The implementation of the General Data Protection Regulation (GDPR) in the EU and Greece: Procedures, risks, challenges and impacts in the context of Good Governance

Athanasios Papadopoulos

DEPARTMENT OF INTERNATIONAL AND EUROPEAN STUDIES

A thesis submitted for the Degree of

Master of Arts (MA) in International Public Administration

September 2020

Thessaloniki – GREECE

Student name: Athanasios Papadopoulos

Register Number: 19011

Supervisor: Dr. Maria Rammata

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the rules of the academic Ethics and the Laws that govern research and intellectual property, as well as the Regulations set in the Student's Handbook

September 2020

Thessaloniki – GREECE

ACKNOWLEDGMENTS

I want to thank Dr. Maria Rammata, whose quality and devotion to her scientific work inspired me to focus on the widely misunderstood Public Administration and comprehend its functions. Despite my professional and family commitments, her invaluable advice and methodical approach, urged me to attend my first MA program in my mid 40s actively and steadfastly. I really enjoyed it.

DEDICATIONS

I dedicate the dissertation to my beloved parents, who taught me the value of emotional and moral intelligence, to my wife and soul mate, Aleksandra, my precious daughter, Sofia, my fellow students and my dear work colleagues who supported me during the course. Finally, I dedicate it to all those who offer solidarity and assistance sincerely, selflessly and spontaneously and especially to the medical and paramedical staff who fight an unprecedented battle against COVID-19.

ABSTRACT

This dissertation was written as part of the MA program in International Public Administration at the University of Macedonia. It examines the new framework of the General Data Protection Regulation (GDPR), in the era of modern public administration. The obligations of public sector organizations, when processing personal data, are mapped step by step and the practical implications are thoroughly analyzed. Processing is every operation performed on personal data. "Personal data" is every information related to a natural person. We live in the "age of information" and "Big Data", thus the European legislation on the protection of personal data affects every public or private activity, including the exercise of public administration. It is no exaggeration to characterize personal data as the "new oil" or "new gold"[1]. The way modern economies and states need oil[2], they also need "Big Data". Privacy and big data are in many cases contradictory. Big data require massive amount of information to be collected with not a predefined and clear purpose at the time of collection. Users do not have any control on their personal information stored and analyzed by the involved data controllers and the parties that participate in data dissemination may be numerous[3]. Such enormity of the scope makes it impossible for the legislator to foresee every possible issue. Therefore, the GDPR and the relevant national legislations may contain numerous and detailed provisions, but the core of it are **firstly** the abstract principles, which have evolved the past 50 years and they reflect the rationale of the legislation and **secondly** the national authorities which enforce its implementation. In order to comprehend the principles of the GDPR, one has to perform a historical and cultural overview of their "source". Hence, this paper will try to present a brief history of personal data protection under the GDPR in the public sector, how it is conceived mainly within the Greek public administration and EU, the weaknesses and corrective adjustments that have to be performed, for the improvement of Good Governance, drawing conclusions from a relevant questionnaire on GDPR, that has been carried out among employees in the Greek Public Administration, and, finally, its impact.

[1] Adams, B. & Judd, K. (2015), *"Global Policy Watch Briefing #19"*, Global Policy Forum. Available at:https://www.globalpolicy.org/home/271-general/53036-data-is-the-new-gold.html(last accessed on 19th July 2020).
[2]Bygrave, L. (2014), *"Data Privacy Law, An international perspective"*, Oxford University Press, p. 4.
[3]Horvitz, E. &Mulligan, D. (2015), *"Data, privacy, and the greater good"*, Science, Vol. 349, pp. 253–255.

Keywords: GDPR, Principles, Good Governance, Public Administration, personal data, DPO, DPIA, survey, OECD, European Union, Greece

LIST OF ABBREVIATIONS

ASA	Administrative Simplification Agency
BDSG	The German Bundesdatenschutzgesetz – Federal Data Protection Act
CCTV	Closed Circuit Television
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés - National Data Processing and Liberties Commission
CNPD	Comissão Nacional de Protecção de Dados (Portuguese DPA)
CoE	Council of Europe
COVID-19	Corona virus disease 2019
DANTE	Detecting and Analyzing Terrorist-related online contents and financing activities
DP	Data Protection
DPA	Data Protection Authority
DPC	Data Protection Commission
DPD	Data Protection Directive 95/46/EC
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Community
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EIU	Economist Intelligence Unit
ENISA	European Union Agency for Cybersecurity
EU	European Union
FORTH	Foundation for Research and Technology- Hellas
GDPR	General Data Protection Regulation
GSIS	General Secretariat for Information Systems (Greek)
GSRT	General Secretariat for Research and Technology (Greek)
HIU	Hellenic Informatics Union
IAPP	International Association of Privacy Professionals
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
IDPC	Information and Data Protection Commissioner (Maltese DPA)
ISO	International Organization for Standardization

IT	Information Technology
LEA	Law Enforcement Agencies
M.O.U	Memorandum of Understanding
NIS	Network and Information systems
NDA	Non- disclosure Agreement
OECD	Organization for Economic Cooperation and Development
PD	Personal Data
PDCA	Plan- Do- Check- Act
QoG	Quality of Government
RBAC	Role- based access control
SIGMA	Support for Improvement in Government and Management
SOPs	Standard Operating Procedures
TEI	Technological Educational Institute
TFEU	Treaty of the Functioning of the European Union
TQM	Total Quality Management
UDHR	Universal Declaration of Human Rights
UODO	Urząd Ochrony Danych Osobowych- Polish DPA
UNDP	United Nations Development Programme
WP29	Working Party 29
ZEVIS	ZentraleVerkehrs- Informationssystem Central Traffic Information System of the Federal Motor Transport Authority (Germany)

TABLE OF CONTENTS

ACKNOWLEDGMENTS iii

DEDICATIONS iii

ABSTRACT iv

LIST OF ABBREVIATIONS vi

1. INTRODUCTION 1

1.1. GENERAL DATA PROTECTION REGULATION (GDPR) AS A NECESSITY IN CONTEMPORARY EUROPEAN UNION 1

1.2. RESEARCH QUESTIONS AND METHODOLOGY 2

2. THE EVOLUTION OF DATA PROTECTION: FROM THE DEVELOPMENT OF CONCEPTS AND PRINCIPLES TO THE CURRENT GDPR COMPLIANCE ISSUES 4

2.1. ELABORATION OF "PERSONAL DATA" AND "PRIVACY" PROTECTION: HISTORICAL AND LEGAL BACKGROUND 4

2.2. THE INNOVATIVE NATURE OF GDPR: GENERAL DATA PROTECTION REGULATION VS DATA PROTECTION DIRECTIVE 7

2.3. GUIDELINES AND PRINCIPLES OF GOOD ADMINISTRATION THAT GOVERN THE DATA PROTECTION LAW 10

2.4. THE TRANSPOSITION OF THE GDPR INTO THE NATIONAL LAW. FROM THEORETICAL READINESS TO PRACTICAL NONCOMPLIANCE 14

2.5. THE ROLE OF THE DATA PROTECTION WORKING PARTY ARTICLE 29 AND EUROPEAN DATA PROTECTION BOARD IN THE GLOBALIZATION OF THE GDPR AND THE PROMOTION OF GOOD GOVERNANCE 17

3. THE SCOPE OF THE GDPR – LEGISLATIVE APPROACH TO THE PERSONAL DATA PROTECTION IN THE PUBLIC SECTOR 19

3.1. TERRITORIAL AND MATERIAL SCOPE OF THE GDPR- REGULATORY FIELD AND EXCEPTIONS 19

3.2. THE IMPORTANCE OF DIRECTIVE (EU) 680/2016 IN THE PUBLIC SPHERE 20

3.3. THE PERSONAL DATA PROTECTION UNDER THE STIPULATIONS OF LAW 4624/2019 22

3.4. THE SCOPE OF APPLICATION OF THE GDPR AND THE CHALLENGES FOR THE PUBLIC SECTOR. THE WAY IT COULD AFFECT THE ORGANIZATIONAL STRUCTURE AND FUNCTIONING OF THE PUBLIC BODIES AND THE QUALITY OF PUBLIC SERVICES 23

4. CONSEQUENCES OF THE GDPR ON THE ORGANIZATIONAL STRUCTURE AND CULTURE OF THE PUBLIC BODIES 26

4.1. PREPARATORY STEPS FOR A PUBLIC ENTITY 26

STEP 1 Preparation of a plan 26

STEP 2 Information, increasing preparedness 27

STEP 3 Designation of a Data Protection Officer (DPO) 27

STEP 4 Listing- Record keeping 28
STEP 5 Scrutiny on the public entity's compliance 28
STEP 6 Reviewing the data protection policies and the information provided to the public ... 29
STEP 7 Revision of internal procedures for the fulfillment of data subject rights under GDPR 30
STEP 8 Data Protection Impact Assessment (DPIA) in a structured and methodical way 30
STEP 9 Preparedness for violations of data protection rights 31
STEP 10 Ensuring continuous compliance with the GDPR 32
4.2. DEPARTMENTS AND PERSONS CONCERNED WITHIN THE PUBLIC ENTITIES- THEIR ROLE IN THE COMPLIANCE PROCESS 33
4.3. A CHECKLIST/ ACTION PLAN WITH DO'S AND DON'TS FOR THE PROPER IMPLEMENTATION OF THE PRINCIPLES OF THE GDPR BY THE EMPLOYEES OF THE PUBLIC SECTOR 34
5. SURVEY – RESEARCH ON THE GDPR IN THE GREEK PUBLIC SECTOR 35
5.1. GENERAL INFORMATION AND PURPOSE OF THE SURVEY 35
5.2. DEMOGRAPHICAL CHARACTERISTICS OF THE PARTICIPANTS 35
5.3. LINKAGE OF THE QUESTIONS WITH THE 10 INDICATIVE STEPS THAT HAVE TO BE FOLLOWED 36
5.3.1. STEPS 1, 2 CONNECTED WITH QUESTIONS 1, 2, 3, 4: PREPARATION OF A PLAN, TIME CONSTRAINTS AND DEADLINES, PRIORITIES AND CRITERIA FOR ACTION 36
5.3.2. STEP 2 CONNECTED WITH QUESTIONS 5, 6, 7: INFORMATION, PREPAREDNESS, INCREASE OF WORKLOAD 39
5.3.3. STEP 3 CONNECTED WITH QUESTIONS 8, 9, 10, 11, 12: MANDATORY DESIGNATION OF A DPO IN EACH PUBLIC ENTITY 41
5.3.4. STEP 4 CONNECTED WITH QUESTIONS 13, 14, 15, 16: DEALING WITH THE RECORD KEEPING AND LISTING 44
5.3.5. STEP 5 CONNECTED WITH QUESTIONS 17, 18, 19, 20, 21: DEALING WITH THE SCRUTINY OF THE PUBLIC ENTITY'S COMPLIANCE AND THE IMPLEMENTATION OF SECURITY MEASURES 46
5.3.6. STEP 6 CONNECTED WITH QUESTIONS 7, 22, 23, 24: REVIEWING THE DATA PROTECTION POLICIES AND THE INFORMATION PROVIDED TO THE PUBLIC PLUS PUBLIC AWARENESS ON THE GDPR 49
5.3.7. STEP 7 CONNECTED WITH QUESTIONS 13, 25, 26, 27: REVISION OF INTERNAL PROCEDURES FOR THE FULFILMENT OF DATA SUBJECT RIGHTS UNDER GDPR 51
5.3.8. STEP 8 AND STEP 9 CONNECTED WITH QUESTIONS 8, 27, 28, 29: PERFORMING DATA PROTECTION IMPACT ASSESSMENT (DPIA) IN A STRUCTURED AND METHODICAL WAY – PREPAREDNESS FOR VIOLATIONS OF DATA PROTECTION RIGHTS 53

5.3.9. STEP 10 CONNECTED WITH QUESTIONS 30, 31, 32, 33: ENSURING CONTINUOUS COMPLIANCE IN THE CONTEXT OF GOOD GOVERNANCE 56
5.3.10. CONCLUSIONS: STRATEGIC AND TECHNICAL BARRIERS 60
6. THE SIGNIFICANCE OF SANCTIONS– PROPOSALS FOR THE BETTER IMPLEMENTATION OF GDPR 63
6.1. SANCTIONS ISSUED UNDER THE GDPR IN PUBLIC SECTOR 63
6.2. TOOLS AND PROPOSITIONS FOR THE BETTER IMPLEMENTATION OF GDPR 65
CONCLUSION 73
BIBLIOGRAPHY 76
BOOKS 76
JOURNALS 77
WEBSITES AND PORTALS 79
PICTURES & TABLES 81
ANNEX I 82
CHECKLIST / GUIDE TO GDPR FOR ORGANIZATIONS ACCORDING TO INFORMATION COMMISSIONER'S OFFICE (UK) 82
ANNEX II 86
QUESTIONNAIRE 86

1. INTRODUCTION

1.1. GENERAL DATA PROTECTION REGULATION (GDPR) AS A NECESSITY IN CONTEMPORARY EUROPEAN UNION

The European Union is one of the most influential "sui generis" international organizations which operates under a system of Conventions and Treaties that are compulsory for its member states in specific fields. In general, this system overrules national legislative frameworks in cases of conflict. For this reason, national legislative systems have been harmonized and in certain matters unified. As a response to the rapid development of emerging technologies, in recent years EU legislators have reformed EU data protection regulations in order to empower European citizens to exercise their rights regarding the processing of their personal data. The highlight of these reforms was the adoption of the General Data Protection Regulation (GDPR)[4]. Its text was finalized on 8 April 2016 and approved by the European Parliament on 14 April 2016. Subsequently, it was adopted on 27 April 2016, entered into force on 24 May 2016, applying from 25 May 2018. Apart from empowering European citizens concerning their data protection rights, the GDPR provides a singular system of personal data protection for all 28 Member States.

The last decade has witnessed an overwhelming shift in European Union Data Protection (DP) Regulation. The pace of development of emerging technologies and the consequences of their implementation in conjunction with the rapidly developing social networking and the computerized interconnection of public services have influenced social, legal, economic and political areas. Governments, police and other public authorities themselves collect and treat data put on the net by the users for legitimate security reasons. The will to prevent terroristic threats immeasurably multiplied the collection and classification of information and data regarding citizens' lives and behaviors. The handling of personal data by public and private sector bodies has become faceless and depersonalized, hence extremely annoying and usually malicious.

Concerning the public sector, as an indicative feature, according to the 2018 Irish Data Protection Commissioner (DPC) Annual Report (May 25 – December 31st)[5], during this short period of application of the GDPR, there were 3,687 reported data breach notifications, in Ireland. Of these, 1,258 were in the public sector with unauthorized disclosure accounting for 1.064 (84.5%). The aforementioned Report cites –among others- as typical examples of data breaches, malicious or criminal cyber incidents, such as brute-force attacks (they consist of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly), hacking, malware, phishing and ransomware. On the other hand, regarding the private sector, extensive debt data have been stored, processed and used by credit institutions and collection agencies, unlawfully and cynically, without the debtor's consent, without any restrictions and for unwanted purposes. A list

[4] 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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj(last accessed on 19th July 2020).

[5]Irish DPC Annual Report (2018). Available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf(last accessed on 19thJuly 2020).

and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation, shall be presented in the following chapters.

Consequently, regulating new technologies is more relevant now than ever before. Regulators must confront the challenge of balancing between responsible innovation and the use of technologies for the general public interest. In many respects, the cross-border movement of services (not only private but public too) and goods produces a need for the harmonization (and in many instances the unification) of national legislative frameworks and the coordination of self-restraint mechanisms by the Member States.

1.2. RESEARCH QUESTIONS AND METHODOLOGY

The present study basically aims to demonstrate the ongoing relation between the implementation of the GDPR in the Public Administration and the wider challenge of improving the services provided to the citizens, especially in the Greek and secondarily in the European context in general. The goal is to shed light on how the application of GDPR affects the mechanisms and the quality of the public administration with regard to their organizational and regulatory aspects. Thus, the study also intends to illustrate the reaction of the civil servants and the citizens- customers to the new Regulation, the possible tension or commitment, the endorsement or disapproval, the knowledge or ignorance of the GDPR. To this end, a questionnaire was addressed to Greek civil servants and its results will be presented, in order to verify the progress or the stagnation of the Greek Public Service towards the new Regulation.

The sad reality is that even in more advanced European countries, time passed uselessly. For instance, the Italian Government approved the measures to actuate the new Community duties under the GDPR, only in March 2018, two months before the direct enforceability of new dispositions. The Legislative Decree 101/2018 ("Harmonization Decree") harmonized the Italian data protection laws with the General Data Protection Regulation (EU) 679/2016 ("GDPR") provisions and was finally enacted and became effective on September 19, 2018. This fact created many problems because many administrations, particularly Municipalities were not able to confront the new requirements. There was also a lack of specific training for public employees, who were called to really actuate the Community Regulation. As Giacomo Mannocci, PhD in Constitutional Law, at the University of Genoa, stated “We are still in ‘work in progress”[6].

Inevitably, the essay focuses on the following general questions, which correspond to the respective parts of the study concerning the GDPR. Each part shall be composed of various sections and subsections:

i) The evolution of data protection, the formulation of its basic concepts and the historical precedents of GDPR.

ii) The data protection principles set out by the GDPR and their connection with the OECD basic principles of public administration and the principles of good administrative behavior.

[6]Mannocci, G. (2018). *“The Public Administration and the Citizens Privacy Protection”*, The Italian Law Journal, p. 94.

iii)The extent to which the GDPR and the relevant European and national legislation deal with and affect the organizational structure of the public entities and the quality of the public services, especially in the Greek context.

iv)The manner in which the application of the GDPR principles affect the functioning and effectiveness of the Public Administration.

v) The preparatory steps that have to be followed to carry out its implementation in the Public Sector.

vi) The most important strategic and technical barriers faced by the modern Public Administration at European and national level.

vii) The most notable sanctions/ fines issued under the GDPR in the public sector at European level.

viii) The final part of the present study provides the author's propositions, instruments and ideas to integrate the GDPR in the traditional way of working in the public sector.

Undeniably, due to the galloping developments to the matters under examination, all presented results and properties are exposed to argumentation and suitable for further research.

2. THE EVOLUTION OF DATA PROTECTION: FROM THE DEVELOPMENT OF CONCEPTS AND PRINCIPLES TO THE CURRENT GDPR COMPLIANCE ISSUES

2.1. ELABORATION OF "PERSONAL DATA" AND "PRIVACY" PROTECTION: HISTORICAL AND LEGAL BACKGROUND

As history helps us understand the past and predict the future, a brief historical overview would be more than helpful, in order to comprehend the importance of the introduction of GDPR and its protective nature to the citizens against the arbitrariness of the might. Governments have been gathering personal information on their citizens for hundreds of years. Since the days of the Roman Empire, government officials maintained taxation records, including the name, address and income of individuals, with surprising accuracy on reusable waxed tablets. The prominent contemporary right to be forgotten just needed a lit candle to be implemented. However, these records were consolidated and supplied to the Emperor and depending on how moral he was, these personal records could be abused. In 1086 William the Conqueror collected vast amounts of **personal data** in his unoptimistically titled "Domesday book". As H. C. Darby noted, "anyone who uses it, can have nothing but admiration for what is the oldest "public record" in England and probably the most remarkable statistical document in the history of Europe. The continent has no document to compare with this detailed description covering so great a stretch of territory. And the geographer, as he turns over the folios, with their details of population and of arable, woodland, meadow and other resources, cannot but be excited at the vast amount of information that passes before his eyes."[7]

The primary purpose of the survey was to ascertain and record the fiscal rights of the king. These were mainly: 1) the national land-tax (geldum), paid on a fixed assessment, 2) certain miscellaneous dues and 3) the proceeds of the crown lands. William would use individuals' personal data within the "Domesday book", in order to whimsically demand tax collection, that consequently led to arbitrary over-taxation, which contributed to social discontent.

Several centuries later, before and during the World War II, issues regarding **personal data** were prevalent and connected with Nazi Germany, where vast intrusions in the **privacy** of citizens of belligerent countries, typically under the guise of national security, took place. In certain situations, these intrusions went far beyond the needs to protect the respective nations against espionage and other acts. The most well-known example was the invasion of the **privacy** of the citizens and residents of Nazi Germany, used to identify those who were members of disfavored groups—racial, political or otherwise. The post-War period was a time in Europe when disclosure of race or ethnicity led to secret denunciations and seizures that sent friends and neighbors to work in concentration camps. As a result, Europe's extensive **privacy regulation** is justified, amongst other reasons, with reference to experiences under World War II-era fascist governments and post-War Communist regimes, where there was widespread unchecked use of personal information[8].

[7]Darby, H.C. (1977), *"Domesday England"*, Cambridge: University Press, p.12.
[8]Moshell, R. (2005), *"And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection"*, Texas Tech Law Review, pp. 357- 364.

At global level, in the aftermath of World War II, in 1948, the General Assembly of the United Nations adopted the Universal Declaration of Human Rights (from now on 'UDHR'). Article 12[9] of the Declaration introduced the prohibition against arbitrary interference with **"privacy"**. The provision distinguished "privacy" from the concepts of family, home and correspondence, implying that the former consists of elements that fall outside of the concepts of the three latter, which are more definable. It was a direct acknowledgment by the UN legislator, that private is not only home, family matters and correspondence, although they are the key elements.

During the same period, at European level, the "right to privacy" became also a well-established right by the European Convention on Human Rights (article 8)[10] (from now on 'ECHR'), which was drafted in 1950, by the then newly formed Council of Europe and became effective on September 3, 1953.

At national level, focusing on the post-war efforts of the Federal Republic of Germany to pass laws to ensure such significant intrusions into its citizens' privacy were legally prohibited, we come across the German national and state laws and cases dealing with privacy. In 1970, the federal state of Hessen (Hessisches Datenschutzgesetz) passed the first national data protection law, which was also the first data protection law in the world. In 1971, the first draft bill was submitted for a federal data protection act. Finally, on January 1, 1978, the first federal data protection act came into force. In the following years, as the BDSG (federal data protection Act) was taking shape in practice, a technical development took place in data processing as computers became increasingly important both in the public and private sector.

Special reference should be made to Sweden, which has been a pioneer and world leader in the production of national legislation concerning the personal data protection. In 1973, Swedish legislation aimed at protecting the informational privacy of individuals when their personal data were processed digitally. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerized registers. The Act did not contain many material provisions on when and how the data should be processed, or any of the general data protection principles described above. Instead, the act required for each computerized personal data register a prior permit from a newly established data protection public authority – the Data Inspection Board (Datainspektionen). By the end of the 1980s, although the 1973 Data Act had been amended several times over the years, since no stable general data protection principles existed, it was hopelessly out- dated. However, the Swedish Data Inspection Board marked a new era for the history of Data protection, since it incorporated for the very first time public concern about personal data and abuse of government power related to mass surveillance and the enactment of the world's first national data protection law: the Data Act, enacted on May 11, 1973[11].

Furthermore, French Legislation is of utmost importance in the field of Data Protection. France, together with Sweden and the German State of Hessen, was one of the first countries in Europe to adopt also a data protection law. The 1978 Law is said to have inspired the drafting of Directive

[9]Article 12 of the UDHR (p. 73). Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217 (last accessed on 19th July 2020).
[10]Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended). Available at: http://www.hri.org/docs/ECHR50.html#Convention (last accessed on 19th July 2020).
[11]Öman, S. (2018),*"Implementing Data Protection in Law"*, Stockholm Institute for Scandinavian Law 1957-2010, p. 390.

95/46/EC on personal data protection, with regard to the processing of personal data and on the free movement of such data[12] (from now on 'DPD'), which was the precursor to the GDPR and came into force on October 24, 1995, becoming effective on October 25, 1998[13].It also provided for procedures ensuring the confidentiality of personal information held by government agencies and private entities. Moreover, it created an independent data protection authority, the National Data Processing and Liberties Commission (Commission Nationale de l'Informatique et des Libertés, CNIL). The CNIL's primary mission was to ensure that the development of information technology would remain at the service of each citizen and it would not infringe upon human identity, the rights of man, or individual or public liberties.

At global level, the stand-alone fundamental right to "data protection" was declared for the first time under the Article 8 of the Charter of Fundamental Rights of the European Union, enacted by Lisbon treaty[14] , ratified on 7 October 2000. It has been pointed out that the principles underpinning the human right to "data protection" reflect some key values inherent in the European legal order, namely privacy, transparency, autonomy and non-discrimination[15] . Therefore, under an instrumental conception, it can be argued that the "right to data protection" could serve as a safeguard not only for "privacy" but also for all fundamental rights[16] . In this respect, it is inextricably linked to the notion of Good Governance, which is directly related to the present thesis.

From the above brief historical overview of the basic legislative texts and treaties, it is concluded that **"privacy" and "personal data protection", which jointly comprise the primary legislative purpose of the GDPR, are two interrelated terms,** often used interchangeably, especially in the past. However, it must be made clear that they actually constitute two different and discrete notions of intertemporal value. The idea of "privacy", especially in Western cultures, derives from concepts such as "human dignity" and "rule of law". Modern conceptions of privacy have begun to be developed following the experiences of totalitarian regimes in World War II and Communist regimes in the post-war period. Within modern European law there is a distinction between "privacy" and "data protection" which defines these two concepts as closely related, and often overlapping each other, but not as synonymous. "Privacy" generally refers to the protection of an individual's "personal space", while "data protection" refers to limitations or conditions on the processing of data relating to an identifiable individual, in both cases predominantly against state or administrative arbitrariness, even in the context of democratic governance. Nevertheless, as legal scholars note, "data protection" and "privacy" overlap on a way whereby "data protection" is both broader and narrower than privacy. It is broader because it applies to the processing of personal data, even if the latter does not infringe upon "privacy". It is narrower because it only deals with the processing of personal data, whereas the scope of "privacy" is wider.

[12]Castets-Renard, C. (2009),*"Droit de l' Internet"*, §26, Edition Montchrestien.
[13]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at:https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (last accessed on 19th July 2020).
[14]Article 8 of the Charter of Fundamental Rights of the European Union, enacted by Lisbon treaty. Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT(last accessed on 19th July 2020).
[15] McDermott, Y. (2017),*"Conceptualizing the right to data protection in an era of Big Data. Big Data & Society"*,SAGE Journals.
[16]Gellert, R. and Gutwirth, S. (2013),*"The legal construction of privacy and data protection"*, Computer Law & Security Review, 29, pp 522–530.

"Legally speaking, "privacy" and "data protection" both represent two distinct fundamental rights under the modern European Law, which defines the first one as a substantive right whereas the second as a procedural"[17]. Under this perspective it is fully justified that GDPR is expressly framed in terms of rights, with Article 1 noting that the regulation "protects fundamental rights and freedoms of natural persons and in particular **their right to the protection of personal data**"[18]. Despite the fact that there is **not any reference to 'the right to privacy'** throughout the GDPR text, the concept of privacy is implied in most of its recitals and articles.

2.2. THE INNOVATIVE NATURE OF GDPR: GENERAL DATA PROTECTION REGULATION VS DATA PROTECTION DIRECTIVE

As it can be seen by the brief introduction above, the adoption of the GDPR was the result of historic, social and legal development, over decades. Since the purpose of the present study is not to deal with specific legal issues and articles or to carry out a rigorous comparative study between different legislative texts, emphasis will be selectively placed on the **key innovations**, introduced by the GDPR, comparing it with the earlier legal mechanism, i.e. the above mentioned DPD.

First of all, being a regulation, the GDPR is entirely binding and directly applicable in all EU Member States[19]. It fully harmonizes the data protection law in all EU Member States, except in rare cases where the GDPR itself allows the Member States to regulate the subject independently. The GDPR specifically applies to the processing of personal data (PD) by controllers or processors established in the EU[20], but also to the processing of PD, of data subjects who are in the EU, by a controller or a processor not established in the EU[21].

On December 15, 2015, the European Parliament, Council, and Commission reached an agreement on the new data protection rules, the EU General Data Protection Regulation. The outcome was a much more modern and collaborative data protection framework across the EU. The importance of PD protection for the EU is evidently high, since the GDPR is a regulation and the issues of data protection, amongst others, found place in the European Commission President's State of the Union Address 2017[22] as the fourth priority and as a part of the first priority 'Strengthening EU trade agenda' that determined that the EU trade is also about exporting EU standards, including data protection requirements and just behind the fight against climate change.

The EC hoped that through the creation of a unique, EU-wide law, fragmentation and extensive administrative measures, associated with implementing and enforcing the DPD across different member states can be eliminated. This also aimed to facilitate cross-border cooperation in terms of the fight against crime and terrorism.

---

[17] De Andrade, N. (2014), *"Oblivion: the right to be different from oneself: re-proposing the right to be forgotten. The Ethics of Memory in a Digital Age"*, Palgrave Macmillan Memory Studies, pp. 65–81.
[18] McDermott, Y. (2017), op. cit.
[19] Art. 288 TFEU (OJ C 326, 26 October 2012, p. 47–390); EUR-Lex, plain clarification on EU regulations. Available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14522 (last accessed on 19th July 2020).
[20] Art. 3 GDPR and preamble points 23 and 24 GDPR.
[21] The issue of the material and territorial scope of the GDPR will be thoroughly analyzed in the following chapter.
[22] Juncker, J.C. (2017), "*State of the Union Address"* in Brussels, 13th September 2017. Available at: https://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm. (last accessed on 19th July 2020).

The GDPR was based on the key tenets of the DPD, with more specific data protection requirements, a global scope, and stiffer enforcement as well as non-compliance penalties. As a result, from the date of its entry into force citizens have more control over their personal data and more recourse if personal data is misused, while data controllers and processors are required to protect sensitive personal data by design. The GDPR offers a much simpler regulatory environment for businesses that collect or process EU citizens' and residents' personal data.

To summarize, the **main differences between the GDPR and the earlier DPD** are as follows:

a. **In the field of Personal Data redefinition**: According to the DPD, personal data was defined as names, telephone numbers, photographs, e-mail addresses and personal ID numbers. Under the GDPR, personal data is defined as any information that could be used, on its own or in combination with other data, in order to identify an individual. This data includes IP addresses, mobile device identifiers, and geolocation and biometric data (fingerprints, retina scans, etc.). The GDPR also covers data related to an individual's physical, mental, psychological, genetic, mental, cultural, social or economic identity. Hence, according to GDPR "**personal data" means any information relating to an identified or identifiable natural person ("data subject")** and the definition of the term is significantly broadened. The updated definition of the term "personal data" is important because it reflects the technological changes over the last two decades and the way organizations collect data about people for various purposes.

b. **In the field of Individual rights:** The GDPR represents progress in privacy considerations; it requires explicit opt-in for the processing of any personal data. Descriptions of data use must be brief and straight to the point. One-size-fits-all agreements should be eliminated. Both consent and explicit consent now demand clear affirmative action. Furthermore, according to the GDPR, another right that the people of the EU are able to invoke is the right to legitimately access their own data. Under the GDPR, data subjects have the right to obtain their personal information from the data controller regarding how their data is being reused (where, for what purpose and for how long). At any time, any person can recall their consent to the use of their data and, in that case, the controllers must erase all of their personal data, cease their further use and, if applicable, halt any third party use of that data.

c. **In the field of Data controllers vs Data processors**: Under the DPD, only data controllers were held accountable for any mishandling of data. Under the GDPR, data processors are due to sign a contract with data controllers concerning the process of personal data. According to the GDPR, the data processor is liable for the security of personal data. To emphasize the accountability of both data processors and data controllers, a data protection officer (from now on: DPO) will need to be designated under the GDPR. As it regards the private sector, a DPO must be appointed when the core activities of the controller or processor involve "regular and systematic monitoring of data subjects on a large scale" (article 37 par. 1 GDPR)[23]. The GDPR does not define what constitutes large scale processing, though recital 91[24]of the GDPR provides some guidance for the sake of clarity. According to the recital "large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk" would be included, in particular.

[23]Article 37 GDPR. Available at: https://gdpr-info.eu/art-37-gdpr/ (last accessed on 19th July 2020).
[24]Recital 91 GDPR. Available at: https://gdpr-info.eu/recitals/no-91/(last accessed on 19th July 2020).

Examples of large-scale processing include: patient data in the regular course of business by a hospital, travel data of individuals using a city's public transport system (e.g. tracking via travel cards), customer data in the regular course of business by an insurance company or a bank and by telephone or internet service providers(content, traffic, location) [25].

On the other hand, the recital specifically provides that "the processing of personal data should not be considered to be on a large scale if it concerns personal data from patients or clients by an individual physician, other health care professional or lawyer". It should be noted that it is mandatory for public authorities or bodies (excluding courts).

d. **In the field of Information governance and security**: GDPR requires that organizations consider compliance with the regulation from the design of systems and processes, i.e. "privacy by design." They have to consider the privacy of collected data from the very beginning. In terms of security, GDPR requires that organizations conduct impact assessments for automated data processing activities, large-scale processing of certain kinds of data, and systematic monitoring of publicly accessible areas on a large scale.

e. **In the field of Data Breach notifications and penalties**: Under the DPD, EU member states were free to adopt different data breach notification legislation. As a result, when multinational companies suffered data breaches in the EU, they had to research and ensure compliance with each member state. Upon the adoption of the GDPR, there is just a single requirement to follow: Data controllers must notify their supervisory authority and individuals affected by a personal data breach within 72 hours of learning about the breach. Moreover, under the Directive, the amount of administrative penalties was left up to the member states. Usually, those fines would be insignificant and would very rarely be applied. Under the GDPR, penalties are mandatory and uniform over all the EU states. These penalties can be imposed for any negligent or intentional violation of the GDPR. Depending on the violation, companies can pay up to 20 million euros or 4% of their global turnover[26] (whichever is higher)[27].

f. **The Global Impact of the GDPR in comparison with DPD**: The GDPR states that it applies to the processing of personal data of subjects located in the EU, even if the controller or processor is not established in the EU. In general, any company that markets goods or services to EU residents regardless of the physical location of the business can be subject to the GDPR. This provision renders the GDPR a worldwide law. The DPD was not nearly as expansive in its geographical reach, and that is partially because it did not plan for the use of digital personal data like IP addresses.

[25]Working Party 29 (2016),*"Guidelines on DPOs"* pp. 7- 8. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (last accessed on 19th July 2020).
[26]Article 83 GDPR. Available at: https://gdpr-info.eu/art-83-gdpr/(last accessed on 19th July 2020).
[27]The sixth chapter of the present paper is dedicated to the issue of sanctions and penalties.

2.3. GUIDELINES AND PRINCIPLES OF GOOD ADMINISTRATION THAT GOVERN THE DATA PROTECTION LAW

After a period of almost thirty years, the aforementioned international conventions and declarations, such as the UDHR and the ECHR, as well as the European national laws, which had been adopted between 1950- 1980, regulating "personal data" and "privacy" protection, needed updating, specific orientation and further interpretation. The new legislative tools at both national and European or even global level needed to be based on firm ground rules and guidelines, in order to achieve uniformity of practices and a common framework on "privacy" and "personal data protection" matters, at least within the European continent, in the context of Good Administration and Good Governance. It is no coincidence that both the DPD (Directive 95/46/EC) and the GDPR are based on a set of similar principles, established at the beginning of the 80s, which still hold true until today. The interrelation between the principles of Good Governance and the principles adopted by the DPD was so apparent that scholars argued "the original rules in the Data Protection Directive and related rules could best be regarded as principles of Good Governance"[28]. In 1980, the Organization for Economic Co-operation and Development (OECD) published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[29], "whether in the public or private sectors", which was a set of recommendations endorsed by both the EU and the US that set out to protect personal data and the fundamental human right of privacy. The Annex to the Recommendation of the Council of the 23rd September 1980 proposed the following eight principles for the processing of personal data, contained within its second part[30]:

Collection Limitation Principle
There should be limits to the collection of personal data, data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle
The purpose for the collection of data should be specified at the time of collection and data should not be used for anything other than its original intention without again notifying the data subject.

Use Limitation Principle
Personal data should not be used for purposes outside of the original intended and specified purpose, except with the consent of the data subject or the authority of the law.

Security Safeguards Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Individuals should have easy access to information about their personal data, who is

[28] Van Der Sloot, B. (2014), *"Do Data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation"*, International Data Privacy Law, pp. 307- 325.
[29] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013). Available at: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf(last accessed on 19th July 2020).
[30] Igglezakis, I. (2004), *"Sensitive Personal Data"* (in Greek), Sakkoulas, Athens- Thessaloniki, p. 25.

holding it, and what they are using it for.

Individual Participation Principle
An individual should have the right to know if a controller has data about him/her and to have access to that data in an intelligible form for a charge, if any, that is not excessive. An individual should also have the right to challenge a controller for refusing to grant access to his/her data, as well as challenging the accuracy of the data. Should such data be found to be inaccurate, the data should be erased or rectified.

Accountability Principle
Data controllers should be accountable for complying with the measures detailed above.

These guidelines became the basis of many national laws regarding "personal data and privacy protection", however, they were non-binding and the levels of data protection varied greatly even amongst different EU member states[31]. Therefore, they are definitely included in and totally correspond to the basic principles of Public Administration- particularly those described in Category D(Accountability) and Category E(Service Delivery)which would be identified by the SIGMA Initiative (Joint Initiative by the OECD and the EU) several years later[32].

COMPARATIVE TABLE I

OECD GUIDELINES (1980) on the Protection of Privacy and Transborder Flows of Personal Data	**SIGMA Initiative – OECD Basic Principles of Public Administration (2014)**
Collection Limitation Principle ("by lawful and fair means")	The lawful exercise of discretion
Data Quality Principle ("to the extent necessary")	Proportionality
Data quality principle	Quality of public service
Data quality principle ("accurate, complete and kept up-to- date")	Interoperability of registries and digital services
Security Safeguards Principle	The policy for citizen- oriented state administration in place and applicable
Openness principle ("easy access to information about their personal data")	The accessibility of public services
Individual participation principle ("individual should also have the right to challenge a controller for refusing to grant access to his/her data, as well as challenging the accuracy of the data")	The right of hearing
Openness principle ("general policy of openness about developments, practices and policies with respect to personal data")	Transparency and openness
Accountability Principle ("Data controllers should be accountable for complying with the measures detailed above")	Accountability

[31]Alexandropoulou- Egyptiadou, E. (2016),*"Personal Data"* (in Greek), Nomiki Bibliothiki, Athens, pp. 241- 255.
[32]The University of Macedonia, MIPA Book, Rammata, M. (2019), *"The Principles of Public Administration"*, pp. 213, 221- 223.

Data protection principles in the GDPR are revised but are broadly congener to the principles set out above, as well as in the earlier DPD (Data Protection Directive):

1) Fairness, lawfulness and transparency [Article 5 par. 1 (a)]

2) Purpose limitation [Article 5par. 1(b)]

3) Data minimization [Article 5 par. 1(c)]

4) Accuracy [Article 5 par. 1 (d)]

5) Storage limitation [Article 5 par.1(e)]

6) Accountability [Article 5 par. (2)]

7) Integrity and confidentiality [Article 5 par. 1(f)].

However, there are few changes. While the DPD constituted the international standard against which all data protection initiatives, in and out of Europe, were benchmarked[33], the GDPR brings the novelty of explicitly imposing organizations to enshrine "data protection by design and by default", (Article 25) enforcing measures, such as data minimization, as a standard approach to data collection and use. Furthermore, the GDPR enabled individuals to control their personal data in the context of automated decision-making (Article 22) and, hence, acts as crucial function for mitigating the risks of big data and automated decision making for individual rights and freedoms and resembles closely the Security Safeguards Principle of the 1980 OECD Guidelines (Article 22 par. 3 of the GDPR) as well as the right of hearing among the OECD basic principles of Public Administration (2014) (see Comparative Table I).

Certainly, the aforementioned principles were by no means unrelated to the principles of other relevant legislation on the European stage. The case of the Data Protection Act 1998 (the 1998 Act) in the UK is **paradigmatic**[34]:

COMPARATIVE TABLE II

	GDPR		**1998 Act**
Principle (a)	lawfulness, fairness and transparency	Principle 1	fair and lawful
Principle (b)	Purpose limitation	Principle 2	purposes
Principle (c)	Data minimization	Principle 3	Adequacy
Principle (d)	Accuracy	Principle 4	accuracy
Principle (e)	Storage Limitation	Principle 5	Retention
Principle (-)	No principle – separate provisions in Chapter III	Principle 6	Rights
Principle (f)	Integrity and confidentiality	Principle 7	Security
Principle (-)	Separate provisions in Chapter V	Principle 8	International transfers
Principle (g)	Accountability principle	(no equivalent)	

[33]De Hert, P. & Papakonstantinou, V. (2016), *"The new General Data Protection Regulation: Still a sound system for the protection of individuals?"*, Computer Law & Security Review, Vol. 32, pp. 179–194.

[34]Hall, J. (2010),*"The 8 principles of the Data Protection Act 1998: a summary for small businesses in the UK"*. Available at: https://www.simplybusiness.co.uk/knowledge/articles/2010/04/2010-04-23-data-protection-key-responsibilities-for-small-businesses/ (last accessed on 19th July 2020).

The principles lie at the heart of the GDPR. They are set out right at the beginning of the legislation, and concern everything that follows. They don't just give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to our compliance with the detailed provisions of the GDPR. Failure to comply with the principles does not only induce moral disdain but it may leave an organization exposed to substantial fines[35].

GDPR principles lie at the heart of Good Administration, too. It is not fortuitous that main values and general principles of Good Administration adopted by the European Commission on 13th September 2000, within the "Code of Good Administrative Behavior for Staff of the European Commission in their relations with the Public"[36] coincide with the main principles of the GDPR. Also, the "White Paper on Administrative Reform[37] that was adopted by the EU Commission on 1st March 2000 stressed the key principles of a European public administration which focuses on service, independence, responsibility, accountability, efficiency and transparency".[38] (*see Comparative Table III*).

COMPARATIVE TABLE III

	GDPR	**CODE OF GOOD ADMINISTRATIVE BEHAVIOR**	**WHITE PAPER ON ADMINISTRATIVE REFORM**
Principle (a)	Lawfulness, fairness and transparency	Lawfulness (Article 4), Fairness (Article 11) Duty to justify decisions (Article 18) – Quality Service	Transparency
Principle (b)	Purpose limitation	Purpose (Articles 6, 7, 21)	
Principle (c)	Data minimization	Proportionality (Article 7)	
Principle (d)	Accuracy	Consistency (Article 10)	Efficiency
Principle (e)	Storage Limitation	Proportionality (Article 6)	
Principle (f)	Integrity and confidentiality	Protection of PD and Confidential Information (Articles 21, 22)- Objectivity (article 9) impartiality (article 11)	Independence
Principle (g)	Accountability principle	Responsibility(article 22)	Responsibility-Accountability

[35]Klosek, J. (2000), *"Data privacy in the information age"*, Westport, CT: Quorum Books, pp. 106- 107.
[36]*"Code of Good Administrative Behavior for Staff of the European Commission in their relations with the Public"* (2000). Available at: https://ec.europa.eu/info/sites/info/files/code-of-good-administrative-behaviour_en.pdf (last accessed on 19th July 2020).
[37]*"White Paper on Administrative Reform"*(2000). Available at: https://op.europa.eu/en/publication-detail/-/publication/1b8f0479-f395-43bd-8e29-be98955bd8a2/language-en pp. 7- 8 (last accessed on 19th July 2020).
[38] Kinnock, N. (2000). Available at: https://ec.europa.eu/info/sites/info/files/code-of-good-administrative-behaviour_en.pdf p.3 (last accessed on 19th July 2020).

2.4. THE TRANSPOSITION OF THE GDPR INTO THE NATIONAL LAW. FROM THEORETICAL READINESS TO PRACTICAL NONCOMPLIANCE

Although, **from a theoretical standpoint, on the principle level**, everything was planned and the adoption of GDPR should take place smoothly in a well- prepared European Union, frustratingly, Greece, alongside Slovenia, were the two last EU Member States, which faced serious difficulties regarding the incorporation of GDPR into their legal framework. The following tables (see tables a and b, below) provide in alphabetical order information about the exact date of the EU Member States' compliance with the GDPR (that is, the date on which their National Law entered into force):

	Country	***Date***		***Country***	***Date***
1	*Austria*	*25/5/2018*	*11*	*Germany*	*25/5/2018*
2	*Belgium*	*30/7/2018*	***12***	***Greece***	***29/8/2019***
3	*Bulgaria*	*1/3/2019*	*13*	*Hungary*	*26/7/2018*
4	*Croatia*	*25/5/2018*	*14*	*Ireland*	*25/5/2018*
5	*Cyprus*	*31/7/2018*	*15*	*Italy*	*19/9/2018*
6	*Czech Republic*	*24/4/2019*	*16*	*Latvia*	*5/7/2018*
7	*Denmark*	*25/5/2018*	*17*	*Lithuania*	*16/7/2018*
8	*Estonia*	*15/1/2019*	*18*	*Luxembourg*	*1/8/2018*
9	*Finland*	*1/1/2019*	*19*	*Malta*	*28/8/2018*
10	*France*	*25/5/2018*	*20*	*Netherlands*	*25/5/2018*

Table a

21	*Poland*	*25/5/2018*
22	*Portugal*	*8/8/2019*
23	*Romania*	*30/6/2018*
24	*Slovakia*	*25/5/2018*
25	*Slovenia*	*Law under process*
26	*Spain*	*7/12/2018*
27	*Sweden*	*25/5/2018*
28	*United Kingdom*[39]	*25/5/2018*

Table b

After a fast- track legal procedure (12-21 August 2019), the long-awaited relevant Greek Law no. 4624/2019 "on the protection of individuals with regard to the processing of personal data" into Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and the transposition into national law of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016" has been published and came into effect on August 29, 2019, in the Government Gazette (A 137/29.8.2019). It repealed the former National Law no. 2472/1997 "on the Protection of Individuals with regard to the Processing of Personal Data", which had transposed the

[39]The United Kingdom has officially left the European Union. However, during the "transition period" personal data can continue to flow freely from the European Economic Area (EEA) to the UK. At the end of the transition period (currently scheduled for 31st December 2020), the UK will become a "third country" for the purposes of the GDPR. To ensure that data flows from the EEA to the UK are not disrupted, the UK will need to secure an adequacy decision from the European Commission.

Directive 95/46/EC at national level and today it constitutes the basic national legal framework on personal data protection in Greece along with the GDPR itself.

It was obvious that individuals, businesses and the public sector needed clarity and certainty. Despite the binding nature of the GDPR, the majority of Greek public entities, hesitated and stubbornly refused to comply with the Regulation directly, staying attached and obsessed with the pre-existing national law 2472/1997rather than the new GDPR[40].

Nevertheless, in accordance with Article 83 of the GDPR, before even Greek Law 4624/2019 was enacted, the Hellenic Independent Authority for the protection of Personal Data[41] (from now on 'Hellenic Data Protection Authority' according to its official portal),which was established by the pre-existing Law 2472/1997, directly exercising its corrective powers pursuant to the GDPR, had already imposed a fine on the **Price Waterhouse Coopers Company (PWC BC**), which amounted to one hundred and fifty thousand Euros (EUR 150,000.00)[42]. However, this was nothing more than an exception that confirmed the general rule in Greece: Political indifference and significant delay in implementing the GDPR.

By contrast, an Asian powerhouse, Japan, has adapted its national Law in order to secure a finding of adequacy from the EU Commission, thereby allowing personal data to flow freely between the EU and Japan. The first observation that can be made is that the GDPR ensures the global visibility of the European Model of Data protection, and international influence even if the readability of this model is still unclear. In any event, the fact that the Commission has adopted on 23rd July 2018 its adequacy decision on Japan, allowing personal data to flow freely between the two economies on the basis of strong protection guarantees, marks a new era for data protection, universally. "This arrangement will serve as an example for future partnerships in this key area and help setting global standards"[43]. The fact that adequacy talks are ongoing with South Korea, exploratory work is continuous with a view to launching adequacy talks with several Latin American countries – such as Chile or Brazil[44]-coupled with the fact that – following negotiations- several other countries have been so far recognized by the European Commission[45] as providing adequate protection, such as Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Israel, Guernsey, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the USA (limited to the Privacy Shield Framework), indicate that GDPR is already a part of the European Culture, it evolves into an indispensable component of the infamous "European way of life", which they are keen to join, based on democracy, civil liberties, human rights and the Welfare State built on trust between civil society and State.

---

[40]The third chapter of the present thesis contains a brief overview of the new Law 4624/2019, its interconnection with the GDPR, the structure of the new provisions and the emphasis given on the public entities, especially in its first section.

[41]Hellenic Data Protection Authority known in Greek as «Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα».

[42]Summary of Hellenic DPA's decision No 26/2019 (2019). Available at:https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF(last accessed on 19th July 2020).

[43]European Commission portal (2019), *"European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows"*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421(last accessed on 19th July 2020).

[44]https://www.jdsupra.com/legalnews/eu-commission-issues-communication-24731/(last accessed on 19th July 2020).

[45]European Commission portal (2019), *"Adequacy Decisions"*. Available at:https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed on 19th July 2020).

From the above, it becomes clear that the actual adoption of the GDPR principles, described in chapter 2.3, as well as the transposition of the Regulation into the EU national legislations or the compliance of third countries with its principles or its basic rules, is primarily a matter of will and previous planning. It is not just a matter of geographical location or common legislative tradition. Although, the GDPR is a European legal tool, **respect for the principles and rules of the GDPR and Good Governance is not the exclusive privilege of the EU Member States. Its global influence was systematically designed and pursued.**

2.5. THE ROLE OF THE DATA PROTECTION WORKING PARTY ARTICLE 29 AND EUROPEAN DATA PROTECTION BOARD IN THE GLOBALIZATION OF THE GDPR AND THE PROMOTION OF GOOD GOVERNANCE

The first signs of working towards the **globalization of the GDPR** were set up and adopted much sooner than the application of the Regulation, by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, commonly known as the "Article 29 Data Protection Working Party" (named after Article 29 of the Data Protection Directive (DPD)[46], on June 25, 1997). The Working Party met four times in 1996. The debates focused on: 1) data transfers to third countries, 2) the level of protection in third countries, 3) the procedures for notification, 4) the exceptions to the fundamental data protection rules and 5) the application of data protection law to the Media in the light of the directive's requirement to strike a balance between freedom of expression and the right to privacy. A recommendation on this issue was subsequently adopted in 1997.European Union has been, from the outset, open to cooperation, transnational exchange of information, multilateral partnerships and Community- wide or even broader dissemination of good practice. As clearly evidenced in the Working Party's first annual report **"The directive not only regulated the processing of personal data within the EU but also included provisions on the transfer of data to third countries (articles 25 and 26).** The basic principle is that Member States should only permit such transfers, where an adequate level of protection for the data is ensured. There is clearly the possibility that there will be cases where adequate protection is not assured and, assuming none of the relevant exemptions applies, transfers will be blocked"[47]. The Working Party's tasks were briefly described in Article 30 of the DPD as follows[48]:

i) Provide expert advice to the States regarding data protection

ii) Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland

iii) Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data

iv) Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

On May 25, 2018, it has been replaced by the **European Data Protection Board (EDPB)** under the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) "equipped with a new governance and coordination model and the power to adopt binding decisions. This will allow us to play our role efficiently in giving guidance on key concepts of the GDPR."[49]The administrative restructuring of the Working Party 29 (WP29) and the focus on improving its communications

[46]Official Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (PII (US)) and on the free movement of such data.
[47]Article 29 Data Protection Working Party (1997), First Annual Report, p. 17.
[48]Article 30 Data Protection Directive. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (last accessed on 19th July 2020).
[49]EDPB portal (2018), Jelinek, A., Chair of the EDPB, statement. Available at:https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en (last accessed on 19th July 2020).

indicate that the EDPB wants to have a louder voice and become a more prominent body. Based on this, it's safe to say that the EDPB is not simply a rebranded Working Party, but a larger and more important body. Certainly, each EU country has its own independent National Data Protection Authority (DPA) to oversee the correct application of the GDPR. "However, to ensure a uniform application of the new DP rules, the GDPR established a European Data Protection Board (EDPB), an independent EU body, which is made up by the National DP Supervisory Authorities, the European Economic Area (from now on EEA) Member states and the European DP Supervisor. If the citizens' data protection rights have been violated, they can contact the National DPA, which is best placed to deal with their complaints. On the other hand, the EDPB makes sure that the GDPR is applied uniformly, so that all EU citizens enjoy the same rights, wherever they live, by adopting binding decisions in cross- border DP cases. The EDPB ensures that people can get help from their National DPAs for cross- border issues. It also encourages cooperation, exchange of information and best practices among the National DPAs. Above all, according to the EDPB Rules of Procedure, adopted on May 25, 2018, as last modified on November 23, 2018, **the Board has to act in the public's interest, "in accordance with the principle of Good Governance, integrity and good administrative behavior"[50].** Hence, data protection, good governance and good administrative behavior are explicitly interconnected and cannot be seen in isolation from one another. Finally, by advising the European Commission on issues related to the protection of PD, the EDPB makes sure that any EU legislation upholds the highest standards of data protection"[51].

In other words the EDPB acts as a guarantor of the application of the **territorial and material scope** of the GDPR, which has to be clarified and it will be covered in the next chapter.

[50] EDPB portal (2018), *"Rules of Procedure"*, Version 2. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop2_adopted_23112018_en.pdf.pdf (p. 5) (last accessed on 19th July 2020).

[51] EDPB portal (2019), promotional video. Available at :https://edpb.europa.eu/news/news/2019/edpb-video_en(last accessed on 19th July 2020).

3. THE SCOPE OF THE GDPR – LEGISLATIVE APPROACH TO THE PERSONAL DATA PROTECTION IN THE PUBLIC SECTOR

3.1. TERRITORIAL AND MATERIAL SCOPE OF THE GDPR- REGULATORY FIELD AND EXCEPTIONS

The GDPR has a wide scope, that does not just affect the business world but it clearly embraces the Public sector, which is the main object of the present study. It applies both in territorial and material terms. According to article 1 par. 1 of the GDPR, the Regulation seeks to protect fundamental rights and freedoms of natural persons and, more specifically, their right to the protection of their personal data**,** although opinions are divided regarding the human- centered character and purpose of the GDPR.

The **territorial application** is set out in article 3 par. 1. It states that "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". The regulatory nexus of the GDPR and its substantial territorial extension, based on article 3, in such a way as to include under wide-range conditions almost every processing of personal data of EU residents, irrespective of where such activities take place, provides – at least theoretically- the possibility to achieve this objective. This in itself is an achievement of the EU Legislative mechanism and a positive sign of consideration for the EU citizens. The term "activities of an establishment" is not explicitly defined in the GDPR but it's broadly interpreted in previous case law[52]. It is about where human and technical resources are available, not where an entity is registered. The processing has to take place in the context of the activities of an establishment, where this is the case the GDPR applies. Thus, establishment is a "broad" and "flexible" phrase that should not depend on legal form. An organization may be "established" where it exercises "any real and effective activity – even a minimal one" –through "stable arrangements" in the EU, consisting of the presence of a single representative within European borders[53].Secondly, the GDPR applies to non-EU established organizations that offer goods and services paid or free to data subjects in the EU and to those who monitor data subjects within the EU. Targeting the EU data subjects is apparent when a controller or processor envisages offering services to data subjects in one or more member states in the EU. In other words, the GDPR seeks to extend the reach of EU data protection Law, compared to the DPD. However, it allows EU Member States to legislate in multifarious areas.

The **material scope** is laid down in article 2. The scope is negatively defined by exceptions to: 1) households, 2) the LEA (Law enforcement agencies) where the LEA Directive 2016/618 applies since April 26, 2016, 3) foreign and security policy of the EU, including those that concern policies in respect of border controls, asylum and immigration and 4) the EU institutions. In those cases the GDPR is not applicable.

Concerning the Public sector, article 4 of the **GDPR explicitly includes public authorities in the definitions of data controllers and processors**, providing, among others, in subparagraphs 7 and 8

[52] CJEU, (C-230/14) Weltimmo VS NAIH, (C-131/12), Google Spain SL, Google Inc. VS AEPD, Mario Costeja González.
[53]Kontargyris, X. (2018), *"IT Laws in the Era of Cloud Computing",* NOMOS e-library, 1st Edition, p. 159.

that: "For the purposes of the Regulation[...] 7. **"controller"** is the natural or legal person, **public authority, agency or other body** which, alone or jointly with others, determines the purposes and means of the processing of personal data;[…] and 8. **"processor"** means a natural or legal person, **public authority, agency or other body** which processes personal data on behalf of the controller;". In addition, article 37 specifically requires **all public authorities or bodies** (except courts) **to designate a data protection officer**, which seems to be a major challenge for the Greek public sector almost three years after the entry into force of the GDPR and it shall be thoroughly examined in the framework of the questionnaire of the present study. There are other instances where specific terms are applied to public authorities to account for local laws and the effective operation of government. But to all intents and purposes, the public sector is indisputably "In".

3.2. THE IMPORTANCE OF DIRECTIVE (EU) 680/2016 IN THE PUBLIC SPHERE

Apparently, since this study deals with issues of the GDPR in the Public sector, that would be an unforgivable oversight if it did not contain any reference to Directive (EU) 680/2016 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[54].Although GDPR monopolizes international interest, Directive (EU) 680/2016, the so- called GDPR's **"little sister"-** a term used, within the DANTE project (Detecting and Analyzing terrorist- related online contents and financing activities)[55]-, regulates an equally important part of the processing of personal data, which should concern all democratic citizens in European Union. In the Greek context, some of the main competent authorities affected by that Directive are: the **Greek Police, the Hellenic Coast Guard and the Special Secretary of the Economic Crime Prosecution Authority**, which is attached to the Ministry of Economics, the backbone of the Greek Civil Service. Moreover, the aforementioned Directive applies on the activities of every **National judicial system**, whose acts and procedures of processing personal data contained in court rulings or archives of criminal procedures, may be further elaborated by the respective EU Member state, through its national legislation. In order to protect the fairness and impartiality of the judiciary, the national monitoring authorities (such as the Hellenic Data Protection Authority) do not have jurisdiction upon the processing of personal data when the courts act under their judicial power. The same safeguard applies to the prosecuting authorities.

[54]Council Framework Decision 2008/977/JHA of 27 November 2008 (2008). Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (last accessed on 19th July 2020).

[55]Fantin, S. (2018), *"Law enforcement and personal data processing in Italy: implementation of the Police Directive and the new data retention law"*. Available at: https://www.law.kuleuven.be/citip/blog/law-enforcement-and-personal-data-processing-in-italy-implementation-of-the-police-directive-and-the-new-data-retention-law/ (last accessed on 19th July 2020).

Nevertheless, in any event, the proper implementation of the "Police Directive" (EU) 680/2016 by judicial authorities, is always subject to fair and independent supervision, according to article 8 par. 3 of the EU Charter of Fundamental Rights[56].

As noted in the preceding paragraph, Directive (EU) 680/2016 is of **equal importance to the GDPR, at least regarding the Public sector**. **The main reason** is that it replaced the insufficient Council Framework Decision 2008/977/JHA, which had a restricted scope (the transboundary exchange of data between law enforcement authorities of the EU Member States) and could not maintain a fair balance between, on the one hand, the needs of the law enforcement authorities in the framework of their investigations and, on the other hand, the rights and interests of the natural and legal persons involved in these investigations. Consequently, the principles and values on processing of personal data were not respected and the rights of the data subjects were undermined.

The second reason that underlines the importance of Directive (EU) 680/2016, regarding the **citizens' treatment by the public authorities**, is that it reflects the first step for the residents of the EU area to enjoy an **equal level of protection**, whenever their personal data are processed by law enforcement authorities. For the first time, a legal act regulates uniformly in the EU context, regarding the way a police officer or a border guard shall process their personal data.

Although, compared to the GDPR, somebody might expect to find the provisions of Directive (EU) 680/2016 -by nature- less protective regarding the citizens' rights and the legal values incorporated during the processing of personal data, nevertheless, there are cases in which the GDPR's "younger sister" is stricter. For example, article 25[57] (under the title "Logging") stipulates that:

"1) Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2) The logs shall be used solely for verification of the **lawfulness** of processing, self-monitoring, ensuring the **integrity and security** of the personal data, and for criminal proceedings.

3) The controller and the processor shall make the logs available to the supervisory authority on request.

On a practical level this means that whenever a police detective carries out an investigation or shares information on a citizen, the police officer's identity, the reason for his police action, as well as the exact time and date, on which he performed that operation must be recorded. Consequently, those records may be used to ascertain the lawfulness of the processing of personal data, or the objectivity or even the security of personal data, in the context of criminal proceedings. The content of the recordings is thoroughly described in article 24 of the respective Directive which adds to the simple

[56] European Union Agency For Fundamental Rights portal, Article 8 of the EU Charter of Fundamental Rights. Available at: https://fra.europa.eu/en/charterpedia/article/8-protection-personal-data (last accessed on 19th July 2020).
[57] Directive (EU) 680/2016. Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (last accessed on 19th July 2020).

filing of the acts of processing, set out in article 30 of the GDPR and that's why the protection provided in this particular situation is considered more complete.

Once again, in the context of another legal text, i.e. Directive (EU) 680/2016, it is confirmed that the aforementioned OECD (see p. 11) basic principles of Public Administrations (2014) are totally and fully applicable.

Directive (EU) 680/2016 had to be transposed by all EU Member States. Due to the similar nature and the relevant disciplines regulated by the GDPR and Directive (EU) 680/2016, **the Greek Legislator considered that these two instruments could be incorporated in a single national law- that would be Law 4624/2019.**In particular, Directive (EU) 680/2016 was incorporated in chapter D of the aforementioned Law, becoming "a law within the Law".

3.3. THE PERSONAL DATA PROTECTION UNDER THE STIPULATIONS OF LAW 4624/2019

Although less than a year has elapsed since the adoption of L. 4624/2019, certain incontestable conclusions can be drawn from a technical angle, in order to have a clear understanding of the context within which the Public sector is required to interpret and apply the relevant legislation[58]:

1) **It is not recommended to approach the legislative framework, beginning from the national law**. The Greek law adopts certain measures for the application of the GDPR, resolves individual issues of national importance but it does not reserve its self-efficiency in relation to the Regulation. It is lacking internal unity and it cannot be read in a linear way from the beginning to the end. Starting from Law 4624/2019 and then moving to the GDPR is similar to "beginning the reading of the book from the index". Legal practitioners as well as those who are implementing the Law, including civil servants, should read, elaborate, **insist on and apply the text of the GDPR**. This provides the basic regulatory framework for the protection of personal data in Greece. That's the starting point of our study and this should be the point of return. This should be taken into account by Greek "public administrators" whose "preoccupation" with the interpretative circulars and the Greek legal texts is proverbial.

2) As indicated above, L. 4624/2019 does not have its own internal unity, however, its structure is very important and it leads us to some useful findings. Chapter A ("General Provisions") is applicable on a horizontal basis, for all processing activities of personal data in Greece, irrespective of whether they take place in the private or public sector. However, especially **Chapter A is couched in such a way as if it had been formulated exclusively for the Public Sector**. Why did the Greek Legislator place so much emphasis on the "Public entities" in Chapter A'? Mainly, **for practical and realistic reasons, probably for reasons of tradition, too**. Greek Public sector was

[58]Papakonstantinou, E. (2019),*"Ten considerations regarding the L. 4624/2019 and its connection with the GDPR"* (interview in Greek granted to ethemis portal). Available at: https://www.ethemis.gr/2019/11/25/%CE%B4%CE%AD%CE%BA%CE%B1-%CF%83%CE%BA%CE%AD%CF%88%CE%B5%CE%B9%CF%82-%CE%B3%CE%B9%CE%B1-%CF%84%CE%BF%CE%BD-%CE%BD-46242019-%CE%BA%CE%B1%CE%B9-%CF%84%CE%B7-%CF%83%CF%87%CE%AD%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%BC%CE%B5-%CF%84%CE%BF%CE%BD-%CE%B3%CE%BA%CF%80%CE%B4.html(last accessed on 19th July 2020).

considered as deserving more attention, as the GDPR brought it in front of new challenges and emergencies. We cannot fail to notice that three out of eight articles of Chapter A, deal extensively with the issues of the Data Protection Officer (from now on DPO) whose designation by the Greek public bodies is mandatory. The private sector was considered more familiar with the issue of the processing of personal data- a consideration that only time can confirm or refute.

3) Prominent place is recognized to article 5, according to which "Public sector entities are allowed to process personal data, when the processing is necessary for the performance of a task carried out in the public interest or in the legitimate exercise of official authority vested to the data controller" [the corresponding article of the GDPR is article 6 par. 1(e)]. This article is applicable on a horizontal basis for all public bodies, because it is contained in Chapter A of the respective Greek Law. The necessity for the very existence of Article 5 is deduced from the direct reading of the GDPR- at first article 6 par. 1(e) and then article 6 par. 3, which illustrate that **the legal basis for the processing is the EU Law or the National Law**. Article 6 par. 1(e) in itself is insufficient. In the existing legislative Greek framework, this specific National Law is Article 5 of the L. 4624/2019, unless a future law provides for special provisions. Until this happens and since each one of the respective processings, carried out by the public bodies, is not regulated by specific provisions, Article 5 shall remain the cornerstone of our legal system, on the basis of which we will continue to operate and perform the processings of personal data, both these falling within the scope of the GDPR and those coming under the scope of the aforementioned Directive (EU) 680/2016 (which is incorporated in Chapter D of the L. 4624/2019).

3.4. THE SCOPE OF APPLICATION OF THE GDPR AND THE CHALLENGES FOR THE PUBLIC SECTOR. THE WAY IT COULD AFFECT THE ORGANIZATIONAL STRUCTURE AND FUNCTIONING OF THE PUBLIC BODIES AND THE QUALITY OF PUBLIC SERVICES

It is clear from the above that the material and territorial scope of application of the GDPR is extremely broad. In order to implement it properly, a considerable number of privacy professionals (obviously and particularly meaning the Data Protection Officers, from now on "DPOs")is required in order to manage this project. Estimates for their number range as high as 75.000 around the globe[59]. The DPO requirement is borrowed from a similar program, Germany had in place since 2001[60]. It is noteworthy that the concept of the DPO is so well established in Germany that the Federal Data Protection Act (BDSG, Bundesdatenschutzgesetz) brought into force stricter provisions for the designation of a DPO than those adopted by the GDPR. According to Sec. 38 BDSG-new, data processors and controllers have to designate a DPO, if at least 10 persons are regularly engaged in the processing of personal data as a whole or in parts by automated means. However, it is still a new concept almost everywhere, inside and outside the EU and is bound to generate some confusion.

[59]Quade, P. (2019),*"The Digital Big Bang: The Hard Stuff, the Soft Stuff and the future of Cybersecurity",* Wiley publications, p. 254.
[60]Calvi, P. (2016),*"German GDPR implementing rules".* Available at:https://europrivacy.info/2016/12/02/german-gdpr-implementing-rules/ (last accessed on 19th July 2020).

According to the European legislative framework, a single DPO may represent a group of undertakings or multiple public authorities or bodies. The GDPR requires a DPO to be "designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices" and the ability to fulfill the tasks designated under Article 39. These tasks involve regulatory compliance, training staff on proper data handling, and coordinating with the supervisory authority, with an ability to understand and balance data processing risks. Therefore, in some instances, the necessary level of expert knowledge may be determined, inter alia, according to the data processing carried out and the protection required for the personal data processed by the organization[61] .

However, based on a 2010 report regarding Public Employment in EU Member States, given the fact that there were around 19.000.000 civil servants in EU, estimating an average of one thousand employees for every agency, which is the average number of a "large" private company within the European Union and amounts to 19.000 major public services across the EU, we will need at least 4000 DPOs in the public sector, even by the most conservative calculations[62]. In our regions, according to Greek experts[63], the number of DPOs needed in the Greek market is hovering at about 3.200 professionals both in the private and in the public sector.

These numbers are quite shocking, especially for the sluggish Greek State mechanism, which is well-known for its slow adoption to the social and legal developments and requirements. Although the real and substantial incorporation of the provisions of the GDPR, starting with the designation of qualified DPOs, should had already been completed, there are worrying indications that Greece is bringing up the rear in the EU. Undoubtedly, it is the most important legislative intervention in the area of personal data protection in the last twenty years, but this cannot be a justification for a period of tolerance and prolongation concerning the application of GDPR[64].

There is no time for idleness. Beginning with the full respect and the unconditional application of the Data Protection principles by the EU Public Administrations, specific checklists and procedures have to be **designed**, in the first instance by the staff responsible, with the greatest possible professional integrity and the greatest possible technical competence, otherwise the whole project is doomed to failure. A range of work has to be mapped according to the aforementioned principles (see pages 10-13) and that is exactly the spirit of the law, described under the term of article 25 of the GDPR as **"Data protection by design and by default"**[65]as well as in the relevant text of the provision ("the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, [….], which are **designed** to implement data-protection principles"), and explicitly referred in recital 26 of the GDPR

[61]Lambert, P. (2017),*"The Data Protection Officer. Profession, Rules and Role"* (analysis of article 37), Auerbach Publications.
[62]Heimes, R. & Pfeifle, S. (2016), *"Study: At least 28.000 DPOs needed to meet GDPR requirements",* International Association of Privacy Professionals. Available at:https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/ (last accessed on 19th July).
[63]Yiannakakis, Y. (2018). Available at: https://www.epixeiro.gr/article/89828(interview) (last accessed on 19th July 2020).
[64]Livadarou, G. (2018). Available at: https://www.eugdpr.gr/gdpr/gdpr-alp/ (interview) (last accessed on 19th July 2020).
[65] Article 25 GDPR. Available at: https://gdpr-info.eu/art-25-gdpr/ (last accessed on 19th July 2020).

according to which "The principles of data protection should apply to any information concerning an identified or identifiable natural person"[66].

A number of specific measures and steps when implementing the GDPR principles will most certainly affect the functioning and effectiveness as well as the quality of the Public Administrations and they will be analyzed in the following chapter.

[66]Recital 26 GDPR. Available at: https://gdpr-info.eu/recitals/no-26/ (last accessed on 19th July 2020).

4. CONSEQUENCES OF THE GDPR ON THE ORGANIZATIONAL STRUCTURE AND CULTURE OF THE PUBLIC BODIES

4.1. PREPARATORY STEPS FOR A PUBLIC ENTITY

A public entity, which functions clearly within the framework of its duly consolidated legal competences, can comply with the GDPR, simply, methodically and patiently. GDPR needs to be addressed by the Public Sector as a challenge for even more transparency and as an opportunity to improve citizens' confidence towards the public bodies and institutions.

According to a workshop held by the National Centre for Public Administration and Local Government, on 11th December 2017, in Athens, the appropriate ten steps[67] that need to be undertaken in this procedure are indicatively mentioned and further discussed below, however, they can also be categorized in a different manner, without precluding the possibility of consolidating two or three of them into one.

STEP 1	Preparation of a plan
STEP 2	Information, increasing preparedness
STEP 3	Designation of a Data Protection Officer (DPO)
STEP 4	Listing- Record keeping
STEP 5	Scrutiny on the public entity's compliance
STEP 6	Reviewing the data protection policies and the information provided to the public
STEP 7	Revision of internal procedures for the fulfillment of data subject rights under GDPR
STEP 8	Data Protection Impact Assessment (DPIA) in a structured and methodical way
STEP 9	Preparedness for violations of data protection rights
STEP 10	Ensuring continuous compliance with the GDPR

A similar 'roadmap' of ten preparatory steps which have to be followed by every public entity was published on the portal of the Hellenic Data Protection Authority[68].

STEP 1 Preparation of a plan

The compliance of a public entity with the GDPR has to be addressed as project of an outmost importance. At first, the necessary **steps, processes and activities** that need to be followed have to be listed, **indicatively according to the present plan (steps 1- 10).** Time constraints and deadlines have to be defined and the most suitable people who are best qualified for carrying out the tasks concerned have to be sought for the implementation of the project. The public entity has to prepare itself to address deficiencies, especially staff and equipment shortages. Although the implementation of the GDPR commenced from the 25th May 2018, no haste is needed. The public bodies must,

[67]Roussopoulos, G., ICT Auditor & Hellenic Data Protection Authority expert, Ministry of the Interior and Administrative Reconstruction (2017), *"GDPR: The new Landscape and the obligations of the Public Administration"* pp. 25-29, a workshop under the auspices of the National Centre for Public Administration and Local Government, held on 11th December 2017.

[68]Greek DPA portal (2020), *"Guide to GDPR compliance"*. Available at: https://www.dpa.gr/portal/page?_pageid=33,209418&_dad=portal&_schema=PORTAL (last accessed on 19th July 2020).

therefore, set out clear priorities and criteria for action, in order to address their outstanding urgent shortages. Their aim has to be the achievement of the compliance within a reasonable period of time, given the conditions within the specific organization.

STEP 2 Information, increasing preparedness

The key personnel in the agency have to comprehend that the Legislation concerned was fundamentally amended and the possibility to face acute compliance issues with adverse effects for the organization is increased. Also, it should be realized that the GDPR shall entail a considerable increase of workload within the public entity. Even if the latter had not initiated proceedings in order to comply with the GDPR and had already been prepared for the next day, prior to the entry into force of the GDPR, it will have to deal with an increased number of citizens' demands. Public entities should be prepared to respond to demanding and well-informed citizens. This, in itself, represents a major challenge.

STEP 3 Designation of a Data Protection Officer (DPO)

The DPO contributes to the proper implementation of the GDPR. His/ her role is not decisive but advisory. Decisions are always taken by the Administration. However, through his/her proposals he/she contributes to the ensuring of a balanced and faster compliance with the GDPR. The designation of a DPO is mandatory for all public authorities and bodies according to article 37[69] of the GDPR, regardless of their size and the range of their services. **The data protection officer: 1) may be a staff member of the controller or processor, or 2) an independent professional that fulfils the tasks on the basis of a service contract**. A single data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size but he/she has to be well aware of the organization's scope of services.

The DPO position is a novice institution for the Greek public sector. The DPO functions non-hierarchically and out of the public employment structure. He/she is directly accountable to the highest management level of the entity (controller or processor). The DPO is able to fulfill his/ her tasks within different public bodies and units, **as long as there is no incompatibility or conflict of interest of any type**. Concrete examples of roles, which would conflict with the DPO's duties[70], have already been given at an earlier stage by the WP29, such as the Chief Executive Officer, the Chief Operating Officer, the Chief Financial Officer, the Head of Human Resources, the Head of IT, within a public entity.

The Article 29 Working Party underlines, in its Guidelines on DPOs, the following safeguards are to enable the DPO to act in an independent manner:

[69]Article 37 GDPR. Available at: https://gdpr-info.eu/art-37-gdpr/ (last accessed on 19th July 2020).
[70]Working Party 29 (2016), *"Guidelines on DPOs"*, p. 15, annotation 34. Available at:https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (last accessed on 19th July 2020).

-the controllers or the processors should not issue instructions regarding the exercise of the DPO's tasks

-the controller must not dismiss or penalize the DPO for the performance of their tasks and

-there should be no conflict of interest with other possible tasks and duties.

STEP 4 Listing- Record keeping

Public entities are subject to the requirement of keeping records of processing activities[71]. It is necessary to identify and categorize those records which contain personal data on the basis of each separate activity. The organization's scope of work has to be analyzed thoroughly and the record keeping of data is required, categorized on the basis of its activities and purposes[72] of the respective public entity.

Typical examples of these records are:

* The Register of documents, which contains citizens' data, details included in these documents – these are considered as the main "cases" of each entity, relating to its basic material scope.

* The Staff files.

* Records on on-line applications: It is very important to specify the purposes pursued by the controller through these records. (for example a portal connected with the Register of documents/ the central register of records of rights, applications and activities for the users / the central register for the appropriate authorization mechanisms which define the access rights). The separation of records of personal data which serve more than one purposes is of significant importance.

* Special registers that may be kept by the public entity such as the DPO registers.

* Records for security and safety reasons, such as CCTV systems, audio or video recording archives, records of access credentials (passwords and other appropriate means) on websites and portals.

* Records for communication purposes (for example email addresses for newsletters)

STEP 5 Scrutiny on the public entity's compliance

For each one of the abovementioned identified purposes of the previous step, the public entity needs to seek, found and set down the ground rules for collecting, keeping and processing personal data, in other words, pursuant to which legal provisions it does that. It has to specify how the data have been

[71] To make the holding of the aforementioned records easier and more understandable, an indicative record base model is provided to the public by the CNIL (Commission nationale de l'informatique et des libertés= National Commission on Informatics and Liberty, an independent French administrative regulatory body, whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data), onhttps://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods (last accessed on 19th July 2020) in order to answer to the most frequent needs in terms of data processing, according to the requirements of article 30 of GDPR.

[72]Voigt, P. – Von Dem Bussche, A. (2017), *"The EU GDPR- A practical guide"*, Springer, p. 4.

gathered, the way in which the original collection of data took place, as well as the period for which the data shall be stored. Furthermore, all security measures regarding data protection, as well as their encryption[73] (refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key) or pseydonymization (meaning the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information) have to be recorded. Moreover, the members of the personnel who shall have access to the data processed should be recorded. In the event, that a public entity shares data with or transmits data to another entity, the type of collaboration has to be determined and the status of the other entity has to be entered, whether it is a public or commercial entity or a single citizen. The aforementioned cooperating legal or natural persons should also be examined concerning their compliance with the GDPR, which is considered as a "conditio sine qua non". In the event that a cooperation agreement has been concluded with such an entity, it should also be compliant with the Regulation. Additionally, it should be examined whether the data collection by the respective public entity takes place with the consent of the person concerned and if the system of obtaining the consent fulfills the legal standards of the GDPR. Finally, it should be recorded whether the entity transfers data outside the European Union or not, according to which Law or pursuant to which Memorandum of Understanding (M.O.U) it does so.

STEP 6 Reviewing the data protection policies and the information provided to the public

When the public entity collects data from citizens, it has to examine the type of information that could be accessible to the public. The GDPR contains a modification of the relevant obligation as more details and justifications are required to be presented to the citizens, in order to carry out a lawful processing. The main changes shall consist of:

-the legal basis for processing data (which inevitably makes the citizens' information, regarding the lawfulness of the processing[74], more complicated, since it presupposes a previous legal analysis and reasoning).

- the period for which the data shall be processed and stored.

The public entity has to publish the contact details of the DPO and communicate them to the national supervisory authority. It needs to examine thoroughly the type of information it provides and the specific circumstances under which the data are collected or otherwise processed. In this case it needs to examine if the relevant documents need to be revised. Whenever the public entity collects personal data from third party sources, it has to seek the most suitable way to provide the relevant information to the citizens concerned.

The previous three steps- record keeping, compliance and protection policies-must be tackled with the highest priority as a single and undivided obligation.

[73]Intersoft consulting portal (2020),*"Key issues- Encryption"*. Available at: https://gdpr-info.eu/issues/encryption/ (last accessed on 19th July 2020).
[74]Article 6 GDPR. Available at: https://gdpr-info.eu/art-6-gdpr/ (last accessed on 19th July 2020).

STEP 7 Revision of internal procedures for the fulfillment of data subject rights under GDPR

GDPR foresees new and improved rights for the citizens/ data subjects and fairly tight deadlines (one month) concerning their satisfaction. This is the time for responding to data protection rights requests. This obligation shall equally apply to public entities, which must elaborate Standard Operating Procedures (SOPs) and possess competent staff in order to perform adequately in this field. At this stage, the entity's applicable procedures should be analyzed and possible gaps, loopholes and weaknesses must be identified. In such cases, a revision of the existing procedures must take place as soon as possible. As a rule, the information has to be provided free of charge. If, in addition, further copies are requested, one can request a reasonable payment which reflects administrative costs. The controller is also allowed to refuse a data subject's requests to have an access, if it is unjustified or excessive. The preparation of standard forms, for the fulfillment of the citizens' rights or for the reasoned refusal could be of great assistance to the competent staff, whose task is to respond to the individuals' requests. Each public entity should be prepared to face complex challenges, multiple requests, tricky cases and handle unforeseen cases. In the event of refusal of a citizen's request, reference should always be made to the option of lodging a complaint with a supervisory authority, in particular in the Member State of his/ her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him/ her infringes this Regulation[75]

STEP 8 Data Protection Impact Assessment (DPIA) in a structured and methodical way

Whenever new activities or measures are about to be adopted but they entail the processing of personal data, which requires previous impact assessment, it would be more appropriate to be conducted before taking such decision or ideally before approving (or at least applying) the relevant legal provisions. A DPIA (article 35 of the GDPR[76]) should form part of the General study of impact assessment of the respective provision (given in the Explanatory Memorandum of the Law or in a separate impact assessment report). Furthermore, the national supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In every new public project that involves processing of personal data, DPIA, in a structured and methodical way, should constitute a necessary precursor to the law-making and the relevant legislative preparatory works. For instance, the proposal submitted by the Police Officers Association of Thessaloniki[77] to the Ministry of the Citizen Protection for the use of body cameras on officers' helmets (first trialed in 2012, in the USA, in Rialto, CA)[78]or the new procurement procedure regarding the creation of a new Greek Integrated Information System

[75]Article 77 GDPR. Available at: https://gdpr-info.eu/art-77-gdpr/ (last accessed on 19th July 2020).
[76]Article 35 GDPR. Available at: https://gdpr-info.eu/art-35-gdpr/ (last accessed on 19th July 2020).
[77]Police Officers Association of Thessaloniki portal (2019). Available at: https://www.eaythes.gr/anakoinoseis/anakoinoseis-e-a-y-thes/509-i-topothetisi-astynomikon-kameron-se-peripolika-kai-stoles-tha-kseskepasei-tin-ypokrisia (last accessed on 19th July 2020).
[78]University of Cambridge portal (2014). Available at:https://www.cam.ac.uk/research/news/first-scientific-report-shows-police-body-worn-cameras-can-prevent-unacceptable-use-of-force (last accessed on 19th July 2020).

Security Forms (O.P.S.E.A.) to issue new identity cards and other security documents are typical cases, where an impact study should precede. Improvisations are not allowed- they are unequivocally condemned[79].In this way, the effective implementation of "Privacy by design" and "Privacy by default" are ensured. Moreover, pursuant to recital 84 of the GDPR: "Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing"[80].The public entity has to consider:

a) who will conduct the DPIA,

b) which departments or legal advisors or experts or information security staff should be involved and

c) who will evaluate the results of the DPIA. Undoubtedly, the supervision of the whole procedure should be carried out by the DPO. A quite informative and indicative **sample DPIA template**[81] can be found on the **UK's portal of the Information Commissioner's Office (ICO)[82].**

STEP 9 Preparedness for violations of data protection rights

Secure processing of personal data with the appropriate technical and organizational measures is the issue at stake**.** In addition to the existing security measures, the Public entity has a duty to:

a) detect and evaluate if an occurrence represents a personal data breach.

b) without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority (article 33 of the GDPR) [83].

c) communicate the personal data breach to the data subject without undue delay in clear and plain language (article 34 of the GDPR)[84].

Employing appropriate techniques, such as encryption or anonymization. It refers to the process of either encrypting or removing personally identifiable information from data sets so that the individuals data remain permanently anonymous. The result is that there remains no connection of

[79]Hellenic Data Protection Authority, Decision 59/2018, (Investigation of a complaint for the use of a body camera by a police officer) (2018). Available at:http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=229,26,141,226,24,168,91,8 (last accessed on 19th July 2020).
[80]Recital 84 GDPR. Available at: https://gdpr-info.eu/recitals/no-84/ (last accessed on 19th July 2020).
[81]ICO Sample DPIA template (2018). Available at:https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx (last accessed on 19th July 2020).
[82] The United Kingdom has officially left the European Union. However, during the "transition period" personal data can continue to flow freely from the European Economic Area (EEA) to the UK. At the end of the transition period (currently scheduled for 31st December 2020), the UK will become a "third country" for the purposes of the GDPR. To ensure that data flows from the EEA to the UK are not disrupted, the UK will need to secure an adequacy decision from the European Commission.
[83]Article 33 GDPR. Available at: https://gdpr-info.eu/art-33-gdpr/ (last accessed on 19th July 2020).
[84]Article 34 GDPR. Available at: https://gdpr-info.eu/art-34-gdpr/ (last accessed on 19th July 2020).

data with an individual[85]. It is considered as the best practice, in line with the requirements of the GDPR, since the minimization of the exposure of the data subjects to a possible risk is ensured. Public entities have to analyze the risks and carry out an inspection regarding which data may represent a breach. In general, in the event of a data breach, it should be ascertained that **"citizen is the first number priority".**

STEP 10 Ensuring continuous compliance with the GDPR

Each and every public entity should revise its strategy and deal with the matter of the protection personal data with the Plan-Do-Check-Act logic. The compliance of a public entity with the GDPR and its provisions is a continuous cycle- in any event, a public organization designs, implements, monitors and reassesses.

[85]Voigt, P. – Von Dem Bussche, A. (2017), *"The EU GDPR- A practical guide"*, Springer, p. 13.

4.2. DEPARTMENTS AND PERSONS CONCERNED WITHIN THE PUBLIC ENTITIES- THEIR ROLE IN THE COMPLIANCE PROCESS

The competent departments and dedicated staff engaged in the compliance process of the GDPR rules are the administrative department (Directors- General and the legal department) and the IT staff. The proportion of their involvement depends on a number of criteria such as the nature of the organization, the Agency's mission, the volume of data and requests managed by the entity and the internal rules of operation. However, their cooperation is necessary at every step of the process described above. The administrative sector has an important role to play in activating, "sensitizing" the entity itself, in order to take initiatives and commence the process of compliance with the GDPR. IT staff shall also have a significant role to play because they have deep knowledge of the IT systems of the organization and they are acquainted with the organization's scope of work. The table below describes the involvement of each department at every step of the way:

STEP:	INVOLVEMENT OF EACH DEPARTMENT
1. Preparation of a plan	Balanced cooperation of both departments, administrative and IT staff, is required
2. Information, increasing preparedness	The burden of responsibility shifts on the administration of the Agency
3. Designation of a Data Protection Officer (DPO)	The Agency's highest authority has to appoint a DPO according to established transparent procedures[86]
4. Listing- Record keeping	Administration shall initiate the process, however the record keeping will be carried out by the IT personnel
5. Scrutiny on the public entity's compliance	The IT staff shall describe the activities of the public service operator and the Administration assisted by the legal department shall verify whether the activities are carried out lawfully, according to the GDPR. Balanced cooperation of both departments
6. Reviewing the data protection policies and the information provided to the public	This phase begins from the IT staff but it ends up being a responsibility that lays mainly with the Administration and the legal department which have to indicate the changes that need to be done
7. Revision of internal procedures for the fulfillment of data subject rights under GDPR	To a large degree, it concerns the Administration of the public entity. It has to ensure the necessary financial resources as well as the recruitment of qualified staff for the Agency in order to cope with the responses to the citizens' requests
8. Data Protection Impact Assessment (DPIA) in a structured and methodical way	It mainly concerns the methodological part of the process and falls within the context of IT and computerized systems. This step is mainly executed by the IT staff
9. Preparedness for violations of data protection rights	It is an exclusive concern of the IT personnel. IT department shall investigate the entire range of potential data breaches and it will define the level of risks that are presented by processing, from accidental or unlawful destruction, loss, alteration unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed
10. Ensuring continuous compliance with the GDPR	Balanced cooperation of both departments, administrative and IT staff, is required

[86]Link from DIAVGEIA (2018).An indicative Municipal Decision published on "DIAVGEIA" website (the clarity programme which is a breaking ground initiative on transparency issues in Greece), regarding the designation of a DPO. Available at:https://diavgeia.gov.gr/decision/view/%CE%A9%CE%9C05%CE%A9%CE%A15-%CE%A7%CE%948 (last accessed on 19th July 2020).

4.3. A CHECKLIST/ ACTION PLAN WITH DO'S AND DON'TS FOR THE PROPER IMPLEMENTATION OF THE PRINCIPLES OF THE GDPR BY THE EMPLOYEES OF THE PUBLIC SECTOR

Having regarded the above and combining them with the basic principles relating to the processing of personal data, outlined in article 5 of the GDPR, we can end up to the formulation of an indicative checklist with the do's and don'ts for the proper implementation of these basic rules of the new Regulation, which was established by the UK's Independent Authority (Information Commissioner's Office- ICO)[87]and provides a guidance in order to avoid misunderstandings and errors. It can be found in Annex I of the present thesis.

After having analyzed in depth the do's and don'ts of the new GDPR, the practical implications and ramifications in the framework of a public entity, in conjunction with the application of the basic principles laid down in the Regulation, with references to relevant scientific forms and reports, originating from the French CNIL and the British ICO, an investigation in the form of a questionnaire shall be presented in the following chapter, with participants from the broader Greek Public Sector. It will ascertain the extent to which employees of the Greek Public Service are familiar with the provisions and requirements of the GDPR, demonstrate the influence of this new institution to their culture and professionalism and allow us to draw conclusions as to the progress made in Greece and for the initiatives that must be undertaken.

[87]ICO portal, Guide to the General Data Protection Regulation (GDPR) (2019). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (last accessed on 19th July 2020).

5. SURVEY – RESEARCH ON THE GDPR IN THE GREEK PUBLIC SECTOR

5.1. GENERAL INFORMATION AND PURPOSE OF THE SURVEY

As stated above, the purpose of the investigation is to ascertain the extent to which employees of the Greek Public Service are familiar with the provisions and requirements of the GDPR, whether they are guided correctly and adequately by the competent personnel and the centralized or decentralized governance to implement the relevant legislation, whether they are following the aforementioned -in chapter 4- or similar preparatory steps individually, since the entry into force of the GDPR.

The research is a combination of quantitative and qualitative research based on the following facts : i) it is an on-line survey which produces "numerical data" and information that can be converted into numbers- there are measureable criteria (quantitative element), ii) the analyst is directly involved in the survey, iii) its purpose is the detailed description and better understanding of the compliance process, iv) the subjective element is quite strong, emphasis is given on the personal interpretation of the facts (empirical element),v) respondents are requested to submit their assessments and evaluations on a multitude of issues, vi) assumptions are presented as the questionnaire progresses.

Unfortunately, given the novelty of many issues of the GDPR in the Public Sector, there is no way of comparing the results of the present investigation with previous surveys in the Greek or the EU context. Partial conclusions and comments shall be presented separately per thematic issue (step). An overall conclusion of the survey shall be set out at the end of this chapter.

5.2. DEMOGRAPHICAL CHARACTERISTICS OF THE PARTICIPANTS

The survey was conducted during December 2019 – January 2020 via an electronic platform, ensuring the anonymity of the participants- members of the Greek Public Service, whose identity was verified by the author of the survey, before participating in the research, in order to avoid extraneous or irrelevant to the survey persons. All of them are in daily contact with citizens and have access to very sensitive personal data, since they mainly originate from various social, healthcare and welfare services in the narrow and broader public sector, within the Municipalities of Thessaloniki, Kalamaria, Neapoli- Sykies, as well as from the National Unified Social Security Fund (EFKA), the Greek Ministry of Finance and the Greek Ministry of Education and Religious Affairs. The total number of participants amounted to 116. 48,3% of the respondents are holders of a Master's Degree, 46,6% of a University or TEI Degree and 1,7% of a Doctoral Degree. Regarding the form of their employment connection with the Public Sector, 27,6% of the respondents are employees under a fixed- term contract[88] , 20,7% belong to the permanent staff, 6,9% are employees under an open-

[88] Fixed- term contract (= Σύμβαση Ορισμένου χρόνου= ΣΟΧ- according to the abbreviation used by ASEP, i.e. the Greek Supreme Council for civil personnel selection).

ended contract[89] and the majority of respondents (44,8%) are related with the Public Sector in another form of employment (mostly under a works contract[90]).

The age of the respondents ranges between 18 and 50 years old at a percentage that exceeds 90%and a significant majority of 57% has no more than 5 years of experience in the Public Sector, meaning that the preponderance of the participants are more tolerant and open to new challenges and adjustments, such as the GDPR, a conclusion that is reinforced by their equally high level of education and the fact that only 1 out of 5 among them belongs to the permanent staff.

5.3. LINKAGE OF THE QUESTIONS WITH THE 10 INDICATIVE STEPS THAT HAVE TO BE FOLLOWED

5.3.1. STEPS 1, 2 CONNECTED WITH QUESTIONS 1, 2, 3, 4: PREPARATION OF A PLAN, TIME CONSTRAINTS AND DEADLINES, PRIORITIES AND CRITERIA FOR ACTION

The first four questions of the present survey deal with steps number 1 and 2 of the aforementioned ideal progression to the GDPR compliance. As described above, the first step to attain compliance with the GDPR is to perform a gap analysis, or simply to compare the current status of the public organization and the ideal one according to the Regulation. This process will point out whether the entity is at odds with the Law and will help it figure out the next steps to full compliance. The first and most usual option for a public entity is to contract an agency to perform the analysis. This choice has the advantage of being conducted by a fresh set of eyes without bias. The second option is to conduct an in- house gap analysis. It presupposes the existence of a qualified and dedicated team with an extensive knowledge of the GDPR and EU data laws. The second option is directly examined through the second question. It is checked whether officers in charge, were assigned to draw a plan of their operational actions in order to ensure the Organization's compliance with the GDPR, under a precise timetable. On the other hand, the first question deals with a broader scope- it refers to the performance of a gap analysis by the public institution- employer in general, without considering the way it could be conducted.

Responses to Questions 1 and 2 are equally worrying and reveal ignorance. A percentage of 55% (See Figures 1 and 2) declares that it has no opinion or does not know if their employer- the public institution they are working for, has at least taken the first step in order to comply with the Regulation. Another 10% responds negatively, meaning that the first step for the preparation of many Greek Public Institutions has not been taken yet, almost two years after the GDPR's entry into force and four years after its construction.

[89] Open- ended contract (= Σύμβαση Αορίστου χρόνου = ΣΑΧ- according to the abbreviation used by ASEP, i.e. the Greek Supreme Council for civil personnel selection).
[90] Works contract (= Σύμβαση Μίσθωσης Έργου = ΣΜΕ- according to the abbreviation used by ASEP, i.e. the Greek Supreme Council for civil personnel selection).

1. Has your Employer- Public institution performed a GDPR gap analysis in order to assess the extent of its compliance with the GDPR?

116 responses

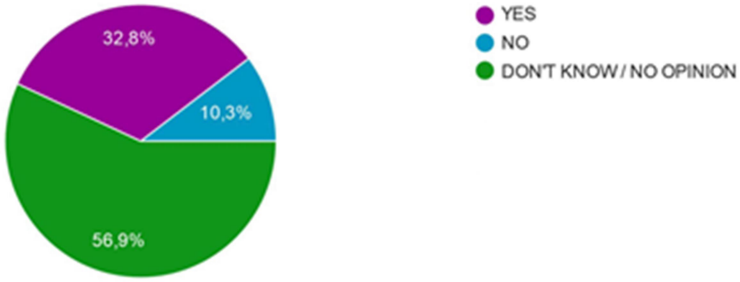

Figure 1

2. Were officers in charge mandated to plan their operational actions in order to ensure the Organization's compliance with the GDPR, under a precise timetable?

116 responses

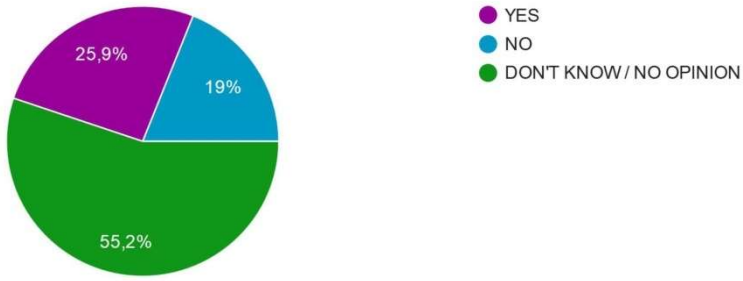

Figure 2

The third question of the present questionnaire is connected with the training of the entity's personnel on the GDPR. Not all staff members are required to have an in- depth knowledge of the relevant legislation as a DPO or an expert compliance officer would, but a good start would be to ensure that all employees are aware of the Regulation and the basic issues of data protection. In the event a public entity experiences a data breach and all staff training has been documented, this could be used as evidence to prove that the appropriate measures to prevent a data breach have been taken and the GDPR has not been taken lightheartedly. Unfortunately, an overwhelming majority of almost 70% "confessed" that they lack training or did not have an opinion about the obligations of their Organization or the respective citizens' rights, a fact that is equally disappointing (see Figure 3).

3. Have you been informed and trained on the implementation of the GDPR, the obligations of your Organization and the respective citizens' rights?

116 responses

Figure 3

The fourth question differs from the previous three. It does not refer to facts that possibly took or did not take place within the entity (such as a gap analysis or the establishment of a plan or the training of the personnel) but it requires the value judgment of the respondents, in a scale of one to ten. To be more specific it requests a certain amount of self- assessment, regarding the level of knowledge and understanding of the matters concerning the application of the GDPR, the obligations of their Organization and the respective citizens' rights. Furthermore, in the event of a negative response to the previous question number 3, there is an option of skipping the fourth question. As a result, the fourth question was answered by 58 participants (50% of their total number), meaning that even a 20,6% of the total participants, who admitted, at the previous question number 3, that they did not receive a proper training on the implementation of the GDPR, decided to evaluate their level of knowledge and understanding of the matters concerning the application of the GDPR. None of the respondents considered to evaluate himself/ herself with an excellent knowledge and understanding of the Regulation (a perfect 10 or even a 9). (see Table 1, below)

4. If the answer to question number 3 is AFFIRMATIVE, in your opinion, which is the level of your knowledge and understanding of the matters concerning the application of the GDPR, the obligations of your Organization and the respective citizens' rights? (1 corresponds to the lowest level of knowledge and understanding – 10 corresponds to the upper level of knowledge and understanding). If your answer to question number 3 was NEGATIVE, then it is not required to answer the present question, without precluding the submission of a reply (58 responses)

LEVEL OF KNOWLEDGE AND UNDERSTANDING	1 (lowest)	2	3	4	5	6	7	8	9	10 (highest)
NUMBER OF RESPONSES	4	8	6	2	12	4	12	10	0	0
%	6,9	13,8	10,3	3,4	20,7	6,9	20,7	17,2	0	0

Table 1

5.3.2. STEP 2 CONNECTED WITH QUESTIONS 5, 6, 7: INFORMATION, PREPAREDNESS, INCREASE OF WORKLOAD

As stated above, "public entities should be prepared to respond to demanding and well-informed citizens". This, in itself, represents a major challenge, because it entails a previous sufficient training of the working personnel. Fairly enough, a unanimous demand (96,6%) for further training and information is reflected through question number 5, on matters concerning the application of GDPR (see Figure 4). At this point it should be mentioned that a frustratingly high proportion of the 116 respondents admitted that they did not even know what does the abbreviation GDPR stand for (A question, half in jest half in earnest, has been raised by a high- ranking civil servant "what is this GBDR??"). Their responses provide a straightforward message- a demand for sufficient training on GDPR and – according to the answers on question number 6- it is considered as a matter of urgency (see Table 2).

5. Do you think that you need further training/ information on matters concerning the application of the GDPR? (116 responses)

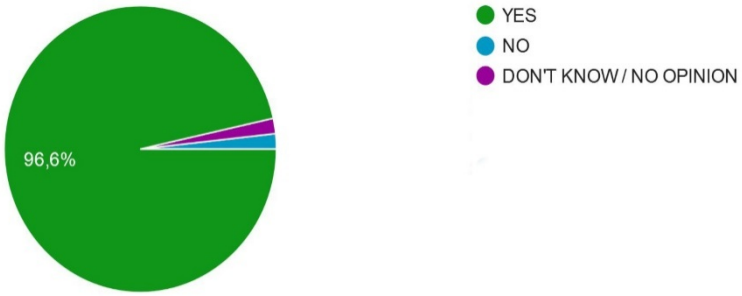

Figure 4

6. If the answer to question number 5 is AFFIRMATIVE, how urgent is the provision of further training/ information on matters concerning the application of the GDPR? (1 corresponds to the lesser urgent need for training– 10 corresponds to the most urgent need for training). Even if you answered "YES" to question number 5, you may submit your answer or proceed to the next question (110 responses)

SCALE OF URGENCY	1 (lesser urgent)	2	3	4	5	6	7	8	9	10 (most urgent)
NUMBER OF RESPONSES	0	2	4	4	10	6	20	28	16	20
%	0	1,8	3,6	3,6	9,1	5,5	18,2	25,5	14,5	18,2

Table 2

However, it is comforting to note that- according to question number 7- the majority of participants (84,5%) do not consider citizens as passive "receivers" of the Regulation or as their opponents. They

regard as vividly important, for the correct implementation of the GDPR, the citizen's summarized and comprehensible information, concerning the way his/her submitted personal data shall be processed (see Table 3). However, this is a question closely linked with the seventh step of the whole process

7. How important for the correct implementation of the GDPR do you consider the citizen's summarized and comprehensible information, with regard to the way his/her submitted personal data shall be processed? (Select 1 if you consider it totally unimportant, 10 if you consider it totally fundamental. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	2	2	10	0	10	24	18	46	4
%	0	0	1,7	1,7	8,6	0	8,6	20,7	15,5	39,7	3,4

Table 3

5.3.3. STEP 3 CONNECTED WITH QUESTIONS 8, 9, 10, 11, 12: MANDATORY DESIGNATION OF A DPO IN EACH PUBLIC ENTITY

According to a publication of the Greek National Documentation Centre[91], even the Greek General Secretariat for Information Systems (GSIS), which is the biggest Data Processing center of the Greek Public sector (meaning the data of the taxpayers), had not appointed a DPO, on the date of entry into force of the GDPR. Likewise, Athens Bar Association, a Legal Entity of Public Law, theoretically the most accountable and surely the most numerous and historical Bar Association in Greece, which – because of its legal expertise- should have fulfilled its compliance obligations in due time, published a Call for Expressions of interest for the position of the DPO, on 26th February 2019[92]. Indicative of the culture of sloppiness that has been ingrained in the Greek public sector is the opinion of certain senior officials of the Civil Service, that the failure to appoint a DPO and the inapplicability of the GDPR will not have adverse impacts on the Greek State, because, even if the Hellenic Independent Data Protection Authority (DPA) imposes a fine on a Greek Public Authority, the amount of money shall be transferred from the one code of the National Budget to another- from the authority that infringed the GDPR to the Hellenic DPA. According to that there is no need to accelerate the process of compliance in the Public Sector. Skepticism, awkwardness and confusion are particularly apparent in the responses of the participants, regarding the designation of a DPO, his/ her duties in the Public Entity, the frequency of his/ her intervention inside the organization and his/ her connection with the staff, in questions number 8, 9, 10, 11, 12. (see Figures 5, 6, 7, 8, 9 below). The most remarkable fact is that only 12% of the participants responded affirmatively as regards the appointment of a DPO by their Organization and an impressive 83,3% doesn't know the frequency of his/ her monitoring.

8. Has a DPO (Data Protection Officer) been appointed by your Organization? (116 responses)

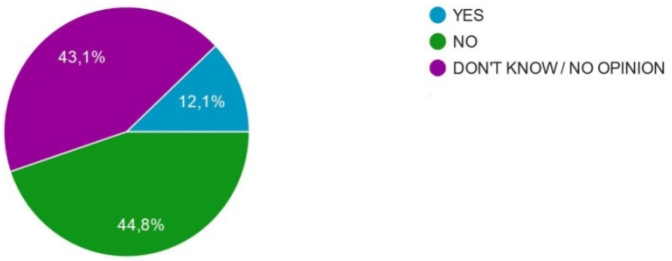

Figure 5

[91]Siasiakos, K. – Dimoula, E.E. (2019), *"The crucial role and the contribution of the Data Protection Officer (DPO) to the fulfillment of the compliance with the GDPR"*, Greek National Documentation Centre, (in Greek), p. 874.
[92]The citizen's guide portal (2019). Available at: http://www.odigostoupoliti.eu/proslipsi-dikigorou-os-ypefthynou-prostasias-dedomenon-dsa/ (last accessed on 19th July 2020).

9. If the answer to question number 8 is AFFIRMATIVE (a DPO has been appointed by your Organization), does he/she monitor the Service's compliance with the GDPR as well as with all relevant legal provisions in the field of protection of personal data? (If your answer to question number 8 was not YES, you may skip the present question) (34 responses)

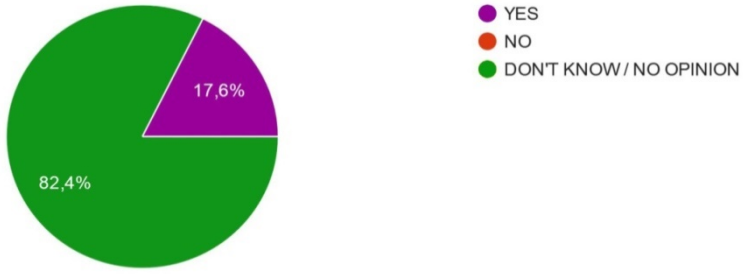

Figure 6

10. If the answer to question number 9 is AFFIRMATIVE, to what extent does the DPO monitor the compliance with the GDPR? If your answer to question number 9 was NO or in case the question was not replied, you may skip the present question (24 responses)

Figure 7

11. If the answer to question number 8 is AFFIRMATIVE (a DPO has been appointed by your Organization), does he / she inform and consult the Organization as well as its employees regarding their obligations arising from the GDPR and the other relevant legal provisions in the field of protection of personal data? If the answer to question number 8 was not YES, you may skip the present question (26 responses)

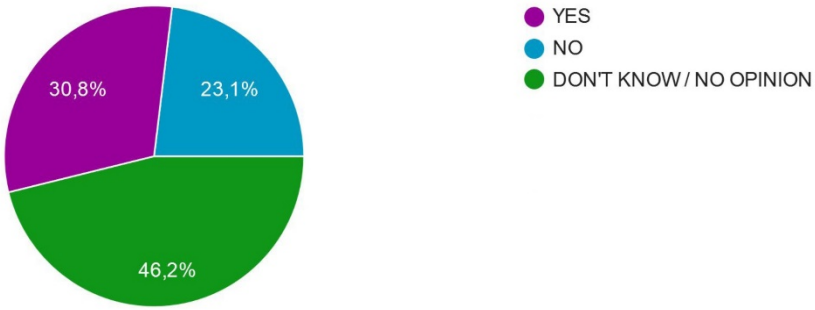

Figure 8

12. Is there an auxiliary group of employees that provides the DPO with the necessary support for the implementation of his tasks? (116 responses)

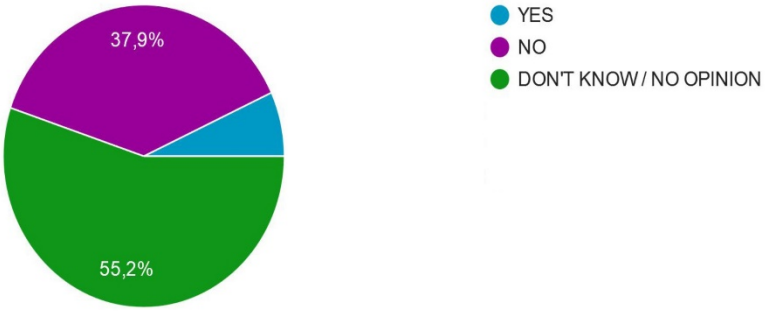

Figure 9

5.3.4. STEP 4 CONNECTED WITH QUESTIONS 13, 14, 15, 16: DEALING WITH THE RECORD KEEPING AND LISTING

As mentioned above, it is necessary to identify and categorize the records which contain personal data kept by the Organization on the basis of each separate activity. Furthermore, it is equally important to specify the purposes pursued by the controller through these records as well as to inform the public precisely about the purposes of collection and processing. The main issue at stake is whether the Organizations have standard operating procedures and specific written fields through which they inform citizens about these purposes or about the minimization of data, the collection, keeping and listing of data for specified, explicit and legitimate purposes. Given the fact that there is a notable lack of DPOs in the Greek Public Sector, it is no surprise to see that very little progress has been made, concerning the citizens' information, about the purpose of collecting and processing personal data(see Figure 10).At least the level of recognition of the value of lawfulness, fairness and transparency, the importance of data minimization as well as the collection of data for specified, explicit and legitimate purposes are exceptionally high among the respondents (more than 80% in all cases), stressing the democratic morale of the contemporary Greek civil servants (see Tables 4, 5, 6).

13. Has your Organization introduced additional specific fields in its transactions with the citizens before any submission of personal data, in order to inform the public precisely about the purpose of collecting and processing personal data? (116 responses)

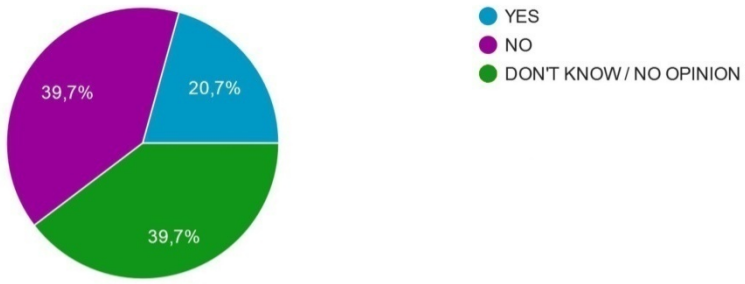

Figure 10

14. How important for the correct implementation of the GDPR do you consider the EXCLUSIVE use of the absolutely adequate, relevant and limited to the minimum necessary data, just for the purposes for which they are processed? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	2	0	8	4	10	26	6	52	6
%	1,7	0	1,7	0	6,9	3,4	8,6	22,4	5,2	44,8	5,2

Table 4

15. How important for the correct implementation of the GDPR do you consider the collection of data for specified, explicit and legitimate purposes and the fact they shall not be further processed in a way incompatible with those purposes? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW/ NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	0	4	2	2	8	20	20	52	8
%	0	0	0	3,4	1,7	1,7	6,9	17,2	17,2	44,8	6,9

Table 5

16. How important for the correct implementation of the GDPR do you consider the retention of data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or processed? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW/ NO OPINION) (116 responses)

ANSWERS	1 (totally not important)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	2	0	10	6	14	18	24	38	4
%	0	0	1,7	0	8,6	5,2	12,1	15,5	20,7	32,8	3,4

Table 6

5.3.5. STEP 5 CONNECTED WITH QUESTIONS 17, 18, 19, 20, 21: DEALING WITH THE SCRUTINY OF THE PUBLIC ENTITY'S COMPLIANCE AND THE IMPLEMENTATION OF SECURITY MEASURES

The purpose of this survey was not to enter into technical details, modalities and procedures, on the grounds that the majority of participants would not be able to answer on complicated codified technicalities. Unfortunately, there are embarrassing situations, where even the backbone of the Hellenic Public Administration, i.e. the Independent Authority for Public Revenue (AADE), is proven blatantly inadequate for the proper citizens' data protection. A complaint addressed to the Hellenic DPA in 2019, according to which thousands of hardcopies of medical archives were auctioned on a per kilo basis for recycling was just the "tip of the iceberg" among several occasions within the Greek Public Sector, where personal data remain particularly "exposed to unwelcome guests" (such as rodents and insects), in unlocked rooms or containers or file cabinets[93], in a massive and indiscriminate way.

Consequently, one of the issues under examination in this survey was to identify whether -at least minimum- precautions and security measures to prevent personal data breaches have been implemented, otherwise there would be no point at all to discuss about encryption and pseudonymization, in an uncontrollable "come one, come all" working environment. In any case, the simplest security measures should have been adopted much earlier, according to the previous legislative framework, i.e. Law 2472/1997, article 10[94], more than 20 years ago.

Unfortunately, it is observed that even the simplest security measures are not always respected. The answers provided were balanced regarding:

• the protection with updated antivirus software,

• the automatic screen locking on PCs and

•the possession of a paper- shredder in the working environment.

On the contrary, the archive system of earlier decades is still in use. Drawer units, file cabinets, round stamps, big locks, underground archive facilities constitute a common occurrence in the Greek contemporary reality (See Figures 12, 13, 14, 15).Emphasis was also given to the role- based access control/ RBAC, through question number 17 (see Figure 11). Role based access control interference is a relatively new issue. Lack of access control and automated provisioning can be costly for an organization, in more ways than one. It means new or unauthorized employees might be given access to systems they are not supposed to, and inadvertently put the security profile of the entity at risk. Unfortunately, there is still a sizeable minority of almost 30% who responded that the RBAC is still not implemented by their Organization. This means insufficient safety standards and failure to meet the requirements of the GDPR.

[93]Hellenic Informatics Union (HIU) portal (2019). Available at:https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11831&cHash=6440c42cae7666465b2640b85f14ec4b (last accessed on 19th July 2020).

[94]Hellenic Data Protection Authority portal, Law 2472/1997, article 10, p. 10. Available at:https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-APRIL010-EN%20_2_.PDF (last accessed on 19th July 2020).

Information security in public organizations revolves around four key principles. Confidentiality, Integrity and Availability (CIA) constitute the traditional triad in the world of IT and resilience of processing systems and services is the fourth one, introduced by the GDPR (article 32). Depending upon the environment, application, context or use case, one of these principles might be more important than the others. When one of the elements is absent, the security of the entity is undermined. The survey showed that in this area, Greek public administration is limping along.

17. Does the access to individual offices, PCs and management systems of the Organization take place according to each officer's particular role (role-based access control/ RBAC) in the Public Institution? (116 responses)

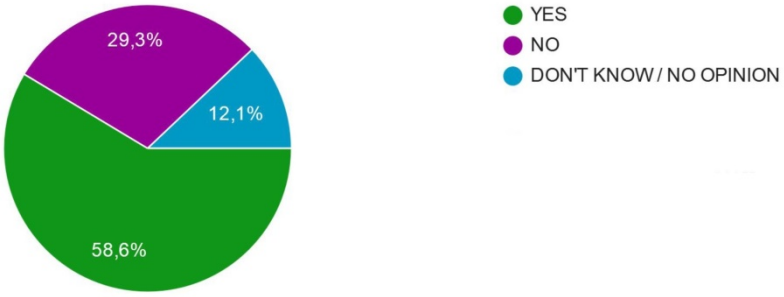

Figure 11

18. Are the servers and computers in your working environment protected with updated antivirus software? (116 responses)

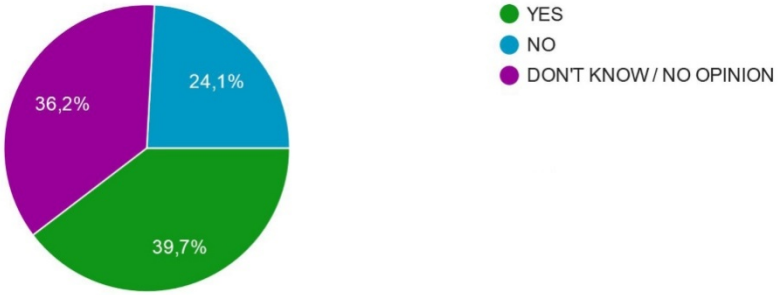

Figure 12

19. Is your computer set to lock screen automatically after 5 minutes of inactivity in combination with a password encryption and storage? (116 responses)

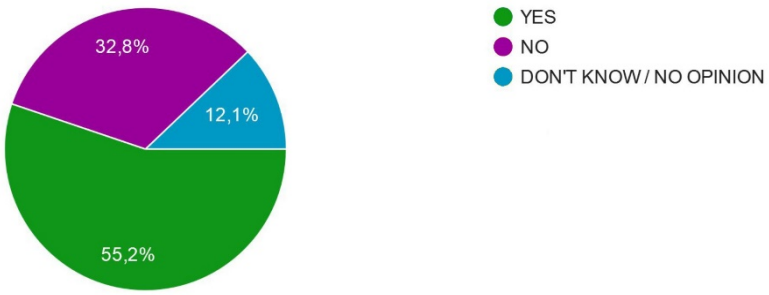

Figure 13

20. Is your office equipped with file cabinets and lockable drawers, in order to keep your physical data files inaccessible? (116 responses)

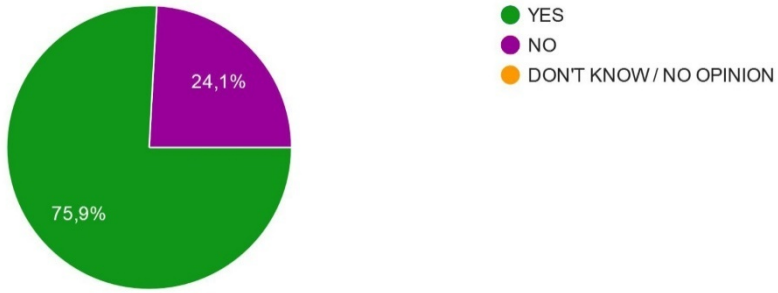

Figure 14

21. Do you have a paper shredder in your working environment? (116 responses)

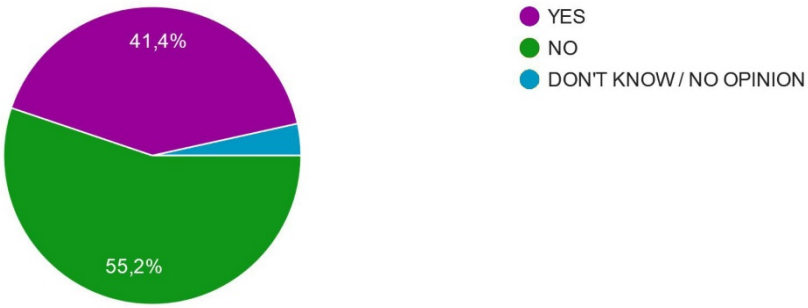

Figure 15

5.3.6. STEP 6 CONNECTED WITH QUESTIONS 7, 22, 23, 24: REVIEWING THE DATA PROTECTION POLICIES AND THE INFORMATION PROVIDED TO THE PUBLIC PLUS PUBLIC AWARENESS ON THE GDPR

At this point, participants were requested firstly to assess the level of awareness and how well informed are the citizens on GDPR (question number 22)at the time of their data collection (implying among others the knowledge of the legal basis for processing data or the time period for which the data shall be processed and stored), secondly whether the citizens' attitude towards the Organization and its employees has been modified, having in mind that a well- informed citizen is usually more demanding (questions number 23, 24)and therefore more aggressive, competitive and difficult to manage. On the contrary, an uninformed citizen remains passive and unaffected.

22. How well informed is the general public concerning the application of the GDPR? (Select 1 if it is totally uninformed and 10 if it is fully aware of the issues arising from the application of the GDPR. There is also the option DON'T KNOW / NO OPINION) (116 responses)

GENERAL PUBLIC'S DEGREE OF INFORMATION	1 (not at all)	2	3	4	5	6	7	8	9	10 (fully aware)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	22	34	8	6	14	2	0	0	0	0	30
%	19	29,3	6,9	5,2	12,1	1,7	0	0	0	0	25,9

Table 7

23. To what extent has the GDPR affected your relationship with the general public, in terms of provision of services to the citizens? (Select 1 if the GDPR hasn't affected at all your relationship with the general public or 10 if it has affected your relationship at the highest level. There is also the option DON'T KNOW / NO OPINION) (116 responses)

GDPR's DEGREE OF AFFECTION REGARDING THE PROVISION OF SERVICES TO THE GENERAL PUBLIC	1 (no affection)	2	3	4	5	6	7	8	9	10 (highest level of affection)	DON'T KNOW / NO OPINION
NUMBER OF RESPONSES	22	10	14	8	18	8	8	2	2	2	22
%	19	8,6	12,1	6,9	15,5	6,9	6,9	1,7	1,7	1,7	19

Table 8

24. Were the citizens' patterns of behavior towards the Organization modified due to the application of the GDPR, and if so, to what extent? (Select 1 if the citizens' patterns of behavior were not modified at all and 10 if they were modified at the highest level. There is also the option DON'T KNOW / NO OPINION) (116 responses)

CITIZENS' PATTERNS OF BEHAVIOUR MODIFIED?	1 (not at all)	2	3	4	5	6	7	8	9	10 (at the highest level)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	40	8	4	4	10	8	0	0	0	0	42
%	34,5	6,9	3,4	3,4	8,6	6,9	0	0	0	0	36,2

Table 9

The Greek routine remains unaltered. The public's level of understanding the importance and the implications of the application of the GDPR seems to be low. Although minimum compliance measures have been taken by the Greek public entities, in accordance with the aforementioned, it seems to be a convenient situation to everyone. Radical changes have never been welcomed in the Greek public sector. As we saw at the beginning of the survey (Question number 7),the citizen's summarized and comprehensible information, with regard to the way his/her submitted personal data shall be processed, was considered as quite important, however theory differs from practice. No civil servant wants to receive complaints from the other side of the guichet. A well informed citizen can place an employee of the public sector in a difficult situation.

5.3.7. STEP 7 CONNECTED WITH QUESTIONS 13, 25, 26, 27: REVISION OF INTERNAL PROCEDURES FOR THE FULFILMENT OF DATA SUBJECT RIGHTS UNDER GDPR

The exercise of data subjects rights under the new Regulation is offered free of charge and public entities should already have prepared standard operating procedures and the appropriate qualified staff in order to respond to requests and questions. They should already have drafted standard documents and electronic platforms in order to respond positively or negatively, but with clear justification and uniform treatment of all applicants. The avoidance of inconsistencies can be achieved only through the establishment of internal procedures and their revision, if and when necessary. Along with the already examined question 13, three additional questions of the survey are connected with this issue (25, 26 and 27- this latter question will be examined in the next section).

From the moment of the citizen's arrival at the public entity's premises, he/she must feel secure and certain that his/ her personal information shall remain safe and respectable. Confidentiality should be guaranteed not only by an unwritten moral rule or a vague commitment but by a legally binding agreement. In this case, the tool for achieving this purpose is the non- disclosure agreement (NDA) concerning the protection of citizens' personal data. It is particularly shocking that only a 26% of the respondents have signed a non- disclosure agreement (see Figure 16). Even if there are binding mandatory rules within the national law[95], which protect citizens from any leak of personal information, the existence of an NDA between the public entity and the employee adds credibility and quality to the public services and fosters a greater sense of responsibility on the part of the civil servant.

25. Have you signed a non- disclosure agreement (NDA) concerning the protection of citizens' personal data? (116 responses)

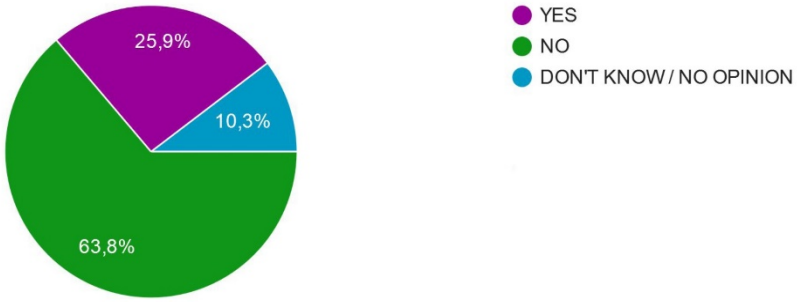

Figure 16

Furthermore, a great variety of instruments and options seems to exist (See Table 10), in the event somebody wishes to submit a complaint regarding the processing and management of his/ her

[95] In Greek Legislation it is article 26 of the Law 3528/2007 (Code of Conduct for Public Administrative Employees) in conjunction with article 1 of the Law 4254/2014 and article 2 of the Law 4057/2012 (Disciplinary Law of Public, Political and Administrative Employees and Employees of Public Entities). There is also article 252 of the Greek Penal Code.

personal data. Despite that, bearing in mind the large number of omissions and the general unpreparedness of the Greek Public Sector which is significantly disproportionate to the relatively small number of complaints, it is obvious that the average Greek citizen prefers getting his/ her job done than getting involved in time- consuming, unpleasant bureaucratic procedures and objections.

26. How does your Organization take into account complaints regarding the processing and management of data? (There is also the option DON'T KNOW / NO OPINION. You may choose as many options as you have) (116 multiple responses)

ANSWER	**RESPONSES (in absolute figures)**	**Percentage %**
In a written form (print format)	56	48,3
In a written form (electronic format)	30	25,9
Directly in person, clearing office for complaints	38	32,8
By e-mail	36	31,0
By telephone	38	32,8
By post- delivery (written notice)	22	19,0
In another way	10	8,6
DON'T KNOW/ NO OPINION	34	29,3

Table 10

5.3.8. STEP 8 AND STEP 9 CONNECTED WITH QUESTIONS 8, 27, 28, 29: PERFORMING DATA PROTECTION IMPACT ASSESSMENT (DPIA) IN A STRUCTURED AND METHODICAL WAY – PREPAREDNESS FOR VIOLATIONS OF DATA PROTECTION RIGHTS

It was chosen to carry out a joint examination of steps number 8 and 9, due to the close interdependence between them. A successful DPIA ensures to a great extent better preparedness against breaches of data protection rights. According to article 35 par. 1 of the GDPR[96]: *"1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in* ***a high risk to the rights and freedoms of natural persons****, the controller shall, prior to the processing, carry out an* ***assessment of the impact*** *of the envisaged processing operations on the protection of personal data"*. The existence of a potential "high risk to the rights and freedoms of natural persons" is equivalent to a possible future infringement of the data protection rights. Following the ancient saying of Hippocrates "prevention is better than cure", article 35 par. 2 of the GDPR stipulates that ***'2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment'***. To the extent that there are still several Greek public entities that have not appointed a DPO yet (See question number 8, above), it turns out that none of these is in a position to benefit from the advisory services of their indisputable expert leader, regarding the performance of a successful DPIA. Apparently, a considerable number of public organizations seem to falter, concerning the conduct of a DPIA.

It is extremely controversial whether a proper DPIA can be carried out in the absence of a DPO. Furthermore, it is not excluded to use the "consultation of the supervisory authority", which "should take place prior to the processing" according to recital 84 of the GDPR[97], whenever "a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation".

Unfortunately, an impressive 67,2% of the respondents (see Figure 17) replied that they didn't know whether their employer has mechanisms in place which effectively ensure the timely and lawful reporting of **potential** breaches to the competent supervisory authority ("without undue delay and where feasible, not later than 72 hours after having become aware of it", according to article 33 of the GDPR). Just a low 5,2% gave a positive answer, which means that even in the event of a personal data breach, there is a strong likelihood to remain irremediable for a long time.

[96]Article 35 GDPR. Available at: https://gdpr-info.eu/art-35-gdpr/ (last accessed on 19th July 2020).
[97]Recital 84 GDPR. Available at:https://gdpr-info.eu/recitals/no-84/ (last accessed on 19th July 2020).

27. Does your Organization have mechanisms in place which effectively ensure the timely and lawful reporting of potential breaches to the competent supervisory authority? (116 responses)

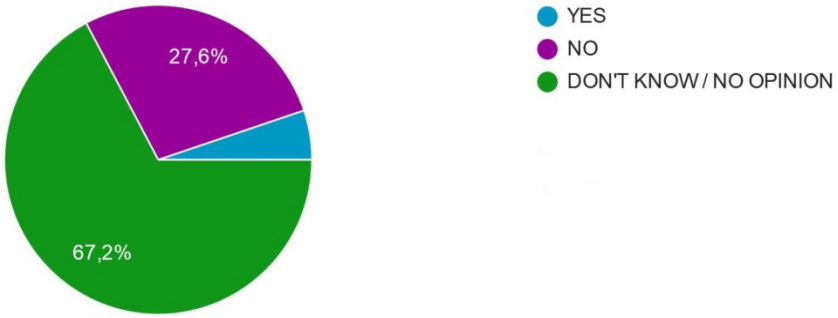

Figure 17

Nonetheless, from a theoretical standpoint, the vast majority of participants agree vividly (more than 95%) that the processing of data in such a manner that guarantees their security and protection against unlawful processing, accidental loss, destruction or alteration is of paramount importance (See table 11). Nobody wants violations of data protection rights, everyone wants to be a law-abiding civil servant, however, when the debate turns to individual responsibility, it is for sure that the average employee of the public sector shall lay the blame on the highest ranking administrative or even political superiors.

28. How important for the correct implementation of the GDPR do you consider the processing of data in such a manner as to guarantee their security and their protection against unlawful processing, accidental loss, destruction or alteration? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (not important)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	0	0	4	4	10	14	14	64	6
%	0	0	0	0	3,4	3,4	8,6	12,1	12,1	55,2	5,2

Table 11

On this issue, GDPR is crystal clear and severe: Derogations from the security rules are unacceptable. According to article 32 of the GDPR[98] *"... the **controller and the processor** shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk..."* ***Paragraph 2****: "..In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed".* In the event of infringements, article 83 of the GDPR provides for the imposition of penalties, i.e. *"administrative 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*

[98] Article 32 GDPR. Available at: https://gdpr-info.eu/art-32-gdpr/ (last accessed on 19th July 2020).

financial year, whichever is higher". Furthermore, article 82[99] of the GDPR lays down that *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to* ***receive compensation from the controller or processor*** *for the damage suffered"*.

29. How important for the correct implementation of the GDPR do you consider the imposition of liability on the Data controller and processor, in order to be able to demonstrate compliance with the GDPR before the competent supervisory authorities and courts? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	2	0	8	8	14	30	18	28	6
%	1,7	0	1,7	0	6,9	6,9	12,1	25,9	15,5	24,1	5,2

Table 12

GDPR has introduced a significant novelty. For the very first time a Regulation becomes a "cumulative" liability regime for both controllers and processors. While the controller is still the party who carries primary responsibility for compliance (the same as under Directive 95/46), processors have become subject to a host of obligations and are directly liable towards data subjects in case of non-compliance (article 82[2]). In situations involving more than one controller or processor, every controller or processor involved in the processing may in principle be held liable for the entire damage, provided the damage results from its failure to comply with an obligation to which it is subject (article 82[4]). The result is a "cumulative" liability regime, whereby each actor can be held liable in light of its role in the processing. This development was obviously welcomed by the large majority of participants (see Table 12). Civil servants always feel more secure when liability falls on more than one entities.

[99] Article 82 GDPR. Available at: https://gdpr-info.eu/art-82-gdpr/ (last accessed on 19th July 2020).

5.3.9. STEP 10 CONNECTED WITH QUESTIONS 30, 31, 32, 33: ENSURING CONTINUOUS COMPLIANCE IN THE CONTEXT OF GOOD GOVERNANCE

As mentioned above, all public organizations should revise their strategies according to the Total Quality Management (TQM) approach and the Plan-Do-Check-Act (PDCA) logic[100]. The compliance of a public entity with the GDPR is a continuous cycle- in any event, a public organization designs, implements, monitors and reassesses. Professor W.E. Deming (1900- 1993), initiator of his infamous PDCA cycle in 1993, whose contribution to the Japanese post- war economic miracle from 1950 to 1960, was recognized as decisive, could never imagine that his cycle would have such an influence outside manufacturing and economics and it would apply in the GDPR.

At this stage, the role of IT staff is of particular importance. Specific technical measures can be taken in order to ensure continuous compliance with the GDPR, such as creating and maintaining accurate inventories of software assets, tracking and responding to alerts on software assets, detecting the security state of desktops, laptops and servers, prioritizing and remediating the most critical vulnerabilities, or deploying new software which is free from known vulnerabilities. Furthermore, there are certain ways to improve data accuracy such as by setting data quality goals, meaning accuracy, completeness, reliability, relevance, and timeliness, according to ISO 9000:2015 or according to ISO 25012, which defines 15 quality dimensions of the data.

The unequivocal majority of respondents (85%) considered as totally important, for the correct implementation of the GDPR, the continuous updating of data and the adoption of appropriate measures for the immediate correction or deletion of any inaccurate personal data (see Table 13). However, it is questionable whether Greece, in the midst of crisis and austerity, can afford to initiate adequate technical support and improve its logistics.

30. How important for the correct implementation of the GDPR do you consider the continuous compliance with the Regulation and the accurate retention and continuous updating of data, the adoption of appropriate measures for the immediate correction or deletion of any inaccurate personal data, in relation to the pursued objectives of the processing. (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10	DON'T KNOW / NO OPINION
NUMBER OF RESPONSES	0	0	0	2	4	0	12	28	16	42	12
%	0	0	0	1,7	3,4	0	10,3	24,1	13,8	36,2	10,3

Table 13

[100]European Commission, Directorate- General for Employment, Social Affairs and Inclusion, (2015), *"Quality of Public Administration, a toolbox for practitioners"*, p. 68. Available at:https://www.minv.sk/swift_data/source/mvsr_a_eu/opevs/dokumenty/Quality%20of%20Public%20Administration%20-%20A%20Toolbox%20for%20Practitioners.pdf(last accessed on 19th July 2020).

However, it is comforting that the majority of respondents, despite the obvious shortcomings, as regards the implementation of the GDPR, appear to be aware of these deficiencies, still have acute reflexes, concerning issues of good governance as well as in terms of respect for citizens' rights, which is rather optimistic, after a long period of crisis and restrictions in the context of the Greek Memoranda, which have created conditions of permissiveness and gradual mithridatism on the part of the civil servants.

They acknowledge that the quality of the provided services remains unchanged (see Table 14) after the entry into force of the Regulation, nevertheless they agree that the faithful implementation of the GDPR is decisive, for the enhancement of the quality of services provided to the general public (see Table 15) and crucial for the application of the principle of good administration which should be a permanent and continuous ambition of the Greek Public sector (see Table 16).

31. How do you judge the quality of the services provided by your Organization after the entry into force of the GDPR on May 2018? (Select 1 if the quality of the services is at the lowest possible level, select 5 if it remains at the same level and 10 if it has improved to the best extent possible. There is also the option DON'T KNOW / NO OPINION) (116 responses)

QUALITY OF SERVICES AFTER GDPR	1 (at the lowest level)	2	3	4	5 (at the same level)	6	7	8	9	10 (improved at the best extent)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	4	10	2	8	48	6	4	8	0	4	22
%	3,4	8,6	1,7	6,9	41,4	5,2	3,4	6,9	0	3,4	19

Table 14

32. How important do you consider the faithful implementation of the GDPR for the enhancement of the quality of the services provided to the general public by the Organization? (Select 1 if you consider it totally unimportant and 10 if you consider it absolutely fundamental. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	8	4	4	0	12	2	20	26	16	18	6
%	6,9	3,4	3,4	0	10,3	1,7	17,2	22,4	13,8	15,5	5,2

Table 15

33. How crucial do you consider the correct implementation of the GDPR for the application of the principle of good administration? (Select 1 if you consider the correct implementation of the GDPR totally irrelevant to the application of the principle of good administration and 10 if you consider it of the utmost importance) (116 responses)

ANSWERS	1 (totally irrelevant)	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	6	6	8	10	22	24	16	22	0
%	1,7	0	5,2	5,2	6,9	8,6	19	20,7	13,8	19	0

Table 16

The last part of the survey (see tables 17, 18, 19) seeks to educe responses, which evaluate the credible application of the GDPR in Greece compared to other EU Member States and the key factors that contribute to the correct implementation of the Regulation in the public sector. Finally, the respondents expressed their opinion about whose interests are particularly served with the implementation of the GDPR. A considerable percentage of 60,3% believe that it was established for the benefit of the citizens.

34. Comparing Greece to other EU Member States, GDPR in the public sector is applicable (select one option): (116 responses)

ANSWER	RESPONSES (in absolute figures)	%
With equal credibility	4	3,4
With more credibility	0	0
With much more credibility	0	0
With less credibility	34	29,3
With much less credibility	20	17,2
DON'T KNOW/ NO OPINION	58	50,0

Table 17

35. Considering the subject of the correct implementation of the GDPR by the Greek Public Authorities, do you believe that it depends on (select as many options as you wish): (116 multiple responses)

ANSWER	RESPONSES (in absolute figures)	%
The proper information/ training/ familiarization of the public servants with the assistance of GDPR experts	98	84,5
The consciousness and professionalism of the public servant concerned	74	63,8
The threat and imposition of severe disciplinary sanctions by the Organization in case of infringement of the Regulation's provisions	40	34,5
The mentality of the average Greek public servant	44	37,9
The complexity of the Organization's structure, systems and mechanisms	58	50
The proper computerization of the Organization	70	60,3
Another factor. Indicate it	0	0,0
DON'T KNOW / NO OPINION	2	1,7

Table 18

36. Do you believe that the GDPR was adopted in order to serve, in particular, the interests of: (116 responses)

ANSWERS	NUMBER OF RESPONSES	%
Citizens	70	60,3
EU Member States	18	15,5
Businesses	12	10,3
DON'T KNOW/ NO OPINION	16	13,8

Table 19

The answers to the last question give an optimistic message. GDPR is not a control tool. There is no room for conspiracy theories. Only a very small percentage of the 116 participants (15,5 %) replied that GDPR was adopted in order to serve the interests of EU Member States. Its major objective is to contribute to the protection of citizens and respect human dignity and privacy. The results of the full questionnaire in absolute terms and percentages are provided at the end of the present Thesis, in ANNEX II.

5.3.10. CONCLUSIONS: STRATEGIC AND TECHNICAL BARRIERS

One primary goal in the EU's enactment of the General Data Protection Regulation was to harmonize the data protection laws of the EU member states and, unlike a directive, a regulation does not need to be transposed. GDPR was specifically designed to "simplify compliance measures and reduce bureaucracy"[101].Nevertheless, the investigation has shown that the sensitive field which is regulated by the GDPR and the Greek National Legislation, in addition to the difficulty in interpreting the relevant provisions, has to face some of the typical major challenges and "pathogenic phenomena" of the modern public administration, which have already been described by OECD as **strategic and technical barriers to administrative simplification**[102]. Unfortunately, most of these **strategic barriers** are present in Greek Public Administration:

a) Lack of high political support. It is obvious that support from powerful entities could make the difference in actually facilitating reform. GDPR introduced a major reform. However, in Greece, it was neither a political nor a legislative priority until 2019 and the adoption of L. 4624/2019, after a fast- track (17 days) process of consultation. Instead of launching comprehensive administrative strategies, there were voices supporting 'a period of tolerance and prolongation concerning the application of GDPR'.

b) Lack of co-ordination. Unclear division of responsibilities, ineffective communication and co-operation mechanisms in place, total failure to perform a GDPR gap- analysis*(question 1),* lack of qualified officers in charge*(questions 2 and 12),* mandated to plan their operational actions in order to ensure the Organization's compliance with the GDPR, under a precise timetable, lack of DPOs or embarrassing uncertainty as to the appointment of a DPO*(question 8),* were some of the main setbacks, during the compliance process.

c) Resistance to change. It is pretty strange that GDPR seems to not have affected the quality of services and the relationship of the civil servants with the general public, whilst, at the same time, the citizens' patterns of behavior towards the Organization remain unaltered *(questions 23, 24).* Hence, resistance derives from technical and operational levels within the administration as well as from the "hypnotized general public". It is commonplace that senior officers prefer to carry out their duties in offices equipped with file cabinets and lockable drawers, in order to keep their physical data files inaccessible. There is an old saying within traditional Greek Public Administration: "If it's not on paper, it doesn't exist". On the other hand, the lack of familiarity of the general public with new technologies, encourages stagnation and this is a condition that suits everyone. Nobody wants to rock the boat.

d) **Limited resource availability**. As pointed above, it is questionable whether Greece, in the midst of crisis and austerity -which shall definitely intensify, due to the COVID19 outbreak- can afford to initiate adequate technical support and improve its logistics. It is doubtful whether the Greek State has adequate resources to finance recruitments of qualified DPOs or well- trained auxiliary

[101] Maltese Office of the IDPC (Information and Data Protection Commissioner) portal. Available at: https://idpc.org.mt/en/Pages/gdpr.aspx (last accessed on 19th July 2020).
[102] OECD portal (2009), *"Overcoming barriers to administrative simplification strategies: guidance for policy makers"*, pp. 26- 30. Available at: https://www.oecd.org/regreform/42112628.pdf (last accessed on 19th July 2020).

employees in the midst of extensive cutbacks and significant brain- drain. In order to encourage the talented young people who left the country during the financial crisis, Greek authorities have launched a wage subsidy scheme called 'Rebrain Greece', which offers, 500 of those deemed the brightest and best, a monthly salary of €3.000 (before tax) if they return to Greece as part of the project[103].However, this project currently concerns the private sector- it should be extended to the public sector too. Effective strategies to attract talents, ensure transfer of knowledge and offer career development need to be put in place[104].

e) Lack of a comprehensive whole of government administrative simplification strategy. From the total responses, we can grasp the embarrassment and confusion of the majority of the participants. Lack of guidance and strategic leadership is apparent, even in cases where DPOs have been appointed *(questions 9, 10 and 11)*.Large and theoretically adequately staffed public entities established official working groups in order to support the implementation of the GDPR, in 2017 and 2018 but they did not appoint a DPO, until the beginning of 2020.The whole project was left at random, heavily dependent on the pride and diligence of certain employees. Unfortunately, the "do it yourself" culture seems to be predominant among civil servants[105].

Technical barriers

a) Legal complexity. It goes without saying that GDPR pertains to a myriad of legal issues, which cannot be sufficiently realized by a common official. Legal complexity reduces compliance and enforcement capacity. GDPR proved to be an over- complex regulation, which can only be interpreted with the support of qualified specialists. It is no exaggeration to deem as necessary 75.000 DPOs with legal expertise, globally, a fortiori after the outbreak of COVID-19 pandemic, which increased further more the needs for well- educated DPOs and workforce in personal data protection.

b) Lack of human skills and capacities. A deafening appeal for help ("vox clamantis in deserto" as one of the respondents very lucidly pointed out, privately) is sent through *questions 3, 4 and 5*, because of the respondents' inadequate training on GDPR. There can be no worse situation for a civil servant than that of the embarrassing exposure to the public, without education, training or guidance. In such cases, the outcome can only be shameful for the employee as well as for the employer/ public entity he/she represents. From the abovementioned questions, it became convincingly apparent that there is a serious mismatch between the needs of public administration and available training facilities and programs on GDPR. There is a unanimous (96,6%) call for further training and information on matters concerning the application of the GDPR.

c) Lack of standardization of procedures. Greek public sector has no reason to be proud of its standard operating procedures. The same applies at present, concerning the SOPs ("standard operating procedures") that pertain to the correct implementation of the Regulation. Almost 67% of the respondents replied that they have no idea whether mechanisms exist or not, In order to ensure

[103]Euronews portal (2019). Available at: https://gr.euronews.com/2019/12/11/rebrain-greece-ellada-ksana-piso-tous-neous (last accessed on 19th July 2020).
[104]European Semester Thematic Factsheet (2017), *"Quality of Public Administration"* p. 4. Available at: https://ec.europa.eu/info/sites/info/files/file_import/european-semester_thematic-factsheet_quality-public-administration_en_0.pdf (last accessed on 19th July 2020).
[105]Rammata, M. (2011),*"Contemporary Greek Public Administration – Between bureaucracy and Management"*, Edition Kritiki, pp. 205-210.

the timely and lawful reporting of potential breaches to the competent supervisory authority. At the same time 27,5% emphatically responded that no such mechanisms exist *(question 27).*

d) Lack of information and data. From the abovementioned, it is made perfectly clear that the GDPR reform is blindly designed, without a comprehensive understanding of reality and there is a strong likelihood of failure, since effective data collection or sharing mechanisms are not always in place.

e) Lack of measurement and evaluation mechanisms. Under these circumstances, it would be a luxury to demand measurement mechanisms to assess performance and target achievement, regarding the implementation of the GDPR.

As a Greek legal pundit[106], aptly puts it "apparently, we are at the beginning of an era. GDPR does nothing short of affecting every single sector of our everyday routine (since automatization must be taken for granted in our digital living environment). Changes incurred by the ambitious EU legislators are not yet fully understood in Greece. To a great extent it is more a matter of troublesome culture than of legislative framework. It will take a certain amount of time until the average Greek citizen understands that he/ she is obliged to respect personal data of third parties. Until then, we have two possible **solutions**: Either we let the DPA and the Courts shoulder the burden of changing the Greek mentality via fines, sanctions and by establishing innovative case- law through their decisions and we emphasize on training programs or we adopt new specific laws (sector- specific regulations) which shall solve today's problems in a specific way". Finally, he concludes that since past is the best predictor of the future, "Greece will pass through a long period of interesting judge-made law and vertical interventions by the Hellenic DPA". To all appearances, these vertical interventions have already begun and they will continue unabated, by the national DPAs, not only within the Greek public sector but at a European level, as set out in the next chapter.

[106]Papakonstantinou, E. (2019),*"Ten considerations regarding the L. 4624/2019 and its connection with the GDPR"* (interview in Greek granted to ethemis portal), ethemis portal. Available at:https://www.ethemis.gr/2019/11/25/%CE%B4%CE%AD%CE%BA%CE%B1-%CF%83%CE%BA%CE%AD%CF%88%CE%B5%CE%B9%CF%82-%CE%B3%CE%B9%CE%B1-%CF%84%CE%BF%CE%BD-%CE%BD-46242019-%CE%BA%CE%B1%CE%B9-%CF%84%CE%B7-%CF%83%CF%87%CE%AD%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%BC%CE%B5-%CF%84%CE%BF%CE%BD-%CE%B3%CE%BA%CF%80%CE%B4.html (last accessed on 19th July 2020).

6. THE SIGNIFICANCE OF SANCTIONS– PROPOSALS FOR THE BETTER IMPLEMENTATION OF GDPR

6.1. SANCTIONS ISSUED UNDER THE GDPR IN PUBLIC SECTOR

Although, in view of the results indicated above, participants replied that Greek public authorities apply GDPR with less or much less credibility than other EU member states, however, an overview of fines and penalties, which data protection authorities within the EU have imposed under the GDPR, indicates that even public entities in mature States and modern European democracies, still encounter similar problems when it comes to implementing the stipulations of the GDPR. This is the unpleasant angle of view.

For instance, on July 17th 2018, the **Portuguese** DPA, Comissão Nacional de Protecção de Dados (CNPD) imposed a fine of **400.000 €** on a public hospital (Centro Hospitalar Barreiro Montijo) for insufficient technical and organizational measures to ensure information security (infringement of Art. 5(1)(f), Art. 32(1)(b) and Art. 83(5)(a) of the GDPR)[107]. Investigation revealed that the hospital's staff, psychologists, dietitians and other professionals had access to patient data through false profiles. The profile management system appeared deficient – the hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the doctor's specialty.

Although, British Airways was privatized in 1987, it is still considered as the flag carrier airline of the **UK** and, furthermore, there is increasing speculation that the UK Government might move to take partial control of it, as part of a bail- out of the aviation sector[108]. However, it was charged with a fine of **204.600.000€**(not final yet), for insufficient technical and organizational measures to ensure information security (infringement of article 32 of the GDPR). More precisely, the ICO issued a notice of its intention to fine British Airways £183.39M for GDPR infringements. The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018.Through a false site, customer details were harvested by the attackers. Personal data of approximately 500.000 customers were compromised in this incident, which is believed to have begun in June 2018.The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.

On 23rd January 2020, the **Italian** DPA (Garanta) imposed a fine of **30.000€** on the Italian (Public) University Hospital of Verona (Azienda Ospedaliera Universitaria Integrata Verona) for insufficient technical and organizational measures to ensure information security (infringement of Art. 5 (1) f) and Art. 32 of the GDPR. The fine was preceded by access to health data by unauthorized persons, allowing a trainee and a radiologist to gain access to the health data of their colleagues. Investigations revealed that the technical and organizational measures taken by the hospital to protect health data had proved to be insufficient to ensure adequate protection of patients' personal data, resulting in unlawful data processing. According to the data protection authority, the breach could

[107]IAPP (International Association of Privacy Professionals) portal (2019).Available at:https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/# (last accessed on 19th July 2020).
[108]Head for points business portal (2019). Available at: https://www.headforpoints.com/2020/03/23/uk-government-may-take-control-of-british-airways-virgin-atlantic-and-easyjet/ (last accessed on 19th July 2020).

have been avoided if the hospital had simply followed the guidelines for health records issued by the data protection authority in 2015, which stipulate that access to health records must be restricted only to health personnel involved in patient care[109].

On October 19th 2019, the **Hungarian** National Authority for Data Protection and the Freedom of Information (NAIH) imposed a fine of **15.100 €** on the Town (Municipality) of Kerepes, for insufficient legal basis of data processing (infringement of Art. 6(1) of the GDPR). The city based its video surveillance practice on its legitimate interests (Art. 6 (1) of GDPR)[110]. However, according to Art. 6 (1) subparagraph 2 this legal basis shall not apply to processing carried out by public authorities in the performance of their tasks. The processing could not be based on another legal basis.

On April 25th 2019, the **Polish** National Personal Data Protection Office, Urząd Ochrony Danych Osobowych (UODO), imposed a fine of **12.950€** on a Public Sports Association, for insufficient legal basis of data processing (infringement of Art. 6(1) of the GDPR). One sports association published PD referring to judges who were granted judicial licenses online. However, not only their names were provided, but also their exact addresses and PESEL (national identification) numbers. Meanwhile, there is no legal basis for such a wide range of data on judges to be available on the Internet. By making them public, the administrator posed a potential risk of their unauthorized use, e.g. to impersonate them for the purpose of borrowing or other obligations. Although the association itself noticed its own error, as evidenced by the notification of a personal data protection breach to the President of the PDPA, the fact that attempts to remove it were ineffective determined the imposition of a penalty. When determining the amount of the fine (PLN 55,750.50), the President of UODO also took into account the duration of the infringement and the fact that it concerned a large group of persons (585 judges). It concluded that although the infringement was finally removed, it was of a serious nature. However, when imposing a penalty, the President of the Office of Competition and Consumer Protection also took into account mitigating circumstances, such as good cooperation between the controller and the supervisory authority or lack of evidence that damage had been caused to the persons whose data had been disclosed.

On October 8th 2019, the **Bulgarian** DPA, Commission for Personal Data Protection (KZLD), imposed a fine of **5.112€** on the Ministry of Interior affairs, for insufficient legal basis of data processing (infringement of Art. 5(1) and 6(1) of the GDPR) and more specifically, for unlawfully processing the personal data of data subject A.K. The Ministry of Interior sent the personal data of A.K. to the Togolese Republic (Togo)[111].

On 21st February 2020, the **Hellenic** DPA imposed a fine of **5.000€** on the Public Power Corporation S.A., for insufficient fulfillment of data subjects rights (infringement of Article 15 of the GDPR)[112]. The Decision clarified that data subjects have a right of access to the processing of their personal

[109]Data guidance portal (2019). Available at: https://platform.dataguidance.com/news/italy-garante-fines-azienda-ospedaliera-universitaria-%E2%82%AC30000-gdpr-violation (last accessed on 19th July 2020).
[110]IAPP (International Association of Privacy Professionals) portal (2019). Available at:https://iapp.org/news/a/hungarian-dpa-issues-huf-5m-gdpr-fine/ (last accessed on 19th July 2020).
[111]Privacy Affairs portal (2020). Available at: https://www.privacyaffairs.com/gdpr-fines/ (last accessed on 19th July 2020).
[112]Hellenic DPA decision No2/2020 (2020). Available at: https://ecopress.gr/wp-content/uploads/DEH-1.pdf (in Greek) (last accessed on 19th July 2020).

data and that they must also be provided with a copy of the personal data processed. No reasons need to be given for the request.

On 18th February 2018, the Maltese Lands Authority was punished with **5.000€,** by the Information and Data Protection Commissioner (IDPC) of **Malta**, for insufficient technical and organizational measures to ensure information security (infringement of Article 32 of the GDPR). Over 10 gigabytes of personal data became easily accessible to the public via a simple google search. The majority of the leaked data contained highly-sensitive information and correspondence between individuals and the Authority itself[113].

On 9th May 2019, the Data Protection Authority of Baden-Wuerttemberg in **Germany** imposed a fine of **1400€** to a Police Officer, for insufficient legal basis for data processing (infringement of Article 6 of the GDPR). The police officer, using his official user ID but without reference to official duties, queried the owner data concerning the license plate of a person, whom he did not know well via the Central Traffic Information System (ZEVIS) of the Federal Motor Transport Authority. Using the personal data obtained in this way, he then carried out an enquiry with the Federal Network Agency, in which he asked not only for the personal data of the injured parties but also for the home and mobile phone numbers stored there. Using the mobile phone number obtained in this way, the police officer contacted the injured party by telephone - without any official reason or consent given by the injured party. Through the ZEVIS and SARS enquiry for private purposes and the use of the mobile phone number obtained in this way for private contact, the police officer has processed personal data outside the scope of the law on his own authority. This infringement is not attributable to the police officer's department, since he did not commit the act in the exercise of his official duties, but exclusively for private purposes.

6.2. TOOLS AND PROPOSITIONS FOR THE BETTER IMPLEMENTATION OF GDPR

From the abovementioned "transnational list" of violations, it is made clear, that the good implementation of the GDPR concerns everyone. However, there is a more optimistic approach. Protective administrative mechanisms are in place and they seem to function adequately. As mentioned above, we are going through a long period of interesting judge- made law and vertical interventions by the European Data Protection Authorities. The fact that even minor violations of the GDPR have been identified and punished within a short period of time by the competent DPAs in most EU Member States, leaves room for optimism. Above all, it must be borne in mind that DPAs are independent administrative authorities and, at the same time, protectors of legality. They serve as a wake- up call for the EU public entities, in order to deliver solutions, long before they reach judicial proceedings and prior to the imposition of sanctions. "Prevention is better than cure" as Hippocrates said. When emphasis is placed on details, there is a pro-quality approach, which is nowadays perceived more as a commitment rather than as a strict obligation in the European context. The ultimate objective should be to preclude litigation in Courts or actions before DPAs. It is a

[113]IDPC Maltese portal (2019). Available at: https://idpc.org.mt/en/Press/Pages/Lands-Authority-Personal-Data-Breach.aspx (last accessed on 19th July 2020).

matter of Good Administration to deliver solutions at an early stage. It is a matter of **high performance organizations**, which have to excel in five factors[114]:

i) **Quality** of management (associated with steps 1, 2, 3 and 4 of the 10 preparatory steps),

ii) **Quality** of workforce (associated with steps 1, 2 and 3),

iii) **Openness and action orientation** (associated with steps 5 and 6),

iv) **Long Term orientation** (associated with steps 6, 7, 8 and 10),

v) **Continuous improvement** (associated with steps 6, 7, 9 and 10)

Good policy-making considers the implications for implementation during policy design: translating the desired state-of-affairs (the high-level objective) into practical steps, weighing up the pros and cons of all available instruments, and choosing the most effective options to achieve the policy goal. Practical steps have been designed and presented, but the single most important variable to consider, when designing a civil service reform program, is the local context in which the reform is taking place[115]. This is a 'mantra' that has been repeated many times. However, it bears repeating again as actions have not always followed words. There are a number of proposals submitted here for the appropriate application of the GDPR, both at national (Greek) and, at European level:

a) Achieving outcomes by changing behavior and simplifying procedures

As mentioned above, the sound implementation of the GDPR also remains a cultural issue. Behavior change should become the primary objective of the policy. Examples include campaigns to encourage people to lead healthier lives, protect the environment (e.g. recycling, installing solar panels or insulation), plan for retirement, engage in lifelong learning, etc. For instance, after a series of failed attempts, 2018 Greek antismoking campaign seems to be fruitful. A telephone hotline for information, as well as citizens to report any violations of the new law (on telephone number 1142) along with an extensive media campaign were created to promote the 1st September 2010 smoking ban in Greece and they proved to be effective, after a decade of innumerable setbacks. However, in the present case of GDPR, **citizens need to increase their awareness and become active in cases of data protection breaches**. **Advertising spots could challenge peoples' conscience**. A 24-hour four digit hotline, providing information, advice or assistance **(helpline),** even receiving complaints in certain urgent cases, would be a good start. Although a complaints procedure already exists and it is thoroughly described on the Hellenic DPA portal[116], it is fairly complicated. Significant paperwork is needed and a previous appeal to the Data Controller or even a contact with the competent DPO of the entity is required. Apparently, even citizens who wish to proceed, they consider the DPO as an integral part of the alleged violator/ public entity and they are reluctant to communicate with him/ her. In other words the procedure is unintendedly structured in such a way as to discourage people from even thinking about submitting a complaint. This issue should have been addressed at European

[114] De Waal, A. (2008), *"The Secret of High Performance Organizations"*, Management Online Review, April, pp.2- 3, table 2. Available at: https://www.hpocenter.nl/wp-content/uploads/2013/07/MORE-The-Secret-of-HPOs-April2008.pdf (last accessed on 19th July 2020).
[115] Repucci, S. (2012), *"Civil Service Reform: A Review"*, WIDER Working p. 3.
[116] Hellenic DPA portal (2019), complaints procedure. Available at:https://www.dpa.gr/portal/page?_pageid=33,43321&_dad=portal&_schema=PORTAL (last accessed on 19th July 2020)

level, since the complaints procedure is regulated by articles 15 to 22 of the GDPR. However, improvements can be made at national level and the establishment of one 24- hour four digit hotline or a helpdesk facility would be a move in the correct direction.

An inspiring example as to how simplification can be achieved is the "Kafka" initiative in Belgium, in 2003[117]. With its motto "la simplification fait la force" (inspired by the national motto "l' union fait la force"), the Belgian government launched it as an innovative way to cut red tape. The success of Kafka is partly linked to **the publicity around the initiative and the continuous political backing**, but also the fact that the national action is mirrored by efforts at the regional level. Managed by the Administrative Simplification Agency (ASA), it allows a user-friendly approach to collect and consider views and priorities from all stakeholders, citizens and businesses, affected by regulations. More ambitiously, the Danish 'Burden Hunter'[118] initiative does not wait for businesses or individuals to come to the administration to complain – the civil servants go out to enterprises to see the impact of regulations for themselves, especially those which are "irritating", as much as time-consuming or costly. When you engage in burden hunting, you need to go to the person ('end-user') who is actually facing the red tape, who must perform the administrative tasks required by the authorities, and can help identify the real problem and develop an appropriate solution.

Furthermore, the role of **academic community and research institutes in raising public awareness** regarding the GDPR implementation is quite important. Interactive workshops that present, in a simple and entertaining way, issues related to the protection of personal data in the digital age and introduce the GDPR and the fundamental rights it guarantees, in classrooms, museums, science centers, outreach centers, community labs, should be encouraged. In the Greek context, initiatives such as the one carried out by the Foundation for Research and Technology-Hellas ('FORTH'), which functions under the auspices of the General Secretariat for Research and Technology (GSRT) of the Ministry of Development and Investments, entitled "GDPR and forty thieves"[119] are exemplary and always welcome.

Picture 1

[117] OECD (2010), *"Better regulation in Europe: Belgium 2010"* p. 50.
[118] OECD (2010), *"e-Government Studies. Denmark: Efficient e-Government for Smarter Public Service Delivery"* p. 94.
[119] SecNews portal (2019), *"GDPR and 40 thieves Free by Mathesis"*. Available at: https://en.secnews.gr/206377/gdpr-mathesis/ (last accessed on 19th July 2020).

b) Adopting innovative approaches to monitoring and evaluation

In addition to the abovementioned helpline, various methods to increase the active citizens' engagement should be encouraged, such as providing input through SMS reporting **(crowd sourcing)**or story-telling**(micro- narrating),** or indirectly, with information being collected and analyzed remotely and in the aggregate, by the competent DPOs or even by the national DPA. Furthermore, an evaluation approach that does not measure progress towards predetermined outcomes, but rather collects evidence of what has been achieved, and works backward to determine whether and how the project or intervention contributed to the change **(outcome harvesting)**[120]**,** would be very useful for the continuous improvement of the GDPR regime and for more credibly measuring and interpreting positive or negative results of the GDPR reform. The challenge is to translate the GDPR monitoring mentality into standard public sector practice and to make the process fit the purpose of day-to-day management, whether of policies, programs, projects, services or organizations.

c) Outsourcing of public services

Public administrations do not hold the monopoly on the delivery of public services. They are looking to co- production: involving citizens and businesses directly in the provision of public goods and services. "In some cases, organizations from civil society may be better placed in terms of local knowledge and specialization to deliver services[121]. Private sector is much more flexible and better prepared in terms of implementing the GDPR, too.

When users and communities help to deliver services, it brings immediate and direct benefits[122]:

More resources to the service, in terms of knowledge, expertise, skills; Better quality services, focused on the features and outcomes that users value most highly and- above all- greater transparency in the way services are delivered. Weakness to comply with the GDPR requirements might become a "hot potato in the hands" of several Greek public entities. In order to get rid of this unpleasant situation, outsourcing certain public services, concerning the handling or processing of personal data, would be preferable. It is no secret that ICT professionals belong to high shortage occupations for Greece[123] as well as in other EU Member states. IT and ICT contractors, DPOs and other auxiliary staff, directly connected with the GDPR application, could make a valuable contribution to this end. A seemingly worthwhile initiative in this direction, adopted by the Greek government, quite recently on April 2020, during the confinement period, due to COVID-19, was the implementation of EU subsidized distance learning programs, which included training and certification on GDPR for potential DPOs- legal practitioners. However, due to its poor design, it

[120] UNDP portal (2013),"Discussion Paper: Innovations in Monitoring & Evaluating Results", p. 5. Available at:https://www.undp.org/content/dam/undp/library/capacity-development/English/Discussion%20Paper-%20Innovations%20in%20Monitoring%20&%20Evaluating%20Results%20%20(5).pdf (last accessed on 19th July 2020).
[121] OECD Conference Centre, Paris (2014),*"Innovation the Public Sector: from Ideas to Impact"* p. 33.
[122] European Commission portal (2017),*"Quality of Public Administration A Toolbox for Practitioners"* p. 83.
[123]Skills intelligence portal powered by Cedefop (2016), *"Greece: Mismatch priority occupations"*. Available at: (https://skillspanorama.cedefop.europa.eu/en/analytical_highlights/greece-mismatch-priority-occupations#_edn6 (last accessed on 19th July 2020).

was doomed to failure. Changing behavior is a hard task even for well- educated professionals, especially when a project is not convincing and well- organized[124].

d) Connecting public servants with innovative ideas from across all levels and territories of the public administration / encouraging periodic training

It is no secret that the greatest possible and most approachable support that can be provided to a public servant, originates from colleagues. Following the Dutch example of "The Smarter Network", the creation of a network of innovating professionals, DPOs, legal experts, throughout the public sector, the establishment of support structures and training programs, in order to mitigate difficulties related to compliance with the Regulation, could provide efficient solutions. On line discussion groups can be used to share knowledge, thoughts and connect public service employees. Webinars, conferences, workshops and special training sessions can be carried out periodically, in order to ensure that they keep pace with developments in the field of the protection personal data.

e) Appealing to pride/ motivating civil servants to improve their performance on GDPR compliance

The possible or potential relation between pride and performance in civil service is unclear in theory, empirically undocumented and, from a "praxiological" point of view, uncertain. However, based on some assumptions, the dynamics between the two concepts (pride and performance) can be described, using indicators. Dr. G. Bouckaert established a table which contains 12 zones of interaction that seem to be relevant[125].High performance brings pride and vice versa. He examined three major types of pride, namely, public service pride, organization-specific mission pride and activity-based task pride, and he concluded by suggesting strategies for improving pride and performance.

Typologies of pride and performance

	Performance as improving input/activity/ output links	Performance as process improvement	Performance as system improvement	Performance as closeness to ideal model
Generic public sector pride	1	2	3	4
Organization-specific mission pride	5	6	7	8
Activity-based task pride	9	10	11	12

Table 20

[124]In.gr portal (2020). Available at: https://www.in.gr/2020/03/28/greece/oxi-sto-voucher-ton-600-eyro-lene-oi-dikigoroi-antidraseis-gia-tin-eksairesi-apo-ektakto-epidoma/ (in Greek) (last accessed 19th July 2020).

[125]Bouckaert, L. & Victor, L. (2001),*"Pride and Performance in the Civil service: the Flemish case",* International Review of Administrative Sciences, pp. 65- 76.

Public servants themselves bear heavy responsibility for enhancing the public's understanding of their contribution to the health of democratic institutions. Whenever necessary, they must demonstrate that they stand by the citizens and they are trustworthy guarantors of their privacy rights.

Undoubtedly, in analyzing data and evaluating results concerning the GDPR compliance, administrations should also consider international governance indices. Governance indices are very valuable, but should be used and interpreted with care, to avoid reading too much into individual numbers without understanding first what lies behind them. Comparative positions of countries will always remain relative: there must be a first and last. While movement up and down the table over the years is an interesting guide to the effect of changes in policies and practices, public administrations are not in competition except with themselves[126]. The higher degree of GDPR compliance a public administration achieves, the higher level of democratic institutions and qualitative services it provides. The prize for improving governance is not the promotion to a "super-league of public authorities", but better societal outcomes: prosperous economies, cohesive societies, sustainable environments. **Governance indices constitute an eye-catching device and can help to focus hearts and minds (especially those of the civil servants) on the underlying problems**[127], such as the GDPR issue. It goes without saying that, due to their competitive culture, Greeks place particular emphasis on indicators and statistical numbers. It is a matter of national pride and democratic sensitivity to elevate to high- ranking positions and excel in indices such as 1) **Government at a Glance**[128], which provides reliable, internationally comparative data on government activities and their results in OECD countries, 2) **Democracy Index**[129],compiled by the Economist Intelligence Unit (EIU), a UK-based company, which concerns civil liberties, the functioning of government, political participation and political culture, 3) **Quality of Government (QoG)**[130], a survey with an information data set on the structure and behavior of public administration, carried out by the University of Gothenburg.

For example, it is gratifying to read in "2019 Fact sheet", presented by "Government at a Glance", that Greece made great progress in supporting the reuse of open government data. Greece managed to move from performing below the OECD average (0.44 in 2017) to become one of the top performers in 2019 when the OECD average was 0.52[131].This is a major step forward in the area of personal data protection, especially since it is recognized as positive development by OECD.

The importance of **international governance indices for public administrations** can be compared with the significance of **ratings** performed by credit rating agencies **for national economies and credit institutions**. They have an **impact both on factual and psychological level.**

[126] European Commission (2017),*"Quality of Public Administration A Toolbox for Practitioners"* p. 90.
[127]Ibid, p. 95.
[128]OECD portal (2019), *"Government at a Glance"*. Available at: https://www.oecd.org/gov/govataglance.htm(last accessed on 19th July 2020).
[129]Democracy Index (2019). Available at: https://www.eiu.com/topic/democracy-index (last accessed on 19th July 2020).
[130]Quality of Government (2020). Available at: https://qog.pol.gu.se/ (last accessed on 19th July 2020).
[131]OECD portal (2019), *"Government at a Glance- Country Fact Sheet- Greece"*. Available at: https://www.oecd.org/gov/gov-at-a-glance-2019-greece.pdf (last accessed 19th July 2020)

Smoother compliance with the GDPR means better quality of public administration, high quality of management, respect to European Institutions and attention to privacy rights and civil liberties, consequently higher global ranking in the international indices and better societal outcomes. It is for sure that GDPR compliance will be duly recognized and valued as a crucial indicator for the evaluation of quality and sound administration in the near future. Greek civil servants might become proud about their democratic sensibilities and the sound application of the GDPR, demonstrating that their country is validly regarded as the cradle of democracy.

f) Encouraging external scrutiny on the GDPR implementation/ the role of Media

The transparency of government helps to stimulate policy development in public administrations, much in the same way that competition entices enterprises to find better ways to satisfy customers' needs, through external pressure. An independent and investigative media may not always be welcomed by governments, but it provides a window into the workings of public administrations and a source of scrutiny that drives up the standards of government and is especially valuable in putting ethics and integrity in the spotlight. Through discourse and dissent, the media might provide a "safety valve", that is vital for the successful implementation of the GDPR. Though it might seem like a constant barrage of privacy-policy bashing from the media, this kind of scrutiny is for the benefit of citizens as well as for privacy professionals, who need to be there from the design phase of a new product, rewrite a privacy policy, remain there to respond to criticism and, often, learn from vulnerabilities or misunderstandings, highlighted by the media. The example of Microsoft, in the private sector, is typical. In the wake of Windows 10 release, Microsoft decided to change its privacy policy and services agreement, and because of that, the company's changes went under predictable media scrutiny[132]. As a result, among other reactions, in October 2017, the DDPA (Dutch Data Protection Authority) issued a complaint asserting that Windows 10's privacy policies did not comply with the laws of the Netherlands, as Microsoft did not provide sufficient information on what information was collected at the "Full" telemetry level and how it was processed. Microsoft disputed the claim that it did not provide enough disclosure of the "Full" telemetry level, and stated that it was working with the DDPA to "find appropriate solutions"[133].

g) Capitalizing on the forward momentum of ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. The Agency is located in Athens, Greece and it also has a second office in Heraklion, Greece. The mission of ENISA is to achieve "a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other

[132]The Post and Courier (daily newspaper in South Carolina, USA) portal, (2015), *"3 Windows 10 privacy gotchas"*. Available at:https://web.archive.org/web/20151117013829/http://www.postandcourier.com/article/20150902/PC05/150909997/1052/3-windows-10-privacy-gotchas(last accessed on 19th July 2020).

[133]Arstechnica portal (2017). Available at: https://arstechnica.com/gadgets/2017/10/dutch-privacy-regulator-says-that-windows-10-breaks-the-law/(last accessed on 19th July 2020).

relevant Union stakeholders"[134].The above- presented survey has shown that one of the main weaknesses of the modern public administration concerning the GDPR application and data protection in general is the enforcement of the existing rules on cybersecurity. One of **the top priorities of the "ENISA Work Programme 2020- 2022"** is supporting EU Policy Implementation, in the framework of which new requirements, "primarily associated with the implementation and secondly transposition of the EU legal instruments in place in the Member States, will be taken into account, including aspects of the Directive on Security of Network and Information Systems ("NIS Directive")[135], the Cybersecurity Act, **GDPR,** as well as the preparation for the upcoming e-Privacy Regulation, etc". This output will analyze gaps and, in particular, **provide guidelines for the development or amendment of standards, facilitating the promulgation and adoption of NIS standards**. ENISA **provides its technical and organizational NIS know-how, which can be further leveraged to extend or assess standards to render them more appropriate to stakeholders.** By bringing its concrete NIS policy expertise to the table, ENISA will produce "how to" and "what else" guides in to contribute to the European standardization[136].

Apparently, ENISA can decisively transfuse added value to all EU policies concerning the GDPR implementation, indicatively by;

i) providing high- quality recommendations, based on the experience of the EU NIS community,

ii) promoting the exchange of best practices between the EU Member States,

iii) creating the conditions for enhanced cooperation in the future,

iv) supporting the development and implementation of the Union's standardization (European and international, as appropriate) and certification policy.

It is obvious that the European Institutions are seeking to enhance the role of ENISA and this is vividly reflected in a statement issued by ENISA Executive Director, Udo Helmbrecht, on June 2019, in which he thanked the Council, European Parliament and Commission and welcomed the reinforced role of ENISA in the European cybersecurity ecosystem[137]. The implementation road map exists. It remains to be seen if it will be carried out.

[134] Article 3(1) of ENISA Regulation (EU) No 2019/881.
[135] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[136]European Union Agency for Cybersecurity (2019), *"ENISA Programming Document 2020- 2022",* Publication Office of the European Union, p. 42. Available at:https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022(last accessed on 19th July 2020).
[137]ENISA portal (2019), *"The European Union Agency for Cybersecurity- A new chapter for ENISA"*. Available at: https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa (last accessed on 19th July 2020).

CONCLUSION

It is clear that the implementation of the GDPR constitutes a tough challenge. While it champions democratic ideals, uncertainty remains when it comes to its cumbersome application. Although being open to citizens sounds great, customer- oriented and, theoretically, it would make the Regulation more accessible, it is questionable if this is the actual ambition of the States, especially under the current circumstances. Some Data Protection Authorities indicate that they are unduly burdened by the number of complaints and data breach notifications, and are therefore **unable to concentrate on compliance checks**, although according to article 52 par. 4 of the GDPR "Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers". Several supervisory authorities are not capable of carrying out the requisite number of inspections due to a significant lack of adequate human and financial resources (even the German Federal and State Data Protection Authorities raised a warning flag on this issue[138]) and **controllers both in public and private sector have identified a shortfall in the number of checks being carried out**. Under these circumstances, a second thought should be given in favor of relaxing the existing regulatory framework of the processing of certain categories of personal data and place emphasis to the really important areas, in both the public and private sector. For better or for worse, more financial resources are not a panacea to address existing weaknesses.

In addition to the proposals presented in the previous chapter, it is also a matter of legislative technique. The solution might lie in adopting a different and more flexible approach. In liberal states, the Law stipulates what is prohibited. Everything else is acceptable, unless it is in conflict with a general legal principle. Of course there are certain activities which are prohibited per se, such as the use of drugs or weapons, apart from certain exceptions laid down in the Law. Whilst, theoretically, one of the main policy objectives of the Regulation is to facilitate[139] the **free flow of personal data**, the aggregate impression is that GDPR rather intercepts the flow of information instead of supporting it. As in the cases outlined above (the examples of drug or gun permit), it appears that in order to be able to process personal data, a controller or a processor has to satisfy exceptional requirements, the principles of the GDPR, instead of merely avoiding to violate them. The rule is that the processing of personal data is generally forbidden, unless you have a right to do it, according to the principles[140].This logic is proving particularly troublesome and inelastic.

Beyond any doubt, processing of information relevant to sexual orientation, health issues, political views, religion or children's rights, which fall within sensitive or special categories of personal data (article 9 GDPR) should be performed exceptionally and only under specific conditions. However, regarding the rest of personal data-**taking into account the excessive administrative, bureaucratic, financial and technical burdens, as a result of the scrupulous application of the GDPR-**an alternative in order to lighten the existing workload of the DPAs, the DPOs, the public administration

[138]Independent German Federal and State Data Protection Supervisory Authorities (2019),*"Report on Experience Gained in the Implementation of the GDPR"*, p. 4. Available at: https://diogoduarte.eu/3d-flip-book/dsk-report-on-experience-gained-in-the-implementation-of-the-gdpr/

[139]Article 51 GDPR. Available at: https://gdpr-info.eu/art-51-gdpr/, Recital 3 GDPR. Available at: https://gdpr-info.eu/recitals/no-3/, Recital 9 GDPR. Available at: https://gdpr-info.eu/recitals/no-9/ (last accessed on 19th July 2020).

[140]Rücker, D.-Kugler, T. (2018),*"New European general data Regulation- A Practitioner's Guide"*, Edition Beck- Hart-Nomos p. 51.

and the private businesses could be the adoption of special laws, regulating other issues, such as breach of confidentiality of banking secrecy or telecommunications, surveillance in private places etc. Instead of describing when the processing of personal data is lawful, GDPR should enumerate the few exhaustive and specific exceptions to the general rule. Although this approach seems to be against the mainstream perspective, it is a matter of common sense and necessity.

It is somewhat ironically highlighted that almost two years after its entry into force, public entities cannot achieve full compliance with the GDPR. It is a laborious and evolving process, whose successful outcome is heavily dependent on the proper organization and preparation of the respective public entities and private businesses. However, nobody can predict certain imponderables (such as the COVID-19 outbreak) which alter priorities or even the whole institutional framework. With regard to GDPR implementation, the public sector will encounter difficulties, on matters of accessing and using personal health data, tracking citizens' movements and contacts through mobile apps, tracking travelers and their relatives and on plenty of other issues for the protection of public health and security. Severe restrictions shall be imposed on people's freedoms, including their privacy and other human rights. Some may be effective, based on the advice of epidemiologists, others will be not. But all of them must be temporary, necessary, and proportionate.

Strategies and plans on the GDPR implementation need to be flexible and adaptable to global game changers, rather than robust and fixed. As the European Data Protection Supervisor, Wojciech Wiewiórowski, eloquently stated, after the COVID-19 epidemic outbreak *"What we had in mind were natural disasters causing unexpected changes in the legislation at both European and national levels. However, we never expected such a tragedy to have occurred so quickly! […] Who would have thought that the external borders of the European Union would be closed, that the Schengen area would literally stop operating, that xenophobia would be on the rise? We could not even imagine that reasonable people would start asking internet and telecom operators to possibly track each and every person in Europe using his or her mobile location data in real time, and to create a diagram representing all physical interactions between people over the last few days.*[…] ***Covid-19 is a game changer.*** *Thinking about the EDPS' strategy for the next five years, we have to look again at our text. Whatever happens in the next few weeks,* ***we know the word will not be the same. We will all be confronted with this game changer in one way or another.*** *And we will all ask ourselves whether we are ready to sacrifice our fundamental rights in order to feel better and to be* ***more secure****"*[141].

It is evident that, for the second time during the last twenty years, fundamental data protection issues arise, in the present case even more intensively, at global level. Almost one and a half month after 9/11 attacks, in the name of national security, the USA Patriot Act[142], signed into law by U.S. President George W. Bush, on October 26, 2001, was the first of many changes to surveillance laws that made it easier for the US government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the activity of innocent Americans on the Internet. While most Americans thought it was created to arrest terrorists, the Patriot Act actually turned regular citizens into suspects.

[141] European Data Protection Supervisor portal (2020), *"The moment you realize the world has changed: re-thinking the EDPS Strategy"*. Available at: https://edps.europa.eu/press-publications/press-news/blog/moment-you-realise-world-has-changed-re-thinking-edps-strategy_en (last accessed on 19th July 2020).

[142] USA Patriot Act of 2001 (2001). Available at:https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (last accessed on 19th July 2020).

However, Europe is a totally different case. It is quite uncertain whether European citizens will uncomplainingly accept unjustifiable and disproportionate restrictions or unaccountable treatment of their personal data, even under the thread of the recent pandemic. The State's abuse of surveillance and record keeping during the Second World War and Cold War, left deep a strong cultural mark in the minds of the Europeans[143], a fact that explains the elevation of the protection of privacy, not only to a positive legal level, but to a fundamental, constitutional right and a European social acquis. Similarly, at national level, the Greek post War anti-liberal governments' and particularly the military junta's practice of keeping files not just for dissidents, but for a broad part of the population, even today subconsciously correlates the collection of personal data by the state, to oppression. **In this context of suspiciousness and distrust, modern public administration needs to win back the public's trust, defending its role as a guarantor of democracy.** The level of confidence towards public administration and the societal well- being can only be improved, by ensuring the high quality of public services in such sensitive policy areas, as the data protection field. Unfortunately, until today, the Sustainable Governance Indicators, which look at governments' capacity to deliver sound policies as well as the participatory and oversight competencies of social actors, demonstrate that Greece has one of the weakest executive capacities among the EU Member States[144]- obviously the same applies to the GDPR implementation. Stronger involvement of civil society and academia in policy development and evaluation can boost the quality of polices. This has been clearly demonstrated, during the COVID-19 crisis (at least until the date of completion of the present thesis), through the successful response to the virus spread in Greece, a campaign led by Dr. Sotirios Tsiodras, spokesperson and Professor of Medicine and Infectious Diseases. His thorough knowledge of the subject, the honest, humanistic and transparent approach of the public won the souls and minds of Greek people. Let this be a guiding example for all of us.

[143]Stute, D.J. (2015),*"Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD"*. Michigan Journal of International Law, p. 652. Available at:https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1085&context=mjil (last accessed on 19th 2020).

[144]European Semester Thematic Factsheet (2017), "Quality of Public Administration" pp. 3- 5. Available at:https://ec.europa.eu/info/sites/info/files/file_import/european-semester_thematic-factsheet_quality-public-administration_en_0.pdf (last accessed on 19th July 2020).

BIBLIOGRAPHY

BOOKS

1. Alexandropoulou- Egyptiadou, E. (2016), *"Personal Data"* (in Greek),Edition Nomiki Bibliothiki, Athens

2. Bygrave, L. (2014), *"Data Privacy Law, An international perspective",* Edition Oxford University Press

3. Castets-Renard, C. (2009), *"Droit de l' Internet",* Edition Montchrestien

4. Darby, H.C. (1977), *"Domesday England",* Edition Cambridge University Press

5. Igglezakis, I. (2004), *"Sensitive Personal Data"* (in Greek),Sakkoulas Publications

6. Klosek, J. (2000), *"Data privacy in the information age",* Praeger Publications

7. Kontargyris, X. (2018), *"IT Laws in the Era of Cloud Computing",*Edition Nomos Verlagsgesellschaft

8. Lambert, P. (2016), *"The Data Protection Officer. Profession, Rules and Role",* Edition Auerbach

9. Quade, P. (2019), *"The Digital Big Bang: The Hard Stuff, the Soft Stuff and the future of Cybersecurity"*, Edition Wiley

10. Rammata, M. (2011), *"Contemporary Greek Public Administration – Between bureaucracy and Management"*, Edition Kritiki

11. Rücker, D.-Kugler, T. (2018), *"New European general data Regulation- A Practitioner's Guide",* Edition Beck- Hart- Nomos (2018)

12. Selinger, E. &Polonetsky, J. (2017), *"The Cambridge Handbook of Consumer Privacy",* Edition Cambridge University Press

13. The University of Macedonia, MIPA Book (2019), Edition University of Macedonia

14. Voigt, P. – Von Dem Bussche A. (2017*), "The EU GDPR- A practical guide",* Springer Publications

JOURNALS

1. Adams, B. & Judd K. (2015),*"Global Policy Watch Briefing #19",* Global Policy Forum. Available at: https://www.globalpolicy.org/home/271-general/53036-data-is-the-new-gold.html(last accessed on 19th July 2020)

2. Ariel, B. (2014), *"Research",* Cambridge University. Available at: https://www.cam.ac.uk/research/news/first-scientific-report-shows-police-body-worn-cameras-can-prevent-unacceptable-use-of-force(last accessed on 19th July 2020)

3. Bouckaert, L. & Victor, L. (2001),*"Pride and Performance in the Civil service: the Flemmish case"*, International Review of Administrative Sciences

4. De Andrade, N. (2014),*"Oblivion: the right to be different from oneself: re-proposing the right to be forgotten. The Ethics of Memory in a Digital Age"*, Palgrave Macmillan, London

5. De Hert, P. and Papakonstantinou, V. (2016), *"The new General Data Protection Regulation: Still a sound system for the protection of individuals?"*, Computer Law & Security Review

6. De Waal, A. (2008),*"The Secret of High Performance Organizations"*, Management Online Review. Available at: https://www.hpocenter.nl/wp-content/uploads/2013/07/MORE-The-Secret-of-HPOs-April2008.pdf (last accessed on 19th July2020)

7. Gellert, R. and Gutwirth, S. (2013),*"The legal construction of privacy and data protection",* Computer Law & Security Review

8. Horvitz, E. & Mulligan, D. (2015),*"Data, privacy and the greater good",* Science Magazine

9. Kulk, S. and Zuiderveen Borgesius, F. J. (2017),*"Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe"*, Cambridge University Press

10. Mannocci, G. (2018),*"The Public Administration and the Citizens Privacy Protection",*The Italian Law Journal

11. McDermott, Y. (2017),*"Conceptualizing the right to data protection in an era of Big Data. Big Data & Society"*, SAGE Journals

12. Moshell, R. (2005),*"And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection",* Texas Tech Law Review

13. Öman, S. (2018),*"Implementing Data Protection in Law",* Stockholm Institute for Scandinavian Law 1957-2010

14. Repucci, S. (2012),*"Civil Service Reform: A Review",* United Nations University (UNU)- World Institute for Development Economics Research (WIDER)

15. Siasiakos, K. – Dimoula, E.E. (2019),*"The crucial role and the contribution of the Data Protection Officer (DPO) to the fulfilment of the compliance with the GDPR",* Greek National Documentation Centre (in Greek)

16. Stute, D.J. (2015), *"Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD",* Michigan Journal of International Law. Available at:

https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1085&context=mjil (last accessed on 19th July 2020)

17. Van Alsenoy, B. (2016), *"Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation"*, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law

18. Van Der Sloot, B. (2014), *"Do Data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation",* International Data Privacy Law

WEBSITES AND PORTALS

1. Arstechnica portal. Available at: https://arstechnica.com (last accessed on 19th July 2020)

2. Citizen's guide portal. Available at: http://www.odigostoupoliti.eu/(last accessed on 19th July 2020)

3. Data Guidance portal. Available at: https://platform.dataguidance.com(last accessed on 19th July 2020)

4. Data Protection Commission (Ireland). Available at: https://www.dataprotection.ie/ (last accessed on 19th July 2020)

5. Democracy Index page. Available at: https://www.eiu.com/topic/democracy-index(last accessed on 19th July 2020)

6. DIAVGEIA portal. Available at: https://diavgeia.gov.gr(last accessed on 19th July 2020)

7. Ecopress portal. Available at: https://ecopress.gr/(in Greek) (last accessed on 19th July 2020)

8. ENISA portal. Available at: https://www.enisa.europa.eu/ (last accessed on 19th July 2020)

9. European Data Protection Board (EDPB) portal. Available at: https://edpb.europa.eu (last accessed on 19th July 2020)

10. European Data Protection Supervisor (EDPS) portal. Available at: https://edps.europa.eu/ (last accessed on 19th July 2020)

11. Euronews portal. Available at: https://gr.euronews.com/(last accessed on 19th July 2020)

12. European Commission portal. Available at: https://ec.europa.eu/(last accessed on 19th July 2020)

13. European Parliament portal. Available at: https://www.europarl.europa.eu/portal/en (last accessed on 19th July 2020)

14. European Union Agency For Fundamental Rights portal. Available at: https://fra.europa.eu/(last accessed on 19th July 2020)

15. European Union Law. Available at: https://eur-lex.europa.eu/homepage.html?locale=en(last accessed on 19th July 2020)

16. Europrivacy portal. Available at: https://europrivacy.info/ (last accessed on 19th July 2020)

17. GDPR Legislation. Available at: https://gdpr-info.eu (last accessed on 19th July 2020)

18. Government at a Glance page. Available at: https://www.oecd.org/gov/govataglance.htm(last accessed on 19th July 2020)

19. Hellenic DPA portal. Available at: https://www.dpa.gr(last accessed on 19th July 2020)

20. Hellenic Informatics Union (HIU) portal. Available at: https://www.epe.org.gr/(last accessed on 19th July 2020)

21. IAPP (International Association of Privacy Professionals) portal. Available at: https://iapp.org/news/(last accessed on 19th July 2020)

22. IDPC (Maltese DPA) portal. Available at: https://idpc.org.mt/en/(last accessed on 19th July2020)

23. In.gr Greek portal. Available at: www.in.gr(last accessed on 19th July 2020)

24. Information Commissioner's Office portal. Available at: https://ico.org.uk/ (last accessed on 19th July 2020)

25. OECD portal. Available at: https://www.oecd.org (last accessed on 19th July 2020)

26. Police Officers of Thessaloniki Association portal. Available at: https://www.eaythes.gr/ (last accessed on 19th July 2020)

27. Privacy affairs portal. Available at: https://www.privacyaffairs.com/gdpr-fines/(last accessed on 19th July 2020)

28. Publications Office of the European Union portal. Available at: https://op.europa.eu/en/

29. Quality of Government page. Available at: https://qog.pol.gu.se/(last accessed on 19th July 2020)

30. Simply business British site. Available at: https://www.simplybusiness.co.uk/(last accessed on 19th July 2020)

31. Skills panorama website powered by Cedefop. Available at:https://skillspanorama.cedefop.europa.eu/en/(last accessed on 19th July 2020)

32. The Post and Courier (daily newspaper in South Carolina, USA) portal. Available at: http://www.postandcourier.com/(last accessed on 19th July 2020)

33. Sigmaweb portal. Available at: http://www.sigmaweb.org(last accessed on 19th July 2020)

34. U.S Government Publishing Office portal. Available at: https://www.govinfo.gov (last accessed on 19th July 2020)

35. UN portal. Available at: www.un.org

36. United Nations Development Programme portal. Available at: www.undp.org

PICTURES & TABLES

1. Picture 1 - Grammenos, D. – Strataki, A. Stefadouros, N.- Toris, M. (2020), *"GDPR and 40 thieves"*, CRETE UNIVERSITY PRESS

2. Table 20 - Bouckaert, L. & Victor, L. (2001),*"Pride and Performance in the Civil service: the Flemish case",* International Review of Administrative Sciences

ANNEX I

CHECKLIST / GUIDE TO GDPR FOR ORGANIZATIONS ACCORDING TO INFORMATION COMMISSIONER'S OFFICE (UK)

Lawfulness

☐We have identified an appropriate lawful basis (or bases) for our processing

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data

☐We don't do anything generally unlawful with personal data

Fairness

☐We have considered how the processing may affect the individuals concerned and can justify any adverse impact.

☐We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐We do not deceive or mislead people when we collect their personal data.

Transparency

☐We are open and honest, and comply with the transparency obligations of the right to be informed

Purpose limitation

☐We have clearly identified our purpose or purposes for processing

☐We have documented those purposes

☐We include details of our purposes in our privacy information for individuals

☐We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals

☐If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose

Data minimization

☐We only collect personal data we actually need for our specified purposes

☐We have sufficient personal data to properly fulfill those purposes

☐We periodically review the data we hold, and delete anything we don't need

Accuracy

☐We ensure the accuracy of any personal data we create

☐We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data

☐We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary

☐If we need to keep a record of a mistake, we clearly identify it as a mistake

☐Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts

☐We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data

☐As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data

Storage limitation (without prejudice to article 17 of the GDPR)[145]

☐We know what personal data we hold and why we need it

☐We carefully consider and can justify how long we keep personal data

☐We have a policy with standard retention periods where possible, in line with documentation obligations

☐We regularly review our information and erase or anonymize personal data when we no longer need it

☐We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'

☐We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes

Integrity and Confidentiality (Security)

[145]**A/N**: It should be noted that "the right to be forgotten" which appears in Article 17 and in Recitals 65 and 66 of the GDPR will play a smaller role in the public sector, compared to other sectors. This is mainly a consequence of the grounds that the GDPR provides for when the 'right to be forgotten' is not applicable, according to article 17 par. 3 of the GDPR : in case the processing takes place for the performance of a public interest task or exercise of official authority, or the processing is executed for compliance with a Union or Member State legal obligation, for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) or for the establishment, exercise or defence of legal claims, the right to be forgotten is not applicable. The abovementioned types of processing occur relatively often within the public sector.

☐ have an information security policy and ensure that is implemented

☐ ensure that regular controls are in place and ready to be enforced

☐ perform an analysis of the risks caused by our processing, and use this to assess the appropriate level of security we need to establish in the organization

☐when deciding what measures are applicable, we take account of the state of the art and costs for the proper implementation of the GDPR

☐ put in place basic technical controls

☐ regularly review our information security policies and measures and update them

☐ use encryption and/or pseudonymization whenever it is necessary

☐ comprehend the requirements of confidentiality, integrity and availability for the personal data we process.

☐ verify that we can restore access to personal data in the event of an "accident", such as by establishing an appropriate backup process.

☐ conduct regular testing and review our measures in order to ascertain that they remain effective and efficient

☐where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism

☐ ensure that any data processor we use, also implements the corresponding technical and organizational measures

Accountability

☐assume responsibility for complying with the GDPR, at the highest management level and throughout our public entity

☐ keep evidence of the steps we take in order to comply with the GDPR

- Establish appropriate technical and organizational measures, such as:

☐adopting and applying data protection policies

☐ following a 'data protection by design and default' approach - putting proper data protection measures in place throughout the entire lifecycle of our processing operations

☐concluding written contracts with other entities, which process personal data on our behalf

☐ keeping documentation of our processing activities

☐ implementing appropriate security measures

☐recording and reporting personal data infringements

☐ carrying out DPIAs for uses of personal data that are likely to result in high risk to the citizens' interests

☐ appointing a DPO

☐ adhering to codes of conduct and signing up to certification schemes (when possible)

☐ review and update our accountability measures from time to time

ANNEX II

QUESTIONNAIRE

A. AGE (116 responses)

AGE	RESPONSES (in absolute figures)	%
18-35 years old	24	20,7
36-50 years old	82	70,7
51-67 years old	8	6,9
I prefer not to say my age	2	1,7

B. GENDER (116 responses)

GENDER	RESPONSES(in absolute figures)	%
Male	52	44,8
Female	64	55,2
I prefer not to say my gender	0	0

C. EDUCATION (116 responses)

LEVEL	RESPONSES (in absolute figures)	%
Holder of a Doctoral Degree	2	1,7
Holder of a Master's Degree	56	48,3
Holder of a University Degree or TEI Degree	54	46,6
Post- Secondary Institute of Vocational Education	2	1,7
Lyceum graduate	2	1,7
High School graduate	0	0
Primary Scholl graduate	0	0

D. EMPLOYEE OF THE PUBLIC SECTOR AS: (116 responses)

FORM OF EMPLOYMENT	RESPONSES (in absolute figures)	%
Permanent staff	24	20,7
Under open- ended contract	8	6,9
Under fixed- term contract	32	27,6
Other form of employment	52	44,8

E. YEARS OF PROFESSIONAL EXPERIENCE IN THE PUBLIC SECTOR/ NUMBER OF YEARS (116 responses)

NUMBER OF YEARS	RESPONSES (in absolute figures)	%
0-5	66	56,9
6-20	40	34,5
21-35	10	8,6
36+	0	0

1. Has your Employer- Public institution performed a GDPR gap analysis in order to assess the extent of its compliance with the GDPR? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	38	32,8
NO	12	10,3
DON'T KNOW/ NO OPINION	66	56,9

2. Were officers in charge mandated to plan their operational actions in order to ensure the Organization's compliance with the GDPR, under a precise timetable? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	30	25,9
NO	22	19,0
DON'T KNOW/ NO OPINION	64	55,2

3. Have you been informed and trained on the implementation of the GDPR, the obligations of your Organization and the respective citizens' rights? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	34	29,3
NO	74	63,8
DON'T KNOW/ NO OPINION	8	6,9

4. If the answer to question number 3 is AFFIRMATIVE, in your opinion, which is the level of your knowledge and understanding of the matters concerning the application of the GDPR, the obligations of your Organization and the respective citizens' rights? (1 corresponds to the lowest level of knowledge and understanding – 10 corresponds to the upper level of knowledge and understanding). If your answer to question number 3 was NEGATIVE, then it is not required to answer the present question, without precluding the submission of a reply (58 responses)

ANSWERS	1 (lowest)	2	3	4	5	6	7	8	9	10 (highest)
NUMBER OF RESPONSES	4	8	6	2	12	4	12	10	0	0
%	6,9	13,8	10,3	3,4	20,7	6,9	20,7	17,2	0	0

5. Do you think that you need further training/ information on matters concerning the application of the GDPR? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	112	96,6
NO	2	1,7
DON'T KNOW/ NO OPINION	2	1,7

6. If the answer to question number 5 is AFFIRMATIVE, how urgent is the provision of further training/ information on matters concerning the application of the GDPR? (1 corresponds to the lesser urgent need for training– 10 corresponds to the most urgent need for training). Even if you answered "YES" to question number 5, you may submit your answer or proceed to the next question (110 responses)

ANSWERS	1 (lesser urgent)	2	3	4	5	6	7	8	9	10 (most urgent)
NUMBER OF RESPONSES	0	2	4	4	10	6	20	28	16	20
%	0	1,8	3,6	3,6	9,1	5,5	18,2	25,5	14,5	18,2

7. How important for the correct implementation of the GDPR do you consider the citizen's summarized and comprehensible information, with regard to the way his/her submitted personal data shall be processed? (Select 1 if you consider it totally unimportant, 10 if you consider it totally fundamental. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	2	2	10	0	10	24	18	46	4
%	0	0	1,7	1,7	8,6	0	8,6	20,7	15,5	39,7	3,4

8. Has a DPO (Data Protection Officer) been appointed by your Organization? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	14	12,1
NO	52	44,8
DON'T KNOW/ NO OPINION	50	43,1

9. If the answer to question number 8 is AFFIRMATIVE (a DPO has been appointed by your Organization), does he/she monitor the Service's compliance with the GDPR as well as with all relevant legal provisions in the field of protection of personal data? (If your answer to question number 8 was not YES, you may skip the present question) (34 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	6	17,6
NO	0	0
DON'T KNOW/ NO OPINION	28	82,4

10. If the answer to question number 9 is AFFIRMATIVE, to what extent does the DPO monitor the compliance with the GDPR? If your answer to question number 9 was NO or in case the question was not replied, you may skip the present question (24 responses)

ANSWERS	RESPONSES (in absolute figures)	%
On a daily basis		
Whenever requested by the Organization	2	8,3
Once a week		
On a monthly basis		
3 times a year		
On a yearly basis	2	8,3
Never		
DON'T KNOW/ NO OPINION	20	83,3

11. If the answer to question number 8 is AFFIRMATIVE (a DPO has been appointed by your Organization), does he / she inform and consult the Organization as well as its employees regarding their obligations arising from the GDPR and the other relevant legal provisions in the field of protection of personal data? If the answer to question number 8 was not YES, you may skip the present question (26 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	8	30,8
NO	6	23,1
DON'T KNOW/ NO OPINION	12	46,2

12. Is there an auxiliary group of employees that provides the DPO with the necessary support for the implementation of his tasks? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	8	6,9
NO	44	37,9
DON'T KNOW/ NO OPINION	64	55,2

13. Has your Organization introduced additional specific fields in its transactions with the citizens before any submission of personal data, in order to inform the public precisely about the purpose of collecting and processing personal data? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	24	20,7
NO	46	39,7
DON'T KNOW/ NO OPINION	46	39,7

14. How important for the correct implementation of the GDPR do you consider the EXCLUSIVE use of the absolutely adequate, relevant and limited to the minimum necessary data, just for the purposes for which they are processed? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	2	0	8	4	10	26	6	52	6
%	1,7	0	1,7	0	6,9	3,4	8,6	22,4	5,2	44,8	5,2

15. How important for the correct implementation of the GDPR do you consider the collection of data for specified, explicit and legitimate purposes and the fact they shall not be further processed in a way incompatible with those purposes? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW/ NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	0	4	2	2	8	20	20	52	8
%	0	0	0	3,4	1,7	1,7	6,9	17,2	17,2	44,8	6,9

16. How important for the correct implementation of the GDPR do you consider the retention of data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or processed? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW/ NO OPINION) (116 responses)

ANSWERS	1 (totally not important)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW / NO OPINION
NUMBER OF RESPONSES	0	0	2	0	10	6	14	18	24	38	4
%	0	0	1,7	0	8,6	5,2	12,1	15,5	20,7	32,8	3,4

17. Does the access to individual offices, PCs and management systems of the Organization take place according to each officer's particular role (role-based access control/ RBAC) in the Public Institution? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	68	58,6
NO	34	29,3
DON'T KNOW/ NO OPINION	14	12,1

18. Are the servers and computers in your working environment protected with updated antivirus software? (116 responses)

ANSWERS	RESPONSES(in absolute figures)	%
YES	46	39,7
NO	28	24,1
DON'T KNOW/ NO OPINION	42	36,2

19. Is your computer set to lock screen automatically after 5 minutes of inactivity in combination with a password encryption and storage? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	64	55,2
NO	38	32,8
DON'T KNOW/ NO OPINION	14	12,1

20. Is your office equipped with file cabinets and lockable drawers, in order to keep your physical data files inaccessible? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	88	75,9
NO	28	24,1
DON'T KNOW/ NO OPINION	0	0

21. Do you have a paper shredder in your working environment? (116 responses)

ANSWERS	RESPONSES(in absolute figures)	%
YES	48	41,4
NO	64	55,2
DON'T KNOW/ NO OPINION	4	3,4

22. How well informed is the general public concerning the application of the GDPR? (Select 1 if it is totally uninformed and 10 if it is fully aware of the issues arising from the application of the GDPR. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (not at all)	2	3	4	5	6	7	8	9	10 (fully aware)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	22	34	8	6	14	2	0	0	0	0	30
%	19	29,3	6,9	5,2	12,1	1,7	0	0	0	0	25,9

23. To what extent has the GDPR affected your relationship with the general public, in terms of provision of services to the citizens? (Select 1 if the GDPR hasn't affected at all your relationship with the general public or 10 if it has affected your relationship at the highest level. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (no affection)	2	3	4	5	6	7	8	9	10 (highest level of affection)	DON'T KNOW / NO OPINION
NUMBER OF RESPONSES	22	10	14	8	18	8	8	2	2	2	22
%	19	8,6	12,1	6,9	15,5	6,9	6,9	1,7	1,7	1,7	19

24. Were the citizens' patterns of behavior towards the Organization modified due to the application of the GDPR, and if so, to what extent? (Select 1 if the citizens' patterns of behavior were not modified at all and 10 if they were modified at the highest level. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (not at all)	2	3	4	5	6	7	8	9	10 (at the highest level)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	40	8	4	4	10	8	0	0	0	0	42
%	34,5	6,9	3,4	3,4	8,6	6,9	0	0	0	0	36,2

25. Have you signed a non- disclosure agreement (NDA) concerning the protection of citizens' personal data? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	30	25,9
NO	74	63,8
DON'T KNOW/ NO OPINION	12	10,3

26. How does your Organization take into account complaints regarding the processing and management of data? (There is also the option DON'T KNOW / NO OPINION. You may choose as many options as you have) (116 multiple responses)

ANSWERS	RESPONSES (in absolute figures)	Percentage %
In a written form (print format)	56	48,3
In a written form (electronic format)	30	25,9
Directly in person, clearing office for complaints	38	32,8
By e-mail	36	31,0
By telephone	38	32,8
By post- delivery (written notice)	22	19,0
In another way	10	8,6
DON'T KNOW/ NO OPINION	34	29,3

27. Does your Organization have mechanisms in place which effectively ensure the timely and lawful reporting of potential breaches to the competent supervisory authority? (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
YES	6	5,2
NO	32	27,6
DON'T KNOW/ NO OPINION	78	67,2

28. How important for the correct implementation of the GDPR do you consider the processing of data in such a manner as to guarantee their security and their protection against unlawful processing, accidental loss, destruction or alteration? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (not important)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	0	0	4	4	10	14	14	64	6
%	0	0	0	0	3,4	3,4	8,6	12,1	12,1	55,2	5,2

29. How important for the correct implementation of the GDPR do you consider the imposition of liability on the Data controller and processor, in order to be able to demonstrate compliance with the GDPR before the competent supervisory authorities and courts? (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10 (very important)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	2	0	8	8	14	30	18	28	6
%	1,7	0	1,7	0	6,9	6,9	12,1	25,9	15,5	24,1	5,2

30. How important for the correct implementation of the GDPR do you consider the continuous compliance with the Regulation and the accurate retention and continuous updating of data, the adoption of appropriate measures for the immediate correction or deletion of any inaccurate personal data, in relation to the pursued objectives of the processing. (Select 1 if you consider it totally unimportant, 10 if you consider it of paramount importance. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (totally unimportant)	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	0	0	0	2	4	0	12	28	16	42	12
%	0	0	0	1,7	3,4	0	10,3	24,1	13,8	36,2	10,3

31. How do you judge the quality of the services provided by your Organization after the entry into force of the GDPR on May 2018? (Select 1 if the quality of the services is at the lowest possible level, select 5 if it remains at the same level and 10 if it has improved to the best extent possible. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1 (at the lowest level)	2	3	4	5 (at the same level)	6	7	8	9	10 (improved at the best extent)	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	4	10	2	8	48	6	4	8	0	4	22
%	3,4	8,6	1,7	6,9	41,4	5,2	3,4	6,9	0	3,4	19

32. How important do you consider the faithful implementation of the GDPR for the enhancement of the quality of the services provided to the general public by the Organization? (Select 1 if you consider it totally unimportant and 10 if you consider it absolutely fundamental. There is also the option DON'T KNOW / NO OPINION) (116 responses)

ANSWERS	1	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	8	4	4	0	12	2	20	26	16	18	6
%	6,9	3,4	3,4	0	10,3	1,7	17,2	22,4	13,8	15,5	5,2

33. How crucial do you consider the correct implementation of the GDPR for the application of the principle of good administration? (Select 1 if you consider the correct implementation of the GDPR totally irrelevant to the application of the principle of good administration and 10 if you consider it of the utmost importance) (116 responses)

ANSWERS	1 (totally irrelevant)	2	3	4	5	6	7	8	9	10	DON'T KNOW/ NO OPINION
NUMBER OF RESPONSES	2	0	6	6	8	10	22	24	16	22	0
%	1,7	0	5,2	5,2	6,9	8,6	19	20,7	13,8	19	0

34. Comparing Greece to other EU Member States, GDPR in the public sector is applicable (select one option): (116 responses)

ANSWERS	RESPONSES (in absolute figures)	%
With equal credibility	4	3,4
With more credibility	0	0
With much more credibility	0	0
With less credibility	34	29,3
With much less credibility	20	17,2
DON'T KNOW/ NO OPINION	58	50,0

35. Considering the subject of the correct implementation of the GDPR by the Greek Public Authorities, do you believe that it depends on (select as many options as you wish): (116 multiple responses)

ANSWERS	RESPONSES (in absolute figures)	%
The proper information/ training/ familiarization of the public servants with the assistance of GDPR experts	98	84,5
The consciousness and professionalism of the public servant concerned	74	63,8
The threat and imposition of severe disciplinary sanctions by the Organization in case of infringement of the Regulation's provisions	40	34,5
The mentality of the average Greek public servant	44	37,9
The complexity of the Organization's structure, systems and mechanisms	58	50
The proper computerization of the Organization	70	60,3
Another factor. Indicate it	0	0,0
DON'T KNOW / NO OPINION	2	1,7

36. Do you believe that the GDPR was adopted in order to serve, in particular, the interests of: (116 responses)

ANSWERS	NUMBER OF RESPONSES	%
Citizens	70	60,3
EU Member States	18	15,5
Businesses	12	10,3
DON'T KNOW/ NO OPINION	16	13,8