPR compliance in a data-driven world Insights from a 2018 survey. Retrieved from Statistical Analysis System (SAS) website: https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/gdpr-compliance-109048.pdf

[11] SEV. (2018). The General Data Protection Regulation (GDPR): opportunities and challenges for businesses in the digital age. Economy and Business. Retrieved from https://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf

VIII. AUTHORS

Nikos Kareklas holds an MSc in Information Science from the CITY University of London, England (School of Mathematics, Computer Science and Engineering) and is a graduate of the Department of Library Sciences and information systems of the Technological Educational Institute of Athens. From 2016 until today he is a laboratory collaborator of the Department of Archives, Library and Information Systems of the University of West Attica and since 2019, a Ph.D. candidate in the Department, investigating the use and the value of new technologies in Records Management which is his field of expertise. He has a rich professional career operating as Information Manager in many innovative projects in Greece such as the modernization and upgrading of the Elefsis Refinery, which is considered until today the largest private industrial investment in Greece. For many years he was the Director of the Records Management department of WWW, one of the few companies in Greece engaged in the professional management of archive material. Since 2019, he is the General Manager of GreenFence Company that operates in the field of confidential destruction of data and recycling. His current research interests relate to the integration of new technologies such as Blockchain and Artificial Intelligence into Records Management as well as the implementation of GDPR in Greek Companies and the creation of a new model for processing active documents.



Zoe Michalopoulou is a private employee in a multinational company. She holds Diploma of Vocational Education and Training at the field of Business Administration and since 2020, a bachelor's degree in information science from the department of Archival, Library and Information Studies of University of West Attica. Her research interests include the GDPR in relation with information science and business administration and new technologies such as Blockchain in relation with records management and digital libraries.

Fani Giannakopoulou is a postgraduate student at the master program, Information Management in LAM's. She holds two BA degrees one in Library and Information Systems, (University of West Attica) and one in Philosophy, Pedagogy and Psychology (University of Athens). Her work experience includes the library of the European University Institute (Florence) and the National Library of Greece.