NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATION

BSc THESIS

Privacy in the post General Data Protection Regulation (GDPR) World

Marilda I. Dajko

Supervisor (or supervisors): **Dimitris Varoutas,** Associate Professor

ATHENS

SEPTEMBER 2021

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ιδιωτικότητα μετά το Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ)

Μαρίλντα Ι. Ντάικο

Επιβλέπων: **Δημήτρης Βαρουτάς,** Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2021

BSc THESIS

General Data Protection Regulation (GDPR)

Marilda I. Dajko

S.N.: 1115200900164

SUPERVISOR: **Dimitris Varoutas,** Associate Professor

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ιδιωτικότητα μετά τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ)

Μαρίλντα Ι. Ντάικο
Α.Μ.: 1115200900264

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Δημήτρης Βαρουτάς,** Αναπληρωτής Καθηγητής

ABSTRACT

This thesis seeks to analyze the motives that correlate to General Data Protection Regulation/ (GDPR 2016/679) one of the toughest privacy and security law in the world which passed by the European Union (EU) and took effect on May 25, 2018. The document's aspects, and the purpose is to provide useful information on how this journey started and what is the current state. The GDPR BSc Thesis was conducted as a result of high personal interest and has been written to fulfill the graduation requirements of the Bachelor studies degree. The thesis was undertaken during a quite challenging time of period, considering personal situation balancing the different aspects of which I undertook the last years while the EU's new data protection law affected many people's lives. My research question was formulated together with my supervisor, Mr. Dimitris Varoutas. I anticipated to address challenges such as "What is the GDPR? Why is this law important and what part/s of it apply to me? How is it affecting the different industries etc." which are concerns that most European or non-European citizens may have arisen. The purpose is to primarily provide useful information regarding this regulation, how did it all start, some key roles and responsibilities, the penalties and hopefully help you understand the people's data privacy rights as well as further analyze the impact of this regulation in different sectors up to today. Nonetheless, conducting an extensive investigation has allowed me to answer many of the mentioned identified questions. Please note that nothing on this document constitutes legal advice rather than creating awareness.

SUBJECT AREA: GDPR: General Data Protection Regulation

KEYWORDS: information privacy, information protection, data regulations, European data law, security, compliance

ΠΕΡΙΛΗΨΗ

Η συγκεκριμένη πτυχιακή εργασία επιδιώκει στην ανάλυση των πτυχών τα οποία σχετίζονται με τον νέο Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ/GDPR 2016/679) που αποτελεί την πιο σημαντική αλλαγή στην νομοθεσία για την προστασία των δεδομέων μετά την άμεση εφαρμογή του σε όλα τα Κράτη-Μέλη απο 25 Μαϊου 2018. Το πάρων έγγραφο αποσκοπεί στην παροχή χρήσιμων πληροφοριών αναφορικά με μια ιστορική αναδρομή απο την έναρξη της προστασίας των προσωπικών δεδομένων μέχρι την σημερινή κατάσταση του κανονισμού. Η διατριβή της πτυχιακής διεξήχθη ως αποτέλεσμα υψηλού προσωπικού ενδιαφέροντας και έχει πραγματοποιηθεί με βάση τις απαιτήσεις της ολοκλήρωσης των προπτυχιακών σπουδών μου. Η πτυχιακή εργασία εκπονήθηκε σε μια αρκετά δύσκολη περίοδο της προσωπικής μου κατάστασης, κατά την προσπάθεια εξισορρόπησης διαφόρων πτυχών των οποία ανέλαβα να αντιμετωπίσω κατά τα τελευταία χρόνια, ωστόσο, ο νέος νόμος της Ευρωπαϊκής Ένωσης (ΕΕ) για την προστασία των προσωπικών δεδομένων επηρέασε τη ζωή πολλών ανθρώπων και μου κίνησε μεγάλο ενδιαφέρον. Ως εκ τούτου, το συγκεκριμένο θέμα διατυπώθηκε κατόπιν συμφωνίας με τον επιβλέπων καθηγητή κ. Δημήτρη Βαρουτά. Αποσκοπώ να απαντηθούν μερικές βασικές ερωτήσεις και προκλήσεις όπως «Τι είναι ο ΓΝΠΔ; Γιατί είναι σημαντικός και ποια μέρη του εφαρμόζονται στις ζωές μας; Πώς επηρεάζει τις διάφορες βιομηχανίες και ποια η επιρροή σήμερα κλπ.» που αποτελούν ερωτήματα τα οποία απασχολούν αρκετούς Ευρωπαίους καθώς και άλλους πολίτες σε παγκόσμιο επίπεδο. Επιπλέον, τα θέματα τα οποία πρόκειται να αναλυθούν στην πτυχιακή εργασία είναι αρχικά η παροχή βασικών πληροφοριών αναφορικά με τον κανονισμό, πώς ξεκίνησαν όλα, ορισμένους βασικούς ρόλους καθώς και ευθύνες, τις κυρώσεις και ευελπιστώ να σας βοηθήσω να απαντηθούν πολλές απο τις ερωτήσεις που αναφέρθηκαν παραπάνω. Παρακαλώ, λάβετε υπόψη οτι το συγκεκριμένο έγγραφο δεν αποτελεί νομική συμβουλή, παρά μόνο αποσκοπεί στην δημιουργία ευαισθητοποίησης και ενημέρωσης περί του ζητήματος.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Γενικός Κανονισμός Προστασίας Δεδομένων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: προστασία δεδομένων προσωπικού χαρακτήρα, προστασία πληροφοριών, κανονισμός δεδομένων, Ευρωπαϊκός νόμος δεδομένων, ασφάλεια, συμμόρφωση

AKNOWLEDGMENTS

I would like to thank all the respondents; without that cooperation I would not have been able to conduct this analysis. Fortunately, Mr. Varoutas has provided an excellent guidance and support during this process, and they were always available and willing to answer my queries.

I hope you enjoy your reading.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

The General Data Protection Regulation (GDPR) BSc Thesis was conducted as a result of high personal interest and has been written to fulfill the graduation requirements of the Bachelor studies degree. The thesis was undertaken during a quite challenging time of period, considering personal situation balancing the different aspects of which I undertook the last years while the EU's new data protection law affected many people's lives. My research question was formulated together with my supervisor, Mr. Dimitris Varoutas. The research was quite challenging because I anticipated address challenges such as "What is the GDPR? Why is this law important? Wat parts of it apply to me? How is it affecting the different industries etc." which most European or non-European citizens may have faced or may be still facing. The purpose is to primarily provide useful information and help you understand the data subjects' privacy rights. Nonetheless, conducting an extensive investigation has allowed me to answer the identified questions. Fortunately, Mr. Varoutas has provided an excellent guidance and support during this process, and they were always available and willing to answer my queries. I would like to thank all the respondents; without that cooperation I would not have been able to conduct this analysis. It may be considered as a useful resource for those trying to understand how to achieve compliance following the General Data Protection Regulation. Despite this paper contains a general summary of the key data protection laws, it is not a legal advice. As the reader of this paper, you should tailor the principles included in this paper to your own unique context and legal framework, consulting with a lawyer for possible legal advice.

I hope you enjoy your reading.

1. INTRODUCTION

On May 25, 2018, a European privacy law took effect that sets a new global bar for privacy rights, security, and compliance.

The General Data Protection Regulation, or GDPR, is fundamentally about protecting and enabling the privacy rights of individuals. The GDPR establishes strict global detailed privacy requirements for companies and organizations for governing how you manage and protect personal data while respecting individual choice—no matter where data is sent, processed, or stored.

Europe's new data privacy and security law includes hundreds of pages worth of new requirements for organizations around the world. The GDPR is the toughest privacy and security law in the world. Even though, it was drafted and passed by the European Union (EU), it imposes obligations onto organizations globally, so long as they target or collect data related to people in the EU. This data protection regulation was put into effect on May 25, 2018. The GDPR will charge tough fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

The GDPR is considered as a very important and challenging journey for a company or organization that wants to achieve the privacy goals and an important step forward for clarifying and enabling individual privacy rights while it requires significant changes and effort by companies and organizations all over the world.

Some years after, there was identified a substantial progress in privacy protection. Although, there is still effort needed to comply the GDPR's principles such as small organizations, which often lack the resources to appoint a data protection expert to guide them through compliance may not have started this journey yet.

2. UNDERSTANDING GDPR

The General Data Protection Regulation (GDPR) is the European Union's new data protection and privacy law for all individual citizens of the EU and the European Economic Area (EEA), which has been in effect since 1995 and adopted in April 2016 and went into effect on May 25, 2018. The GDPR sets out some detailed requirements for companies and organizations on the way of collecting, storing, and managing personal data. GDPR applies both to European organizations that process personal data of individuals in the EU, and to organizations outside the EU that target people living in the EU [1]. Therefore, the aim of the GDPR is to protect all EU citizens from privacy and confidential data exposes in today's data-driven world.

The GDPR is considered as the toughest privacy and security law worldwide. Even if it was drafted and passed by the EU, it imposes obligations onto organizations in global level, in case they target or collect data related to people in the EU. This regulation levies harsh fines [2] against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Europe marks with GDPR, its firm stance on privacy and data security a time when most people trust their personal data in cloud services and data breaches are constantly increasing. The regulation is considered large and extensive and very light in some specifics, making compliance with the GDPR a particularly difficult prospect, especially for small and medium-sized enterprises (SMEs).

2.1 How data protection started

The EU's data protection laws have long been regarded as a gold standard all over the world. Over the last years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed.

The GDPR is Europe's new framework for data protection laws which replaced the previous 1995 data protection directive which, was adopted at a time when the internet was in its infancy. The new regulation started on 25 May 2018. However, who did it all start? In 2016, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years, which replaces the 1995 Data Protection Directive. The GDPR which was recognized as law across the EU Member States had two years deadline to ensure that it is fully implementable in their countries by May 2018. The timeline in Figure 1 contains key dates and events in the data protection reform process from the 12th century until today including the GDPR landing in EU.

Moreover, the timeline [3] contains highlights of some of the ways that the GDPR strengthens your right to data protection. GDPR replaced the Data Protection Directive, which has been in effect since 1995. While the GDPR preserves many of the principles established in the Directive, it is a much more ambitious law. Among its most notable changes, the GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, or analyze personal data. The GDPR also gives national regulators new powers to impose significant fines on organizations that breach the law. The GDPR superseded the Data Protection Directive and fully phased out the DPD and become national law for all EU Member States on May 25, 2018. The GDPR builds 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, citizens will have more control over their personal data and more recourse if personal data is misused, while data controllers and processers will be required to protect sensitive personal data by design. Finally, the GDPR offers a much simpler regulatory environment for businesses that collect or process EU citizens' and residents' personal data. Another view of the history of GDPR, of data protection, how this domain started and evolved over time is shown in the following the reproduced [3] Figure 1**Error! Reference source not found.**:

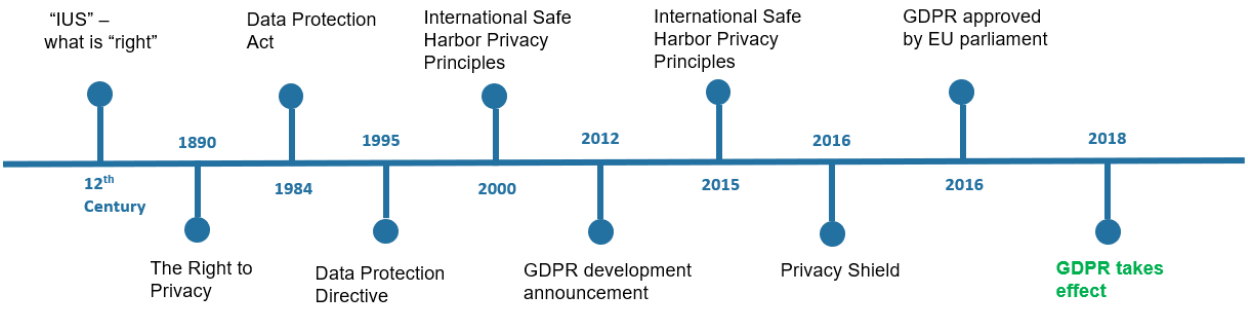

Figure 1: A brief history of how the data protection may started – Source: Sourcing International

"IUS" – 12th Century: The human rights concept towards "right to privacy" started by Decretum Gratiani in the 12th Century in Italy, when the Latin word "ius" was expanded from the concept "what is fair" to include "a right - an entitlement a person possesses to control or claim something," [4].

The Decretum Gratiani, also known as the Decretum, is a collection of canon law compiled and written in the 12th century as a legal textbook by the jurist Gratian. It is the first part of the collection of six legal texts, which became known as the Corpus Juris Canonici. The canonists of the Roman Catholic Church used the Decretum until the Decretals, promulgated by Pope Gregory IX in 1234, obtained legal force.

The Right to Privacy – 1890: Two United States lawyers, Samuel D. Warren and Louis Brandeis, wrote "The Right to Privacy" [5] an article that argues the "right to be left alone", using the phrase as a definition of privacy. The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals. Over 150 national constitutions mention the right to privacy.

Data Protection Act – 1984: The Data Protection Act (DPA) [6] is a United Kingdom Act of Parliament which was passed in 1988. Act was developed to control how personal, or customer information is used by organizations or government entities. It protects people and lays down rules about how data about people can be used.

Data Protection Directive – 1995: The Data Protection Directive [7], officially Directive 95/46/EC, passed in October 1995, is an EU directive which regulates the processing of personal data within the EU and the free movement of such data. The Data Protection Directive is an important component of EU privacy and human rights law. The principles set out in the Data Protection Directive are aimed at the protection of fundamental rights and freedoms in the processing of personal data. When GDPR was adopted in April 2016, it superseded the Data Protection Directive and became enforceable on 25 May 2018.

International “Safe Harbor” – 2000: or Safe Harbour Privacy Principles [8] were principles developed between 1998 and 2000 aiming prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information.

European Commission (EC) announces GDPR development – 2012: EC proposal to strengthen online privacy rights and digital economy and the European Commission proposes a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. EDPS opinion on EC data protection [9] reform package on which the European Data Protection Supervisor adopts an Opinion on the Commission's data protection reform package.

International Safe Harbor Privacy principles overturned – 2015: The International Safe Harbor Privacy Principles were overturned on October 6, 2015, by the European Court of Justice (ECJ), which enabled some US companies to comply with privacy laws protecting European Union and Swiss citizens. The European Commission and the United States agreed to establish a new framework for transatlantic data flows on 2 February 2016, known as the "EU–US Privacy Shield", which was closely followed by the Swiss-US Privacy Shield Framework.

Privacy Shield – 2016: an EU–US framework for regulating transatlantic exchanges of personal data for commercial purposes between the EU and the US. One of its purposes was to enable US companies to receive personal data more easily from EU entities under EU privacy laws for EU citizens [10]. The EU–US Privacy Shield replaced the International Safe Harbor Privacy Principles, which were declared invalid by the European Court of Justice in October 2015. In 2020 the ECJ declared the Privacy Shield invalid due to identified legal challenges.

GDPR is approved by EU parliament – 2016: The EU regulation 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). Therefore, the GDPR was approved.

GDPR takes effect – 2018: The GDPR has been a historic achievement for Europe and EU citizens for protecting individual regarding the processing of personal data, which has been a sensational achievement for Europe and its citizens, acting as a lighthouse for the entire global policy-making scene, and illuminating long-held privacy and data protection values enshrined across the horizon of the European legislative landscape. GDPR acted as a catalyst for many jurisdictions around the world to draft and implement their own privacy and data protection legislation. Even the most disillusioned ones would acknowledge that we now have more than 130 states with a data privacy law and several other jurisdictions with official Bills at various stages of development, compared to the roughly 80 data privacy laws when the legislator started to negotiate the GDPR.

2.2 GDPR overview

The GDPR establishes rules for organizations aiming the personal data protection in all its forms and changes the rules of consent and strengthens people’s privacy rights. Any

type of organization such as companies, charities, even small enterprises, that handles the personal information of EU citizens or residents is subject to the GDPR law.

The regulation establishes rules relating to the protection of natural persons about the processing of personal data and rules about exchanging personal data. It aims to protect fundamental rights and freedoms of natural persons and most important, their right to the protection of personal data. It is worth noting that the case of exchange or processing of personal data for the protection of natural persons will not be excluded from GDPR.

The GDPR applies to the company/entity:

- which is established outside the EU and is offering commodities/services or is collecting/ handle personal data of individuals in the EU, regardless of where the data is processed; or
- which is established outside the EU and is offering goods/services (paid or for free) or is monitoring the behavior of individuals in the EU.

Note: The GDPR and its official supporting documents do not give guidance for situations where processing affects EU individuals across multiple member states. Until this requirement is interpreted, it may be prudent to designate a representative in a member state that uses your language. Some organizations, like public bodies, are not required to appoint a representative in the EU.

The GDPR states in [11] the territorial scope of the law and 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.
- to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    - the monitoring of their behavior as far as their behavior takes place within the Union.
- to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The key GDPR check points are becoming aware and accountable, communicating with staff, considering personal privacy rights, access request change, lawful basis, consent, children and minors, breaches, the data protection impact assessments, taking into consideration the data protection officers and the international organisations. These areas will be analyzed reading through this document.

The GDPR covers all the European Union member states (as of 2019): Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. However, under certain conditions, the GDPR applies to companies that are not in Europe. That includes organizations not in the EU [12] but that offer goods or services to people there. If you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU. The European Union's General Data Protection Regulation is peculiar in the fact that it applies to organizations that may have little to do with the EU. If your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR.

If your company is a SME that processes personal data as described above, it must comply with the GDPR. However, if processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you such as appointing a Data Protection Officer (DPO). The core activities should include activities related to processing of data forms an inextricable part of the controller's or processor's activities.

The requirements essentially concentrate to two factors: secure people's data and make it easy for people to exercise control over their data. As GDPR aims to protect data belonging to EU citizens and residents, the law applies to organizations that handle such data whether they are EU-based organizations or not, known as "extra-territorial effect." The fines for violating the GDPR [13] are very high, so those who don't follow the rules can get hit with a fine of €20 million or 4 percent of global revenue, whichever is higher, plus compensation for damages. These sections, however, will be analyzed in more detail below. However, the GDPR explicitly states that one can lower the fines if efforts around data protection are comprehensively evident, constructive, and proactive.

Data subjects may also raise a claim for non-monetary loss and involve a syndicate to file an action on their behalf. Penalties out of those claims are not already covered by administrative fines and will come on top of the financial risk. The burden of proof of compliance with the GDPR lies entirely upon the offending data controller against whom a claim has been filed. It is up to the data controller to build a proper contractual framework with other service providers which process the data to make them liable for any state of noncompliance. Under the GDPR, fines are administered by the data protection regulator in each EU country. That authority will determine whether an infringement has occurred and the severity of the penalty. They will use 10 criteria to determine whether a fine will be assessed and in what amount which is going to be analyzed afterwards.

2.2.1 Key Definitions

The GDPR defines an array of legal terms [14] at length. For the purposes of this document, below are some of the most important definitions for GDPR terms used in this document:

Personal data: an information that relates to an individual who can be directly or indirectly identified. Specifically, any information relating to an identified or identifiable natural person or data subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data can include names, home address, work address, telephone number, mobile number, email address, passport number, National ID card, Social Security Number (or equivalent), driver’s license, physical – physiological or genetic information, medical information, cultural identity, bank details/account numbers, tax file numbers, work address, credit/debit card numbers, tax file number, work address, locations are obviously personal data. Additionally, social media posts, IP address (EU region), locations/GPS data, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions, administrative or criminal sanctions and genetic or biometric data, can also be personal sensitive data. There is no distinction between a person's private, public, or work roles.

Data subject: an identifiable natural person is one who can be identified, directly or indirectly. The person whose data is processed. For instance, your customers or site visitors.

Data controller: the legal person, public authority, agency, or other body which, alone or jointly with others, who determines the purposes and means of the processing of personal data. The controller decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Restriction of processing: marking of stored personal data with the aim of limiting their processing in the future.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Pseudonymous data: can also fall under the definition if it's relatively easy to ID someone from it.

Pseudonymisation: processing the personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Controller: a 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Data processor: a natural or legal person, public authority, agency, third party or other body, which processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers or email service providers.

Data processing: any action performed on data, whether automated or manual. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Consent: of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from an analysis of a biological sample from the natural person in question.

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Data concerning health: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Main establishments mean:

- as regards a **controller with establishments** in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

- as regards a **processor with establishments** in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

Representative: a natural or legal person established in the Union who, designated by the controller or processor represents the controller or processor with regard to their respective obligations under this Regulation.

Enterprise: a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Relevant and reasoned objection: an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

International organization: an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

The official GDPR.eu website provides the full all Articles and Recitals of the Regulation, as well as helpful guides and checklists that walk you through how the Regulation may apply to you. However, based on the Regulation of the (EU) 2016/679 (General Data Protection Regulation) of the European parliament and of the council of in the current version, we will be able to refer to some of these articles each article in detail in this thesis.

The GDPR gives rights to people to manage personal data collected by an organization. These rights can be exercised through a Data Subject Request (DSR). The organization is required to provide timely information regarding DSRs and data breaches and perform Data Protection Impact Assessments (DPIAs).

Several points should be considered when implementing or assessing GDPR requirements:

- Developing or evaluating your GDPR-compliance data privacy policy.
- Assessing the data security of your organization.
- Who is your data controller?
- What data security processes may you have to perform?

2.2.2 Data Protection Principles

The Article 5 of the GDPR imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with seven key principles that summarize its many requirements. If you process data, you must do so according to seven protection and accountability principles outlined in the relevant the regulation. Therefore, the essential protection and accountability principles guiding the regulation are the below:

1. **Lawfulness, fairness, and transparency** on handling and using personal data while processing lawfully, fairly and with transparency. You should have a good reason and need to be clear with the data subjects about how you are using personal their data and need a “lawful basis” to process that data.
2. **Purpose limitation** on processing personal data for the legitimate purposes specified explicitly to the data subject when you collected it. You do not need to reuse or disclose personal data for any other purpose rather than that for which the data was originally collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes.

3. **Data minimisation** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. while you should collect, process and storage only as much data as necessary for the purposes intended.

4. **Accuracy** on the collected personal data which require updating where necessary. In case of inaccuracy, reasonable steps must be taken to ensure that personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay allowing individuals to correct or request deletion of their personal data. It is necessary to ensure that the personal data kept is accurate and that it can be corrected in case of errors.
5. **Storage limitation** of personally identifiable data for only as long as necessary for its intended purpose. You need to ensure that you retain personal data only for as long as necessary to achieve the purposes for which the data was collected.

6. **Integrity and confidentiality** ensuring personal data is protected using appropriate security, integrity, and confidentiality practices (e.g. by using encryption). Your organization need to keep personal data secure through technical and organizational security measures.
7. **Accountability** as the data controller is responsible for being able to demonstrate GDPR compliance following these principles. According to GDPR the data controllers must be able to demonstrate they are GDPR compliant, which cannot happen after the fact.

Thinking that you are compliant with the GDPR but cannot show how, then you are not GDPR compliant. Among the more proactive ways you can do the following:

- Designate data protection responsibilities to your team.
- Maintain detailed documentation of what data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- Train your staff and implement technical and organizational security measures.
- Establish Data Processing Agreement contracts in place with third parties you contract to process data for you.
- Appoint a Data Protection Officer, though not all organizations need one.

2.2.3 People's Privacy Rights

According to GDPR data subjects must be informed of their privacy rights, (Chapter 3) including their right to revoke consent to data processing at any time, their right to view their personal data and access an overview of how it is being processed, their right to obtain a portable copy of the stored data, their right to erasure of their data under certain circumstances, their right to contest any automated decision-making that was made on a solely algorithmic basis, and their right to file complaints with a Data Protection Authority. As such, the data subject must also be provided with contact details for the data controller and their designated data protection officer, where applicable.

Chapter 3 of the GDPR lays out the data privacy rights and principles that all "natural persons" are guaranteed under EU law. As an organization, you are obligated to facilitate these rights. Failure to comply will result in penalties. A very basic summary is shown in reproduced [2] Figure 2 below there is an analysis on each the data subject's rights under GDPR's Chapter 3.

1. **Right to be informed:** Data subjects have to be informed, whether their data have been processed and if so, what's the purpose each time their data is collected or processed.
2. **Right to access:** Data subjects have the right to know certain information about the processing activities of a data controller. This information could be the source of their personal data, the purpose of processing, and the length of time the data will be held.
3. **Right to rectification:** The accuracy of processed data is part of privacy; however, people have a right to correct inaccurate or incomplete personal data that are being processed.
4. **Rights to erasure:** or "right to be forgotten," data subjects have the right to request that you delete any information about them that you have. There are five exemptions to this right, including when processing their data is necessary to exercise your right to freedom of expression. You must make it simple for data subjects to file right to erasure requests. You can find a template for such requests here.
5. **Right to restrict processing:** In case you are not asked to erase their data, the data subjects can request that you temporarily change the way you process their data (e.g., removing it temporarily from your website) if they believe the information is inaccurate, is being used illegally, or is no longer needed by the controller for the purposes claimed. The data subject has the right to simply object to your processing of their data as well. Additionally, if you decide to take any additional action, then it requires you to notify the data subject.
6. **Right to data portability:** store the data subjects' personal data in a format that can be easily shared with others and understood. Moreover, if someone asks you to send their data to a designated third party, you must do it (if technically feasible), even if it's one of your competitors.
7. **Right to object:** Data subjects have the right to object to you processing their data. You can only override their objection by demonstrating the legitimate basis for using their data.

   Therefore, individuals have the right to know what, why, what personal data is held by Data Controllers. Additionally, they have the right to access their won data and any related right regarding the processing of their personal data.

Figure 2: Understanding the GDPR data subject rights – Source: gdpr.eu

2.2.4 The role of the Data Controller

According to EU GDPR the key decision-maker role is the Data Controller [15], while determines the why and how personal data will be processed. A data controller could be either a private company - legal entity or an individual person or employee in the organization. Many companies use third parties, like email or cloud storage services, to handle their data. In case the third party has higher technological capacity, this can help with GDPR however, it does not absolve the hiring organization (i.e., the controller) from ensuring that personal data is processed in accordance with the GDPR. Unless the controller can clearly demonstrate that it was “not in any way responsible for the event giving rise to the damage,” it will be fully liable for any infringement caused by a non-compliant third party. For this reason, it is important to carefully vet any third-party services you use to make sure they have a good track record for security.

An EU GDPR checklist [16] is provided to the data controller, although to understand it is also important to know some of the terminology and the basic structure of the GDPR

law. The data controller needs to follow GDPR compliance requirements by establishing an information audit about personal data to be able to answer questions concerning “who, what and how”. Organizations require to keep detailed and updated list for the following:

- the purposes of the processing;
- what type of data are processed;
- who has access to these data
- any third parties (and where they are located) that have access
- what you're doing to protect the data (e.g., encryption), and
- when you plan to erase it (if possible).
- data processing activities and be well prepared to report it to regulators upon request by conducting a privacy impact assessment (PIA)

A legal justification is also required for data processing activities following the GDPR conditions such as provisions related to children and special categories. If you choose "consent" as your lawful basis, there are extra obligations, including giving data subjects the ongoing opportunity to revoke consent. If "legitimate interests" is your lawful basis, you must be able to demonstrate you have conducted a PIA. The data controllers, requires providing clear information and legal justification about data processing in the organization’s privacy policy informing data subjects accordingly: how the data is processed, who has access to it, and how you're keeping it safe. This information should be included in your privacy policy and provided to data subjects at the time you collect their data. It must be presented "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

Data protection should be following the principles of "data protection by design and by default," including implementing "appropriate technical and organizational measures" Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data that are no longer needed. Encrypt, pseudonymize whenever feasible, or anonymize personal data wherever possible as nowadays the productivity tools used by businesses are available with end-to-end encryption built in, including email, messaging, notes, and cloud storage. The data controller needs to create an internal security policy their team

members to and build awareness for both technical and operational security about data protection. The team members need to knowledgeable about data security following guidance about email security, passwords, two-factor authentication, device encryption, and VPNs. Employees who have access to personal data and non-technical employees should receive extra training in the requirements of the GDPR. An additional process is required for notifying the authorities and data subjects in a data breach event because if personal data is exposed, you are required to notify the supervisory authority which is stated by the EU members, in your jurisdiction within 72 hours.

The data controller requires to assign a person who will take GDPR compliance accountabilities, who will evaluate data protection policies and the implementation of those policies. Sign a data processing agreement between your organization and any third parties for third-party services that handle the personal data of your data subjects, including analytics software, email services, cloud servers, etc. Most services have a standard data processing agreement available on their websites spelling out the rights and obligations of each party for GDPR compliance. In case the organization is outside the EU, then representative within one of the EU member states is needed especially in case of processing data relating to people in one member state, then it is required to appoint a representative in that country who can communicate on your behalf with data protection authorities. The data controller will appoint a DPO if necessary, as the DPO should be an expert on data protection such as monitoring the GDPR compliance, assess data protection risks, advise on data protection impact assessments, and cooperate with regulators.

Under GDPR the data subjects have rights related to their personal data. Following these rights, upon request, the data controller, has to send them the first copy of this information for free but can charge a reasonable fee for subsequent copies. Identity verification is needed while there is an SLA of complying within a month. If the data subject requests for data correction or update, a data quality process will be required for keeping accuracy and completeness. Again, an identity verification is required. The SLA for the data the person requesting the data. You should be able to comply with requests under GDPR is within a month. In case of receiving a request of personal data deletion, which has to be done within a month after the identity verification. Denial of the deletion can be within exercise of freedom of speech or compliance with a legal obligation. If the data subjects’ requests to restrict or stop processing of their data if certain grounds apply, mainly if there's some dispute about the lawfulness of the processing or the

accuracy of the data. It is required to honor their request within about a month. While processing is restricted, it is still allowed to keep storing their data however, the data subject has to be notified before beginning processing their data again. In case the data subject requests for providing a copy of their personal data, this should be addressed by providing in a commonly readable format (e.g. a spreadsheet) either to them or to a third party they designate. While it may seem unfair from a business standpoint in that you may have to turn over your customers' data to a competitor, however, from privacy standpoint, people own their personal data. Additionally, in case of objection of processing personal data, if this is being done for direct marketing purposes, the process should immediately stop.

Therefore, summarizing the data controllers' responsibilities below:

- **Comply with the GDPR**: adopt appropriate measures which implement the data protection principles to comply to the data protection by design and by default.
- **Demonstrate compliance:** or otherwise, prove compliance by following the GDPR documentations that proves the measures you have in place to comply with the regulation, their effectiveness as well as who they are reviewed and updated.
- **Assing a DPO:** if needed provide sufficient guarantees related to the technical and organizational measures as required by the GDPR. Establish a written contract
- **Record the processing activities**: to maintain an internal documentation that demonstrates how and why personal data is being processed.
- **Cooperate with the Supervisory Authority:** with performance of its tasks as of GDPR guidance.
- **Secure the processing:** following the GDPR points set when implementing the GDPR measures that ensure a level of security managing the relevant risks.
- **Personal data breach notification**: in case a data breach occurs, notify the Supervisory Authority within 72hours after becoming aware unless the breach does not risk the rights and freedoms of the data subject.
- **Personal data breach communication**: in case a data breach occurs and is likely to result in a high risk to rights and freedom of the data subject, then the natural person has to be notified without undue delay.

- **Data protection impact assessment:** carry out one when the processing is likely to result in high risk to the rights and freedom or in compliance with codes of conduct or seeking the view of data subjects.

Finally, I would like to remind you once again that the above checklist is by no means a legal advice. You can consult a legal representative to make sure your organization complies with the GDPR.

2.2.5 The role of the Data Protection Officer

The primary responsibility of the DPO [17] is to ensure that their organization processes the personal data of its staff, customers, providers, or any other individuals (i.e., data subjects) in compliance with the applicable data protection rules. In the EU institutions and bodies, the applicable GDPR obliges them each to appoint a DPO. The DPO is responsible to ensure that all personal data are collected, processed, and stored are compliant to the appropriate data protection rules for all individuals, personnel, customers, or providers. This role requires highly skilled, experienced, and specialized to data protection as well as understanding of the processes/ operations of the organization and fully guarantees compliance inside this body. In the EU institutions and bodies, there are several policies guaranteeing this independence:

1. The applicable rules for EU organizations and bodies expressly provide all the means for the total independency of the role of DPO.
2. No conflict of interest must exist between the duties of the individual as a DPO and other duties:
   - should not also be a controller of other activities (other role in the organization like HHR, Staff role) and should report directly to top management
   - should not be an employee on a short or fixed term contract
   - should not report to a direct superior rather than top management
   - should have financial independence/own budget
3. The DPO should be supported by other roles and resources like assistants and deputies as well as data protection coordinators (DPCs). The organization must offer staff and resources for supporting the DPO while access to resources also includes training facilities.

4. The DPO should have the authority to investigate which means access to all personal data and data processing operations; those in charge are also required to provide information in reply to the DPO's questions.
5. The DPO role is appointed to a certain time frame with minimum term of appointment and strict conditions for dismissal should be set out by the organization. DPO is appointed for a period between three and five years and can be replaced under strict rules of the EDPS. In the EU institution and bodies, the DPO must:
   - ✓ Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them
   - ✓ Provide advice and recommendations to the institution about the interpretation or application of the data protection rules
   - ✓ Create a register of processing operations within the institution and notify the EDPS those that present specific risks (so-called prior checks)
   - ✓ Ensure data protection compliance within her institution and help the latter to be accountable in this respect.
   - ✓ Handle queries or complaints on request by the institution, the controller, other person(s), or on own initiative.
   - ✓ Cooperate with EDPS and handle requests (queries or complaints) around data protection and personal data
   - ✓ Highlight and raise a risk (red flag) on any failure to comply with the data protection rules

Consequently, the GDPR EU articles the GDPR obligations can be divided into those that are placed on controllers and those that are mandatory for the processor. Summarizing some of the key GDPR requirements below:

- DPIA is required for high-risk personal data processing activities to identify risks and define mitigating actions.
- Data privacy accountabilities assigned to data controller who responsible for confirming that an organization adheres to the GDPR principles.
- Processing personal data condition must rely on a lawful basis as per GDPR.
- DPO must be assigned by following relevant qualifications, especially for organizations that conduct large-scale systematic monitoring of EU residents' data or process large amounts of sensitive personal data.

- Privacy by design is required to establish privacy controls from the outset of product or process development.
- Right to erasure as an individual can request the deletion or removal of personal data when there is no lawful reason for its continued processing.
- Consent must be freely given and explicit, indicating the individual's specific agreement to the processing of personal data.
- Data breach notification while a firm must notify the supervisory authority of a data breach within 72 hours of becoming aware of it.
- Secured data portability allowing individuals to move, copy or transfer personal data easily.

2.2.6 Fines

The fines for violating the GDPR [18] are very high. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

According to the GDPR, fines are managed by the data protection regulator in each EU country. That authority will determine if there has been an infringement and the severity of the penalty. The following 10 criteria will be used to decide if a fine will be assessed and in what amount:

Gravity and nature: The overall infringement's view. Questions-answers such: what, how, why happened, the number of people affected, the number and the extend of the damage they suffered, and how long it took to resolve.

Intention: whether the violation was intentional or the result of negligence.

Mitigation: if the organization has acted to mitigate the damage suffered by those affected by the infringement.

Precautionary measures: The amount previously invested by the company to comply with the GDPR for prior technical and organizational preparation.

History: Any relevant previous infringements, including infringements under the Data Protection Directive despite the GDPR, as well as compliance with previous administrative corrective actions under the GDPR.

Cooperation: Whether the organization cooperated with the supervisory authority to discover and correct immediately the infringement.

Data category: the kind of personal data is affected by the infringement.

Notification: Whether the company or a third party has been appointed, it has reported the breach to the supervisory authority.

Certification: Either the organization followed approved codes of conduct or was previously certified.

Aggravating/mitigating factors: Any other issues arising from the circumstances of the case, including the financial benefits gained or the losses avoided as a result of the infringement.

If it is determined by the regulators that an organization has multiple breaches of the GDPR, then the organization will be punished only for the most serious, provided that all breaches are part of the same processing process. Many companies use third parties, such as email or cloud storage services, to handle their data. While this may be helpful in complying with the GDPR if the third party has higher technological capacity, it does not relieve the recruiting body (i.e., the controller) of ensuring that personal data is processed in accordance with the GDPR. However, if the controller can clearly demonstrate that "he was in no way responsible for the incident that caused the damage", he will be fully responsible for any infringement caused by a non-compliant third party. For this reason, it is very important to carefully check all third party services to make sure they have good security record. The GDPR’s stiff fines are aimed at ensuring best practices for data security are too costly not to adopt. While it remains to be seen how fines will be applied by different EU member states, these fines loom for any organization not making strides to ensure GDPR compliance.

Infringements and fines need to be assessed by national authorities in accordance with the General Data Protection Regulation. The fines must be effective, proportionate, and dissuasive for each individual case. For the decision of whether and what level of penalty can be assessed, the authorities have a statutory catalogue of criteria which it must consider for their decision. Among other things, intentional infringement, a failure to take measures to mitigate the damage which occurred, or lack of collaboration with authorities can increase the penalties. For especially severe violations, listed in Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year,

whichever is higher. But even the catalogue of less severe violations in Art. 83(4) GDPR sets forth fines of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher. Especially important here, is that the term “undertaking” is equivalent to that used in Art. 101 and 102 of the Treaty on the Functioning of the European Union (TFEU). According to case law of the European Court of Justice, “the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed”. An undertaking can therefore not only consist of one individual company in the sense of a legal person, but also out of several natural persons or corporate entities. Thus, a whole group can be treated as one undertaking and its total worldwide annual turnover can be used to calculate the fine for a GDPR infringement of one of its companies. In addition, each Member State shall lay down rules on other penalties for infringements of the Regulation which are not already covered by Art. 83. Those are most likely criminal penalties for certain violations of the GDPR or penalties for infringements of national rules which were adopted based on flexibility clauses of the GDPR. The national penalties must also be effective, proportionate and act as a deterrent.

The GDPR’s stiff fines are aimed at ensuring best practices for data security are too costly not to adopt. The risks vary from causing reputation damages, 4% loss of income as well as regulatory enforcement. While it remains to be seen how fines will be applied by different EU member states, these fines loom for any organization not making strides to ensure GDPR compliance.

3. HOW GDPR IMPACTS DIFFERENT SECTORS

Since the General Data Protection Regulation (GDPR) was enforced on May 25, 2018, it pressed every business, private and public sector entity to effectively protect, process and store data related to EU residents. Thanks to GDPR, data subjects now have the right to allow or restrict businesses to access their personal data. Moreover, taking into consideration the right to be forgotten, individuals can demand permanent deletion or even erasure of their data. Any business that processes or handles EU citizens' data within EU states must adhere to GDPR even if they present in Europe.

As almost all businesses participate in the processing of personal data in one or more processes, all organizations across industries are obliged to adopt procedures, policies, and systems to become compliant with EU GDPR. Over the last years, GDPR has significantly impacted the industries globally, irrespective of region, size, and service offerings etc. The data relating to everything from financial records to medical and internet activity have been strictly impacted and the handling of these had to be changed. The whole engagement of the customers right down to tools used and how they are used had to be reshaped. Consequently, GDPR affected many different sectors so we will be tackling the top industries affected by GDPR, the challenges that they face since the regulation has come into effect, and the benefits they receive from this data privacy law. These industries are the following: technology including telcos and AI, education sectors, public sectors, financial services, retail and even health care industries. Obviously, there are more industries affected by the GDPR although due to personal interest in this document some of the key affected sectors will be covered only in this document.

3.1 Technology Sector

As technology institution [19] we often refer to the business of selling technology, an electronics-based technology, including business relating to digital electronics, software, and internet-related services, such as e-commerce services. The technology culture has changed a lot since GDPR went into effect on 25th May 2018, while many businesses in the tech sector have already been fined millions for GDPR breaches out of thousands reported cases in the years which are constantly increasing. The implications of GDPR on technology companies that provide software products and services are enormous. Most of the technology companies are compelled to revisit their business processes that deal with personally identifiable information (PII) - any data that can be used to identify a specific individual- and assess the level of compliance with GDPR.

The technology organizations are pressed to assess their technology platforms and data architecture including various information systems, websites, databases, data warehouses, and data processing platforms to meet the GDPR requirements. The GDPR was created to redress the imbalance of power between big tech and consumers, forcing big tech companies to be accountable for how they store and use data. Many tech businesses stepped in by organizing webinars and events relevant to GDPR topics in order to create awareness. Although, it is still unclear to many about the GDPR compliance limits, what does the regulation mean for their businesses or even how it has affected the larger tech industry where the main GDPR principals such as consent, transparency, accountability are still imprecise terms without a consistent reference for most of them. Moreover, those accessing the internet from within the EU, over the past years, there has been an onslaught of “click-through” windows for users to navigate to access sites never visited by them.

The EU internet users experience is affected too because as per user’s feedback while trying to visit some websites they use to receive pop up messages stating that that EU data laws prevent access to the content. According to Forbes, many other end users were unable to access sites in other countries with some reverting to VPN to be able to access those sites.

Another challenge faced by the tech companies under GDPR is the need to employ Data Protection Officers (DPOs) and respond to any data breach within the 72-hour window. In the meantime, the cloud providers and the remote service providers are trying to adopt stringent security measures, standards, and regulations within their organizations to protect and handle data subject or customer data to be able to remain compliant with GDPR.

The GDPR does not apply to individuals using social media for their own purposes, although, it applies to individuals acting as sole traders’ organizations who use social media for processing data such as posting personal data on a website, downloading, or even using personal data from a website. Some of the most famous online social media and social networking services, Facebook, and its companies, including Instagram, Oculus and WhatsApp, will all comply with the GDPR. GDPR made it harder for social media companies to collect customer information and behavior for systematic targeting and profiling. GDPR requires companies give consumers the ability to access, rectify, and remove their data. Marketers should familiarize themselves with their company's data storage policies and procedures, and identify who within the company to contact,

should an individual request access to their data. Social media marketing is one of the most affected industries by GDPR. The social media and online communities are pressed to fully disclose and make it clear to the users how their personal information is gathered and used. Moreover, the marketers are also obliged to receive full consent from the users to utilize their data.

3.1.1 GDPR 5G and IoT

The fifth-generation cellular network or “5G” as is formally defined by global standards agencies, is considered by many as the fourth industrial revolution. The 5G in telecommunications is the latest iteration for broadband mobile networks including a hybrid suite of technologies between Wi-Fi and cellular networks, machines, objects, and devices providing higher connectivity and download speeds to most current cellphones. It is a new global wireless standard after 1G, 2G, 3G and the 4G networks. Countries such as China, South Korea, Australia, Germany, the US, and UK have already embraced 5G. It is strongly believed that 5G will be widely available in the next years while experts expect at least 20 billion connected IoT devices by 2023 [20] as of MIT, representing millions of usually low-cost devices with long battery lives and low latency connectivity, which is required for critical applications such as traffic safety, remote surgery or accurate positioning for industrial uses. It is obvious that 5G is already considered as mature concept for different fields such as entertainment, manufacturing, health care, and retail.

5G is used across three main types [21] of connected services, including enhanced mobile broadband, mission-critical communications and massive IoT – reproduced [21] Figure 3

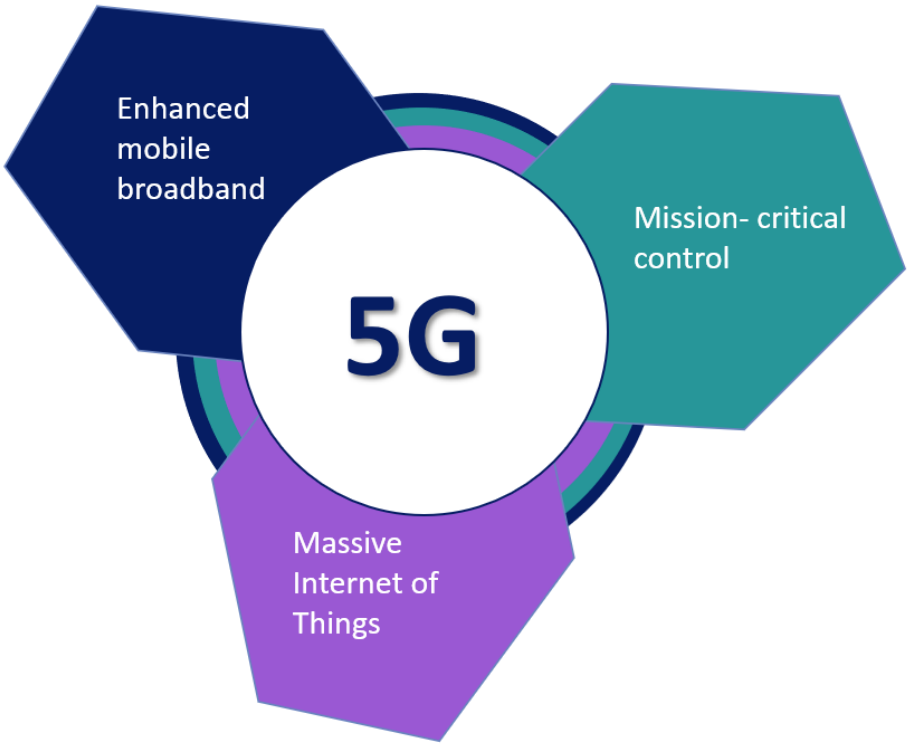

Figure 3: Where is 5G being used – Source: Qualcomm Developer Network

Enhanced mobile broadband (eMBB) which unifies network capacity and peak following the below:

- Extreme capacity: 10 TBps per km²
- Extreme data rates: multi-Gbps peak rates; 100+ Mbps user experienced rates
- Deep awareness: Discovery and optimization

Mission-critical control which include the services as vehicle-to-vehicle communication and factory automation:

- Strong security: health/government/financial trusted
- Ultra-high reliability: <10^-5 per 1millisecond
- Ultra-low latency: as 1millisecond
- Extreme user mobility: up to 500km/h

Massive IoT low-power and complexity devices like smart meters and environment sensors which provide the below benefits:

- Deep coverage: to reach challenging locations
- Ultra-low energy: 10+years of battery life
- Ultra-low complexity: 10s of bits per second
- Ultra-high density: 10 million nodes per km²

As Internet of Things/IoT [22] we refer to the network of physical objects or things that are embedded with sensors, software and technologies that is used to purpose of connecting and exchanging data with other devices and systems over the Internet. An IoT device is usually made up of a circuit board with sensors attached that use WiFi to connect to the internet. Therefore, an IoT can include anything you can think of today's "smart" devices such as smart mobiles, watches and TVs, cars - autonomous vehicles, drones, printers, refrigerators, cameras, smart TV, alarm, healthcare sensors or even security systems, and more. Many businesses will combine 5G and Internet of Things/IoT applications, virtual and augmented reality, and larger-scale robot and drone deployments.

The following 5G innovations are of interest for privacy issues:

- Higher data rates: 4G networks offer the maximum peak data rate (maximum achievable data rate for a user under ideal conditions) of 1Gbps and the maximum user experienced data rate (achievable data rate for a user in the real network environment) of around 10 Mbps.
- Higher traffic density: because of massive MIMO antennas and millimeter wave communication technologies, although 5G ultra-dense cellular network is still a density-limited communication system
- Higher reliability: the capability of guaranteeing the success rate of data transmission under stated conditions over a certain period.
- Lower latency: expected to reduce the latency ten times in the user plane, down to 1 millisecond, and half in the control plane.
- Connectivity for many more devices: to support a connection density of up to 1 billion connected devices per square kilometer.
- Lower power in support of the Internet-of-Things (IoT) causing IoT devices growth.

The evolution of the above digital transformation including 5G and IoT and hence the possibilities offered to both individuals and entities, aiming primarily at economic

progress, has made integral the introduction of specialized legal protection and clarification of the existing privacy framework because the PII data and generally massive data will rapidly increase now more than ever. Securing your IoT devices is an important step in protecting data, resources, and privacy. IoT devices require additional steps prior to connecting to the network as well as continuous monitoring while connected. The above-mentioned requirements are of key importance as both 5G and IoT boost security in some ways, with encrypted data, segmented networks and user's authentication but also has security vulnerabilities, including potential spying and attacks. The increased connected devices create more targeted attacks on vital connected systems which could become more chaotic and significant. Beyond this worldwide technical base of 5G and IoT, the EU legislation has widened the EU territorial privacy borders, as not only companies and individuals in the EU have to comply with GDPR but also the non-EU based entities and individuals, as the focus has now shifted to where the data subject is located as well as to data processing of people living inside EU.

The 5G technology will provide some many improved features and benefits worldwide in terms of cross border connections and EU aims to deploy 5G infrastructures and services with full implementation expected after 2021. However, to this point, it is important to review the security and privacy concerns considering the association between 5G and GDPR rights and obligations as per recent research reproduced [23] Table 1 represents the correlation between them.

Table 1: Correlation Between 5G Technology and GDPR Obligations and Rights – Source: IEEE Xplore

5G innovations components / GDPR Rights and obligations	High speed data rates	High traffic density	Massive number of connected devices (IoT)	IP-based

Right to be informed	X		X	
Right of access			X	
Right to rectification	X		X	
Right to erasure/to be forgotten	X		X	
Right to rectification	X		X	
Right to be notified about rectification or erasure	X		X	
Right to data portability			X	
Right to object			X	
Right in relation to Automated Decision Making and Profiling	X	X	X	X
Subject's consent and withdrawal of consent			X	
Child consent			X	
Privacy by design		X	X	X

Breach notification within 72h	X		X	
Privacy Impact Assessment (PIA)	X	X	X	
Location Privacy		X		X

5G promises anonymized authentication methods to provide secure end-to end communication. Although, these security features aren't activated by default which may cause some risks. Moreover, the smaller 5G cells, allow easier location data coverage, which data is constantly available to the network provider and could allow access to other service operators. Location-tracking data are potentially very harmful for vulnerable individuals who may be targeted for political, religious, or even commercial purposes important notes that do not comply with the current European requirements for location data as per GDPR.

As per IoT part, 5G offers the possibility of directly connecting billions of IoT devices to the internet through the "Massive Machine to Machine" mode, without any user interaction by design and by default. This raises the need for enhanced transparency for individuals who eventually need to know who processes their personal data, for what purposes and for how long etc. Furthermore, there is an increased risk of data breaches, because of the increased possibility to collect and process higher volumes of data related to physical human activities and health data. Another important fact which requires attention is that the major 5G network and IoT device manufacturers are located in third countries outside the EU/EEA, where personal data transfers are subject to a greater risk because those countries have no "essentially equivalent" data protection standards.

Despite 5G still IP-based, it could be an effective factor to privacy concerns since the allocation of IP addresses could result in other personal data as well as per the above challenges. However, the European Commission recognizes the importance of 5G as a fundamental block of necessary digital transformations and has taken steps to strengthen Europe's "digital independence". To be able to provide the appropriate technological and organizational measures to mitigate possible personal data protection

risks connected with 5G technology, considering the data protection by design and by default as well as data protection impact assessments as legal obligations under EU data protection law, controllers and processors have the justification and the tools at hand and will help the EU embrace more the 5G innovation.

3.1.2 GDPR and AI

There is a great analysis on correlation between AI and GDPR and the impact of the GDPR on AI below. AI is not explicitly stated in the GPDR, but many requirements in the GDPR are relevant to AI, and many are confronted by the new ways of processing personal data that are enabled by AI [24]. There is indeed a tension between the traditional data protection principles – purpose control/ limitation, data minimization, the handling of “sensitive data”, the restriction on automated decisions– and the utilization of the power of AI and big data. The last involves mainly the gathering of large amounts of personal data, social relations and not having quite determine the intentions of this processing during that time. Nevertheless, there is the ability to completely implement, understand such GDPR principles to take the most out of the use of big data and AI. For both above the re use of the personal data can be incompatible with the requirement of purpose control/ limitation if the purposes of the analysis are different of the ones of the initial ones during the collection of the data apart from statistical purposes (unless there are risks for the data subject).

On the data minimization principle, the benefits produced by the use of AI, involve in several cases the removal of personal identification through the use of pseudonymization and not the amount of data itself. So, any additional data which can lead to identification of the persons collected are being minimized or removed in a way such there is no possibility of re – identification. Re- identification can happen but if this required by laws and it is strictly determined by the purposes of the initial collection of these. GDPR information requirements determined can be satisfied regarding AI based processing with also considering the complexity of the AI application. The purposes of the data collected and AI – based processing involved should be provided to data subjects without providing any unnecessary technical details.

The GDPR provides conclusions based on personal data when appropriate safeguards are adopted. Profiling is in principle prohibited, but there are some exceptions (contract, law or consent). Uncertainties exist concerning the extent to which an individual

explanation should be provided to the data subject. It is also uncertain to what extent reasonableness criteria may apply to automated decisions.

The preventive measures which concern the development of AI systems regarding GDPR are privacy by design and by default, if correctly designed and implemented may require some additional costs and do not hinder the development of these. Additionally, there are many ways in high-risk AI applications to comply with GDPR from data protection assessment to preventive involvement of data protection authorities.

In essence, using personal data for statistical purposes which do not involve the inference of new personal data most possibly opens opportunities for the processing of these. It requires several security measures which should include at least pseudonymization and are proportionate to the risks for the data subject.

The GDPR prescriptions are often open-ended and vague, but they allow the development of AI systems and big data applications, even if they don't provide enough guidance to achieve this. These AI and big data applications are the ones balancing data protection and other social and economic [25] interests.

In the case of these applications, the uncertainties are aggravated by their complexity, the broad scope of their individual, the novelty of the technologies and social effects. It is a fact that processing of personal data with risk-prevention and accountability the advantages outweigh its possible disadvantages. Moreover, the any inclusiveness issues involved in these applications is avoided with learning and experimentation. The penalties for non-compliant combined with the uncertainty may comprise a "novel risk" so as to prevent smaller companies to attempt new endeavors. The success of AI application to be compliant is related to other competent authorities and guidance data protection bodies which will be provided to controllers and data subjects. Legal uncertainty will be reduced with appropriate guidance especially for smaller companies that need this kind of advice to implement compliant and efficient solutions.

The following suggestions are to be made regarding AI and the processing of personal data:

- The GDPR can be applied and interpreted accordingly without delaying the design and implementation of AI powered application about processing personal data.

- For the companies inside EU the GDPR doesn't mean automatically a disadvantage compared to non-EU competitors.

- The GDPR is more like meaningful suggestions - indications and it will not require major deviations in AI application which process personal data, nevertheless several aspects of AI related issues do not have a clear answer in the GDPR.

- Additional costs and risks like legal uncertainty can be minimized with providing more guidance on the applications of the AI on personal data, finally compliance will be enhanced.

- The different levels which should be approached involve all the stakeholders, specialized agencies, civile and data protection authorities.

- The debate is much broader involving civil and academic in addition to administrative and political authorities.

- In addition to the above the political authorities like EU Commission, Council and EU Parliament should provide further open-ended suggestions about the values in risk and how to achieve them.

- With the debate for AI processing personal data there is the opportunity to revise in further extend, with higher concentration and more precision, several principles of law and ethics, such as a more fair, practical, and acceptable conception of non-discrimination.

- National Data Protection Authorities should also provide guidance, when contacted for advice by controllers, or in response to data subjects ‘queries.

- Data protection authorities, and in particular the Data Protection Board, should provide controllers with specific guidance on the many issues for which no precise answer can be found in the GDPR. Such guidance can often take the form of soft law instruments designed with dual legal and technical competence, as in the case of Article 29 Working Party opinions.

- The use of personal data in a training set, for the purpose of learning general correlations and connection, should be distinguished from their use for individual profiling, which is about making assessments about individuals.

- The fundamental data protection principles – especially purpose limitation and minimization – should be interpreted in such a way that they do not exclude the use of personal data for machine learning purposes. They should not preclude the creation of training sets and the construction of algorithmic models, whenever the resulting AI systems are socially beneficial and compliant with data protection rights.

- Guidance is needed on profiling and automated decision-making. It seems that an obligation of reasonableness – including normative and reliability aspects – should be imposed on controllers engaging in profiling, mostly, but not only when profiling is aimed at automated decision-making. Controllers should also be under an obligation to provide individual explanations, to the extent that this is possible according to the available AI technologies, and reasonable according to costs and benefits. The explanations may be high-level, but they should still enable users to contest detrimental outcomes.

- It may be useful to establish obligations to notify data protection authorities of applications involving individualized profiling and decision-making, possibly accompanied with the right to ask for indications on compliance.

- The inference of new personal data, as it is done in profiling, should be considered as creation of new personal data, when providing an input for making assessments and decisions. The same should apply to the re-identification of anonymous or pseudonymous data.

- Normative and technological requirements concerning AI by design and by default need to be specified.

- The possibility of repurposing data for AI applications that do not involve profiling – scientific and statistical ones – need to be broad, if appropriate precautions are in place preventing abuse.

- Strong measures need to be adopted against companies and public authorities that intentionally abuse the trust of data subjects by using their data against their interests.

- Collective enforcement in the data protection domain should be enabled and facilitated.

- It needs to be ensured that the right to opt out of profiling and data transfers can easily be exercised, through appropriate user interfaces. The same applies to the right to be forgotten.

As a summary, the data controllers can engage with AI processing personal data for them to be compatible with the available technology, public interest and economic effectiveness, the controllers should provide the values of GDPR and take a risk-oriented and responsible approach. The controllers should not be alone in this attempt because of the ambiguities and vagueness due to the gaps and the complexity of the matter. As per above recommendations the data protection authorities should address and actively engage with all the levels of audiences like processors, controllers,

stakeholders, and civil society to produce all the appropriate guidance & responses with having in mind all the technology aspects and shared values as well as the institutions which need to provide precise indications to promote a broad societal debate. The most important 2 pillars as: trust and prevention of risks can be achieved with the ability to use AI efficiently combined to consistent application of data protection principles.

Apart from the mainstream approach of AI opportunities, either complementing several human capacities (like the ability to know and act) supporting creativity and invention or completely replacing human activities, it may be possible to achieve higher levels if cooperation between human and machine. This cooperation overcomes the classical model in which machines complete reparative and routine tasks, and includes creative activities like taking decisions, managing synergies but also preserve and enhance human initiative and work satisfaction. However, there are serious risks in eliminating or devaluing work for those who can be replaced by machines to be excluded from or marginalized in the job market by the development of AI and its convergence with big data. These actual risks not only for individuals but for groups and the whole society, some additional risks are below:

- Certain abuses are led by the fact that many platforms hosting and processing user content are incentivized by two or more markets, so even if the services are given to the users in certain context (social networking, search etc..) the revenue stream comes from influencers, advertisers, and opinion makers.
- Profit-driven algorithms can be used in order to advance anticompetitive strategies, to disadvantage not only competitors but also of consumers. AI also can contribute to polarization and fragmentation in the public sphere, and to the proliferation of sensational and in some cases fake news.
- The ad campaigns lead to a massive collection of personal data about individuals, to the loss of privacy, but also to a pervasive influence on their behavior, to the loss of both individual autonomy and collective interests, the users can further be subject to pervasive surveillance, manipulated in their choices, controlled in their access to information and opportunities.
- Apart from the ethical and social risks, AI and big data systems can fall subject to cyberattacks (designed to disable critical infrastructure, or steal or rig vast data sets, etc.), and they can even be used to commit crimes (e.g., autonomous vehicles can be used for killing or terrorist attacks, and intelligent algorithms can be used for fraud or other financial crimes).

- Advanced anticompetitive strategies can be further implemented to further loss for not only competitors but also of consumers by profit-driven algorithms.

The below section describes the danger of profiling as it is further defined in the below case. [26] The dangers involved in profiling have emerged with clarity in the Cambridge Analytica case, concerning attempts at influencing voting behavior – in the United States' 2016 election and possibly also in the Brexit referendum – based of massive processing of personal data.

Terms of the case: people being registered as voters in the USA were invited to take a detailed personality/political test (about 120 questions), available online. The individuals taking the test would be rewarded with a small amount of money (from two to five dollars). They were told that their data would only be used for the academic research. About 320 000 voters took the test.

The process of the case: in order to be receive the reward each individual taking the test had to provide access to his or her Facebook page (step 1). This allowed the system to connect each individual's answers to the information included in his or her Facebook page. When accessing a test taker's page, Cambridge Analytica collected not only the Facebook page of test takers, but also the Facebook pages of their friends, between 30 and 50 million people altogether (step 2). Facebook data was also collected from other sources. After this data collection phase, Cambridge Analytica had at is disposition two sets of personal data to be processed (step 3): the data about the test takers, consisting in the information on their Facebook pages, paired with their answers to the questionnaire, and the data about their friends, consisting only in the information on their Facebook pages. Cambridge Analytica used the data about test-takers as a training set for building a model to profile their friends and other people. More precisely, the data about the test-takers constituted a vast training set, where the information on an individual's Facebook pages (likes, posts, links, etc.) provided values for predictors (features) and the answers to the questionnaire (and psychological and political attitudes expressed by such answers) provided values the targets. Thanks to its machine leaning algorithms Cambridge Analytica could use this data to build a model correlating the information in people's Facebook pages to predictions about psychology and political preferences. At this point Cambridge Analytica engaged in massive profiling, namely, in expanding the data available on the people who did not take the test (their Facebook data, and any further data that was available on them), with the predictions provided by the model. For instance, if test takers having a certain pattern of

Facebook likes and posts were classified as having a neurotic personality, the same assessment could be extended also to non-test-takers having similar patterns in their Facebook data.

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence finally (stage 4), based on this personality/political profiling, potential voters who were likely to change their voting behavior were identified (in US States in which a small change could make a difference) if prodded with appropriate messages. These voters where targeted with personalized political ads and with other messages that could trigger the desired change in voting behavior, possibly building upon their emotions and prejudice and without making them aware of the purpose of such messages.

3.2 Education sector

Educational Services sector prescribe the institution or the process of facilitating learning, knowledge, skills, values incorporating educational methods such as teaching, training or even researching in a wide variety of subjects. This framework is divided by specialized establishments, such as schools of all stages like preschool, kindergarten, primary and secondary school, colleges, universities, or even the training centers.

The education institutes collect a significant amount of personal and sensitive data related to either student's profile such as name, surname, birth date, family information, images, medical information, grades, addresses, or staff's data, volunteers and many more. Furthermore, most of them usually exchange PII with other institutions, and on many occasions, involve different countries. The GDPR's changes in data protection and privacy law revealed several areas of uncertainty on how the education sectors are impacted, however, the organizations including the educational institutions - even if they have no physical presence in the EU, regardless of location, need to be mindful of data protection and comply with GDPR rules and restrictions when engaging EU's data collection, processes, storage, and transfer. Thus, the processing of personal data stored on each educational service sector/institution such as e-classes, websites, papers, servers, and databases and more is covered by GDPR especially when engaged EU's data the education institute is subject to the GDPR's requirements. A non-EU educational institution is subject to the GDPR if it has a "connection" in the EU, such as a study program out of the country, even if the institution does not own or control the facilities used, or if it provides remote learning services. Furthermore, the

GDPR would apply to educational sector if an institution falls under one of the below circumstances:

- A data subject is employed or conducts research in EU
- Monitors personal data which come from an EU data subject
- Recruit possible candidates' such as students or employees in the EU
- Performs initiatives such as volunteering, donating from individuals in the EU

The age that students can be consulted over their personal data processing, depends on local data protections laws. However, under GDPR it is stated that with exception, the organizations - including educational institutions, cannot legally obtain consent from minors. Therefore, it depends on each country to determine when someone is no longer considered as "minor" like for instance their age. If the data subject is younger than the predefined age, the institution has to act accordingly depending on the occasion.

An institution deals with different ages of young pupils, students, or employees and to comply GDPR the institution has to provide communication in written and formatted text so that the contents are legible. A qualitative content analysis of how the University of Athens/UOA/EKPA [27] has managed this communication about the data subjects' rights are supported by appropriate procedures within EKPA that allow the required action to be taken within the timescales stated in the GDPR. In the reproduced in the reproduced [27] Table 2 represents the timescales.

Table 2: Timescales for EKPA data subjects' requests – Source: uoa.gr

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right of rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	One receipt of objection
Rights in relation to automated decision making and profiling	Not specified

In addition, it is recommended to test the consent requests and the relevant privacy policies. Therefore, GDPR brings a new responsibility to institution to inform relevant

stakeholders or parents under certain circumstances, about how they are using individuals' (pupils, students etc.) data, how it is being used by and more. According to GDPR the instruction requires to assign at least one lawful representative for PII's processing. The data protection officer (DPO) is responsible for ensuring that the school is managing data properly and advising on how to do so. Moreover, as per GDPR the two roles of data processor and data controller take different responsibilities even in the institutions. The data processor can be either a third-party supplier that the institution hired or a department within the institution. The data controller in this sector is usually assigned to the institution to manage the data processing activities.

It is challenging for institutions to protect individuals' personal data especially, under their usually tight budgets, with limited resources, and assign a dedicated security team. Expected risks also include the big cache of learner's data which usually institutions maintain for years after their graduation due to legal requirements.

In case of a data breach the relevant institution must investigate the incident immediately and has to determine if it needs to be reported to the relevant authority to take actions considering the 72 hours deadline. A data breach can cause many damages for the affected individuals like social damage, identity theft or fraud, facing economic or financial loss as well as reputation damages.

Taking steps to ensure that the learning platforms comply with the privacy laws in your country will help the institution keep this information secure and mitigate any legal and financial exposure. An institution can simplify the data protection compliance requirements in consultation with counsel, with the DPO's help and refer to the official GDPR compliance resources for education sectors.

3.3 Public Sector

In public sector the GDPR emphasizes to the protection of personal data as it brings numerous significant adjustments and limitations. Again, a thorough assessment must be executed as some of the principles are applicable due to exceptions which should be respected before the application of the generic rules. Upon this, it is highly advised to refer to local laws because maybe there are stricter or additional requirements to be enforced and are different from country to country or region to region [28] , [28].

The public sector administration is always subject to rules like the GDPR on processing personal data, so for the individual data there is always the responsibility of local administrations (national or not) to prepare for the submission under GDPR regulations.

Most of the data collected and held are subject to legal obligations, so it is paramount to any activities executed to be in the public interest and official authorities. In relation to public administration the personal data must be a subject of key principles, like:

- Processing to be fair and in accordance with laws
- Purpose limitation
- Data minimization
- Data retention

In the case of processing on the lawful basis, this law should already ensure that these principles are observed such as the type of data, the retention policy and location as well as appropriate safeguards. The above principles are emphasized for any compliant cloud service that provides storage and processing not only for the public sector but also for private ownership. Consequently prior to processing any type of data (personal or not), individuals must be informed about this, its purposes, the type of data collected, the recipients, and their data protection rights.

The key to all the above is the role of Data Protection Officer which is required to be set in the organization along with the appropriate technical and organizational measures/ precautions to secure personal data. In cases that one DPO is not enough the role can be appointed to multiple or even outsource to an external. In the last case of external then the organization should be covered with a contract or other legal acts to meet the standards of GDPR. The external organization will be called “processor” and can take act under this contract and or other legal acts to safeguard the GDPR standards. In the unfortunate event of data breached or disclosed accidentally then the breach must be reported to this Data Protection Authority the sooner possible without delays within 72 hours for handling the event, this DPA or the administration may need to inform individuals which data breached and react to the event. GDPR does not apply to government agencies and law enforcement when data are collected and processed for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties or for preventing threats to public safety. [29] Although, in the GDPR regulation words like public administration or authority are referenced about 49 times and in this context, there is a clearer concept of how GDPR applies on these organizations, below there are few examples of how public authorities can approach personal data like private sector.

“(6) …The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.”

GDPR outlines a model that references “controllers” and “processors” of personal data and deems them responsible for protecting personal data in their respective roles. The regulation clearly states that public authorities can play these roles.

“(7) ‘controller’ means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;”

GDPR even considers that public authorities could be subject to fines for violation of the regulation.

“(150) …It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.”

Apart from the above the GDPR also considers the cases that does not apply in contexts of criminal investigation and prosecution.

“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, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes.”

As a summary the application of GDPR to the processing of personal data by public authorities is context dependent, and public sector customers will need to individually assess the applicability of GDPR to their activities.

The GDPR does allow a data transfer based on consent of the data subject, however, public sector organizations can hardly ever use this exemption. The rationale behind

this is the relational imbalance between the government and its citizens, which is impeding with the requirement that consent must be 'freely given'.

3.4 Healthcare and Medical Sector

For the Health care sector, the GDPR impacted greatly the way data are collected, handled, and stored similar to other industries so it is empowering every patient with more control over his personal information collected. In more detail, it has introduced the “detailed patient profiles” which means that the providers can have more details about patient information which led a more accurate and better diagnosis but one principle – the “right to be forgotten” has challenged the practices for healthcare organizations to retain patient data. These data in most cases were retained even after the discharge or death of a patient which means these should be dealt in accordance with the GDPR regulations. As a result of the regulations there should be a timeframe in which personal data are kept and how these are stored. The GDPR is quite significant for the healthcare industry, as an example in the US most of these regulations are incorporated in the Health Insurance Portability and Accountability Act (HIPAA) which is a healthcare law with data protection elements with above others include sweeping regulations.

The consequences for medical records even if the GDPR does not explicitly require a controller to give access to a patient regarding original records, given the circumstances it may be required for the controller to be informed for this particular action. Hence, if a patient is permitted access the controller may be informed. In the above context for a health institution not located in the EU, even if GDPR may not apply to an institution like a hospital directly, it applies to any health company in global level who collects, stores and process personal data for individuals located in the EU, because these residents are based in the EU. Therefore, the major issues related to data protection in the health care industry, concern technical aspects of data protection and inappropriate setup of the access management systems. Specifically in hospitals, the IT systems which are being used for data processing of patients usually are open to the employees without sufficient restrictions. I assume one of the main reasons why this happens is because of the fear that access restrictions and usability issues to avoid situations for forgotten passwords or loosing security tokens. While this is a common issue across many health care institutions, it could be resolved if all involved stakeholders, including software

developers and data protection authorities – to develop access protection systems that meet both health care needs as well as GDPR's data requirement protections.

3.5 Financial Services Industry

The financial services prescribe the economic services provided by the finance industry, which encompasses the set businesses that manage money, banking, investing and insurance activities. Key role in the FSI plays the institution's types: banks including retail, commercial and web banking, credit unions, brokerage and insurance, loans, mortgage, stock, investment funds and more. The FSI institutions are being represented by different roles and offer wide range of type of products and services to their clients.

The reviewed resources refer to several challenges associated with the implementation of the GDPR in the FSI, while GDPR forces financial institutions to ensure the privacy of their customer data like the organizations being involved in EU's data. The GDPR has drawn the FSI's security and privacy professionals' attention in order to comply with this privacy regulation, despite that the FSI is already a subject to broader global privacy regulations.

While data subjects/consumers are becoming more sensitive about their privacy, and with each incidence of data mismanagement announced in the news, they demand more transparency in how their data is processed, stored, or shared. On the other hand, financial institutes collect huge amounts of customer data, which is used for different activities such as client onboarding, customer relationship management and accounting. During these activities, customer data is exposed to many different people and third-party vendors. The most challenging for the financial institutions, though, is that the data management is performed with different systems and solutions, resulting massive data increase which from one perspective cause more complexity in their ability to know how to manage and server their customers in a better way while complying with GDPR. Additionally, many financial institutions use modern AI technologies while store biometric information, and privacy concerns and complexity are expected to grow even more. The data subject as per GDPR, has the right not to be excluded from any kind of profiling, so, in other circumstances where profiling it permitted, it is recommended to perform privacy measures considering the data subject's rights. This has caused significant impacts on big data projects of profiling or for marketing purposes, fraud detection or recognizing customer's behavior. While GDPR, clearly applies to the data processing activities of EU based companies, it also

provisions apply to any organization that handle PII covering EU residents, including the FSI instructions in other countries that have EU residents as customers.

Therefore, still GDPR requires end-to-end accountability to ensure that EU's residents data stays protected by enforcing even the FSI and its support functions to embrace privacy and compliance. FSI institutions have to inform their consumers what they will do with their data prior collecting and how individuals can keep their privacy and security. The financial institutions can address some GDPR privacy areas as per below:

- Detect PII in the FSI institution
- Perform privacy practices for securing personal data
- Comply with GDPR obligations
- Manage the customer requests/concerns related with their personal data
- Responding to and reporting data breaches within the required SLA
- Prepare for data deletion requests.

Hence, according to GDPR, financial organizations must inform the data subjects what they will do with their data before it is collected/processed and how individuals can keep their privacy and security. The GDPR's prerequisites on EU's personal data processing forced the financial institutions placing them restrictions on managing PII. Although, all companies in the future will need to keep a record of personal data while the data subject has the right to ask that the institution deletes their data.

The GDPR fines in this sector have been increased lately with now several fines ranging in the millions. The common reason why this happened is due to lack of adequate internal compliance measures to ensure a sufficient legal bass for processing their customers PII. FSI industry should strongly establish and implement comprehensive processes to have a clear basis for every data processing activity. The authorities are looking more closely at how consent was obtained and if data subjects where informed by the data controller. Additionally, insufficient data security measures resulted in fines which cause reputational damage. Unfortunately, not all FSI companies focus on strong data security measures yet, so data security will become more important in this sector as long as it is transforming the core business into digital such as online banking, payments insurances applications etc.

3.6 Retail

Regarding the retail industry the GDPR has tremendous impact on this sector and businesses due to fact that e-commerce business is quite tightly connected with personal data. Modern retail services like online shopping websites which collect, track customer identity for processing advanced metrics, profiling and targeting via customization have been quite pressure by GDPR and many of them are at risk. According to data from Eurostat [31] the early impact of GDPR on European Web Traffic, Web Traffic and E-commerce, e-commerce revenue decreased by 8.3%, page views fell by 9.7% and website visits dropped by 9.9% due to GDPR.

The impact on e-commerce is so remarkable because GDPR is reshaping the whole "business" after May 2018. While e-commerce is evolving rapidly [32], the terms of the business had to be changed. For instance, in tourism business the legal aspects had to be kept with e-commerce in mind when both services and products have to been given online, like online bookings. In effect, the European legislation had to be followed so in the above example the service – website must clearly inform the users for many aspects:

Contractual information: The contractual procedures regarding the purchase must be clearly stated so a user who agrees to go on with a purchase must know that he agrees to this and the terms of this purchase as a service. The terms of the modification or elimination of the information gathered have to be stated as well as the terms of use of this service/ website which is being used for this purchase, the provider, client and or services information that will be stored. This service/ website should confirm all website purchases within 24 hours with notifications which can be electronic or by any other mean indicated in the above contract. The only requirement is that the notification must be saved by the user according to the method chosen.

Withdrawal period: The e-commerce platform should also state clearly to the user about the ability to withdraw form this contract within 14 days if the product/ service is not satisfactory. This withdrawal is in context of the directive on consumer rights.

Use of cookies: E-commerce services like websites are obligated to have a cookie policy notifying the user about their use when they access the website, even if these (the cookies) are pieces of data sent by the websites that remain on the user's personal computer to help with future browsing etc. these may be also a security risk. From the

GDPR standpoint the use of these must be clear for the user and no other aspects are clearly defined.

Data protection: When personal data (like user information) are gathered with any process like registration, purchase or contact form, under GDPR the users must be informed that these data are collected in line with the requirements of the General Data Protection Regulation (GDPR).

In this context, there should be a clear indication of where these data are being stored, and what are the tools the users may use to future data access, modification, or elimination. With all these regulations user is offered a higher level of security in using online services, these obligations have to be respected in any form of these services. These regulations have to followed aiming to establish a consistent regulatory framework among EU countries and all the services must comply to these and their updates - e-commerce in the EU single market including any local law regulations.

The ways of accessing an online service with compliance, are many considering the rules to be complied with. We will refer to some examples below:

Newsletter subscriptions:

- Visible link to the Data protection policy which should be in line with the principles of GDPR
- Confirmation action (tick box) in which the user is notified for the policy before sending the information to the platform
- Confirmation action (tick box) in which the user agrees to provide personal information before a purchase
- Access to the service / website
- Message for the use of cookies
- Visible link and in permanent location about the use of cookies
- At least one method so the user can contact the service provider (website owner) to find out more on the contractual legal aspects of products and services given by this service (website)

Upon a user’s purchase:

- Access to all contractual information right before a user proceeds to a purchase (on delivery periods, payment methods and cancellation options)

- Notification of a purchase within 24 hours either electronically or other method giving the ability to the user to store this information

Finally, there are roughly 4 steps that providers can use to comply with GDPR and review their services given to users:

Step1: Assessment of the data captured, methods and details on these.

Step 2: Clear statements made available of the processes of the above, how and when data is captured, stored, handled and is available to the users.

Step 3: Development of the individual policy for the personal data complying fully to GDPR

Step 4: Consistent and continues updates in security measures implemented for the service

Considering the impact of GDPR in retail especially in e-commerce customers in Europe a recent study shows that a year after the GDPR took place, e-commerce customers in Europe appeared to have a significant behavior in Europe as per below reproduced [31] chart Figure 4. According to the chart, 32% of European consumers shopped online 1 or 2 times, 17% did 6 to 10 times, and 87% purchased from national e-commerce websites. Finally, 35% bought online from other EU countries.

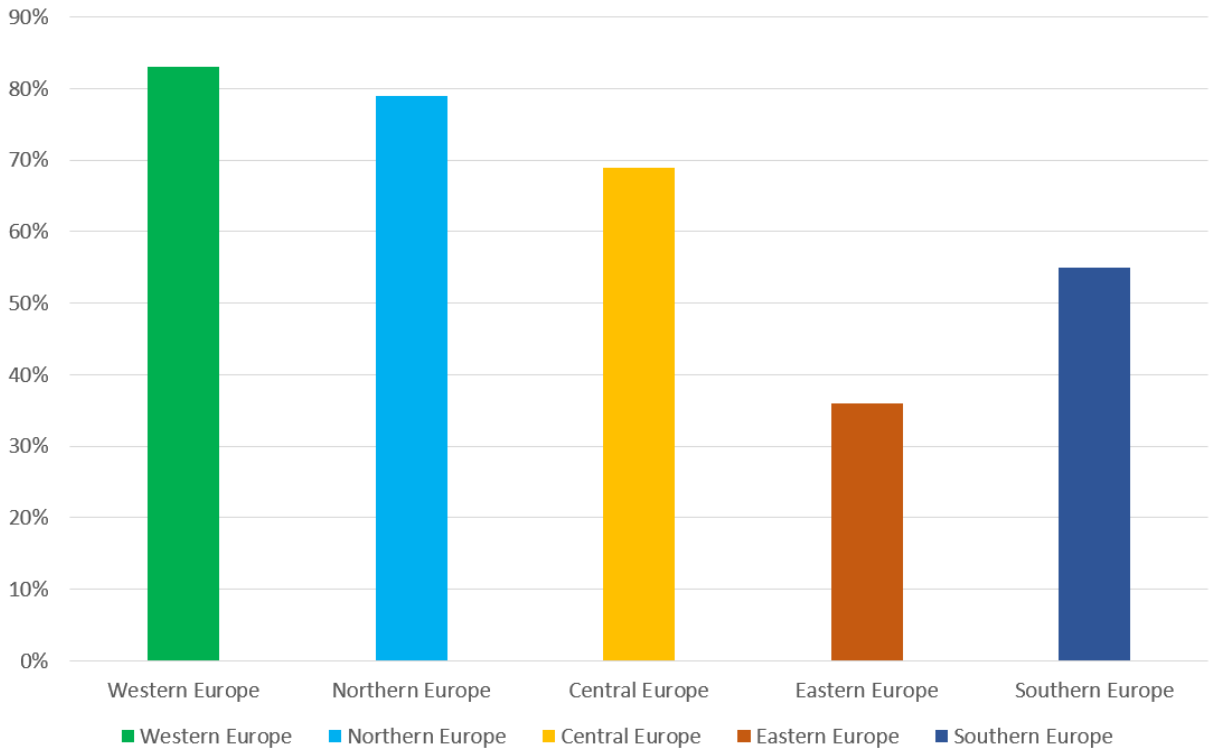

Figure 4: E-commerce customer behavior in EU countries – Source: Ecommerce News

4. THE IMPACT OF GDPR TODAY

Reaching the first anniversaries of the GDPR implementation, we can assess how past months have marked a transition to this new data-protection concept, and what are the outcomes of the EEA GDPR which applies to the member countries of the EU and to all countries in the EEA.

In 2019 the European Union Agency for Fundamental Rights/FRA prepared a document reporting [33] opinions and experiences of people in the EU linked to data protection and technology. The major conclusions of this report are the following:

- Two years after the GDPR succeeded meeting many expectations despite the identified areas of future improvement
- The Commission will provide updated proposals considering the above areas.\
- The Member of States will benefit more in the next years
- GDPR embraced globally the data protection and offered new opportunities
- EU citizens are more empowered and aware of their rights while 69% of the population above 16years old has already heard about the GDPR and 71% of people heard about GDPR.
- Businesses and Small and medium-sized enterprises/SMEs have just one set of rules to which to adhere and GDPR creates a level playing field with companies not established in the EU but operation here.
- The GDPR is an essential and flexible tool to ensure the development of new technologies according to fundamental rights and the future proof and risk-based approach of the GDPR will be applied in the future AU framework of AI and in the implementation of the EU Data Strategy.
- Cooperation and consistency mechanism between data protection authorities and members of the European Data Protection Board (EDPB) has been performed by using the cooperation tool of mutual assistance intensively and EDPB adopted sever opinions over the past two years.
- GDPR contributed to global data protection standards helping other in the privacy rules modernization like: Chile, South Korea, Brazil, Japan, Kenya, India, Tunisia, Indonesia, Taiwan, and California state.

- GDPR facilitated international data flows offering a modernized toolbox for transferring data from EU to third countries or international organizations while ensuring that the data stays protected.
- GDPR gives national data protection authorities harmonized and strengthened enforcement powers such as administrative fines, warnings, reprimands, orders to comply with data subjects' requests, orders to bring processing operations into compliance with the GDPR to rectify, erase or restrict processing.
- Main future improvements can be made and require a strong engagement from all actors:

  1. Ensuring that national regulation is fully in line with the GDPR
  2. Member States providing data protection authorities with the necessary human, financial and technical resources to properly enforce the data protection rules but also reaching out to stakeholders, both citizens SMEs.
  3. Data protection authorities developing efficient working procedures regarding the functioning of the cooperation and consistency mechanisms, including on procedural aspects
  4. Making full use of the toolbox under the GDPR to facilitate the application of the rules
  5. Closely monitoring the application of the GDPR to new technologies such as AI, IoT and blockchain.

A punishable situation in a company can be revealed through proactive inspection activities conducted by the data protection authorities, by an unsatisfied employee or by customers or potential customers who complain to the authorities, through the company making a self-denunciation, or by the press in general, especially through investigative journalism. Although the legislation has no doubt resulted in a more demanding regulatory landscape, many of the initial fears – for example, maximum penalties for data breaches – have not occurred. Furthermore, the regulation has largely been well integrated into the financial services sector.

The Enforcement Tracker [34] gives an overview of reported fines and penalties which data protection authorities within the EU have imposed so far.

1. Penalties for failing to comply with the basic processing principles of GDPR may subject the organization to fines up to €20 million or 4% of the organization's total global revenue, whichever is greater.
2. Imposes new obligations for both controllers and processors of personal data.
3. Places a greater emphasis on accountability requiring greater documentation and records.
4. GDPR is not a one-off compliance regulation and requires a fundamental organizational transformation about data protection and privacy.

There are also questions raised about UK's next steps regarding Brexit and GDPR. As per reviewed resources [35], [36] Britain will attempt to move away from European data protection regulations as it overhauls its privacy rules after Brexit, the government has announced. However, the GDPR rules are part of UK law even after Brexit under the Data Protection Act.

The past years businesses pay more attention on digital data, cloud computing and remote working as data breaches have been increased significantly. A data breache expose sensitive data and usually leaves the exposed individual or the company at risk of identity theft, business loss and reputational damage. Therefore, compliance and privacy regulations occurred as the need of providing information security within the GDPR's SLA. Worldwide countries are conducting privacy laws and regulations to guide companies and organizations on how to secure and protect their citizens' data and privacy. Many companies and organizations have complied for facing unprecedented non-compliance fines and other penalties. GDPR primary, is the new set of data privacy rules designed for EU individuals to control better their EU individual's data. Its objective is to make the regulatory environment simple so that both businesses and their customers in the EU can ultimately benefit from the digital economy following the GDPR's recommended actions:

- Reporting the data breaches within the 72 hours SLA.
- Privacy-by-design principles need to be integrated into the development of new processes and technologies.
- The data subject's consent is required prior processing personal data.
- Assigning a DPO.

- Keeping records of data processing activities.
- Increase security measures considering the privacy risks.
- International transfers are subject to specific requirements and mechanisms.
- Reporting to one supervisory authority.
- Act accordingly on the right to erasure, right to portability, and an increased right of access.

4.1 GDPR and coronavirus

The GDPR fundamental rights to data protection and privacy is being challenged during Covid-19, with respect to working remotely with a few practical ways to handle them cost-effectively. The battle against the COVID-19 [37] caused many corporate technology companies introduce different solutions living or working remotely. Attempting to enforce employees to work remotely/virtually involved configuring remote work mechanisms while some of them were not in place yet, causing sudden mass personal data protection risks. Unfortunately, the organizations were not prepared for such a situation while this caused threats and reasonable concerns about their investments. Moreover, all sectors had to replace many daily duties into digital ones. Even the covid-19 vaccination in many countries has allowed individuals access to new digital health services. EU Member States, EU institutions and Big Tech companies are trying to explore solutions to tackle the uncontrolled spread of the virus.

During Covid-19, many employees were not ready and those who are unfamiliar with data security topics may not understand how a simple action like an update, can lead to a data breach exposing their personal data, while with this update probably data protection changes occur. Such a data breach will challenge the end user, the company's reputation and such an incident will lead to costly GDPR fines.

The teleworking during COVID-19 challenged European Data Protection Supervisor /EDPS and adjusted the approach to core activities, while leveraged the relationship with stakeholders of public and civil authorities as well as education institutions. Another critical sector was ensuring the EU's personal data protection within the supplement transfer tools. During the data protection global crisis, EDPS continued acting fast, while cooperating with the EU institutions and the EDPB to secure and protect the fundamental rights. As a result, there was established a Covid-19 task force to monitor and assess public - government and private sectors to prepare and follow the future of

data protection and privacy after Covid-19 crisis. The essential tools provided towards EUIs are according to the Action and Foresight pillars following the 2020-2024 strategy, the Dat protection Impact Assessments (DPIAs) and many more.

4.2 Key GDPR Compliance Statistics

Although it is an EU regulation, the GDPR has far-reaching consequences, as all organizations across the globe must follow its rules if they want EU citizens use their services. As GDPR has already came into effect, we will look at some GDPR statistics that will help us measure its impact. After some years after the regulation came into force, the compliance statistics to GDPR facts about compliance statistics to GDPR facts about fines, what is the impact to the above sectors, who follows the GDPR requirements, who is not and what, if any, has affected the way we used to use technology and more.

Based on the recent survey of the Fundamental Rights Survey which collected data opinions and experiences of people in the EU, two of scenarios are going to be analyzed below.

The EU-27 people who were interviewed whether they have heard about the GDPR or not and the reproduced pie [33] in Figure 5 shows that overall, 69% of them have heard about it while 31% have either never heard about it or don’t know/preferred not to say. Moreover, 69% of Greek interviewed did know about the GDPR.

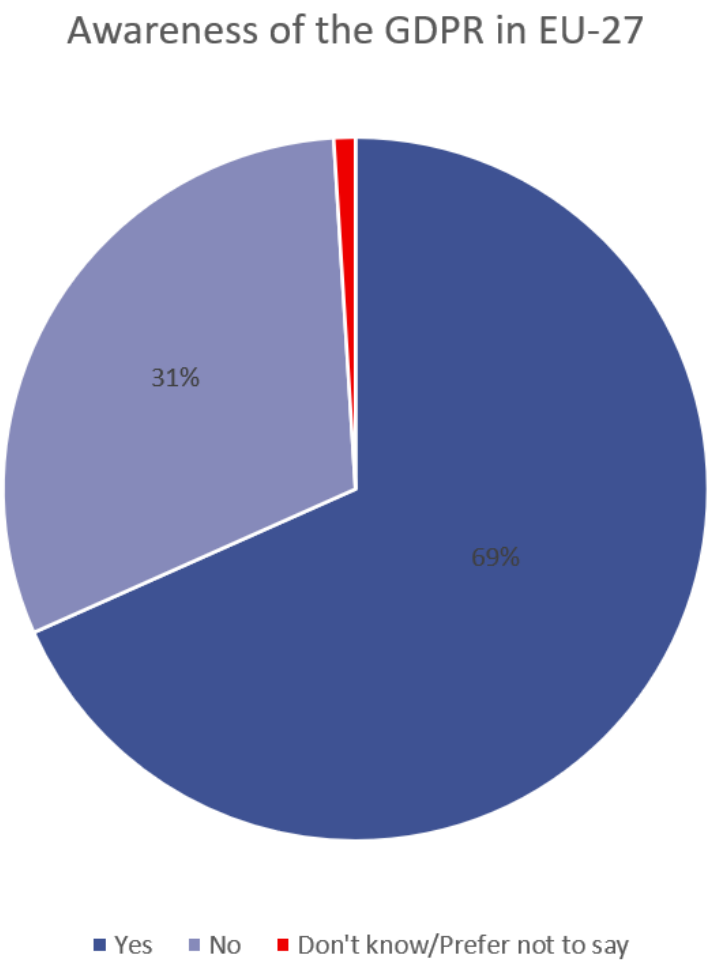

Figure 5: Awareness of GDPR in EU-27 countries – Source: europa.eu

When focused on the willingness to share personal data to public and private institutions out of the 27-EU countries 23% do not want to share any of these data with the public authorities and 41% do not want to share with the private sector. However, more than half of them would be willing to provide basic PII to public administration and more than one third would be willing to share such data with private companies. Since as PII can be digital identity data such facial images, fingerprint scan and more, the survey covered this topic too. Only 6% is willing to share facial images and only 4% willing to share fingerprint scan with private sectors. The results differ across countries as per reproduced chart [33] in Figure 6 and the reproduced chart shows the percentage of their willingness to share facial images to public and private sectors across the EU-27 countries. Following the survey and as per the reproduced chart flow, out of the 27 EU countries, Cyprus is the most willing country to provide facial images to public authorities while Germany, Poland and Romania are the most unwilling ones.

Moreover, the most willing country to share facial images to private organizations seems to be Malta, while the most unwilling ones is the country of Italy. Finally, 9% of the interviewed Greek people wanted to share their data with private sectors while 33% is more willing to share with public authorities.

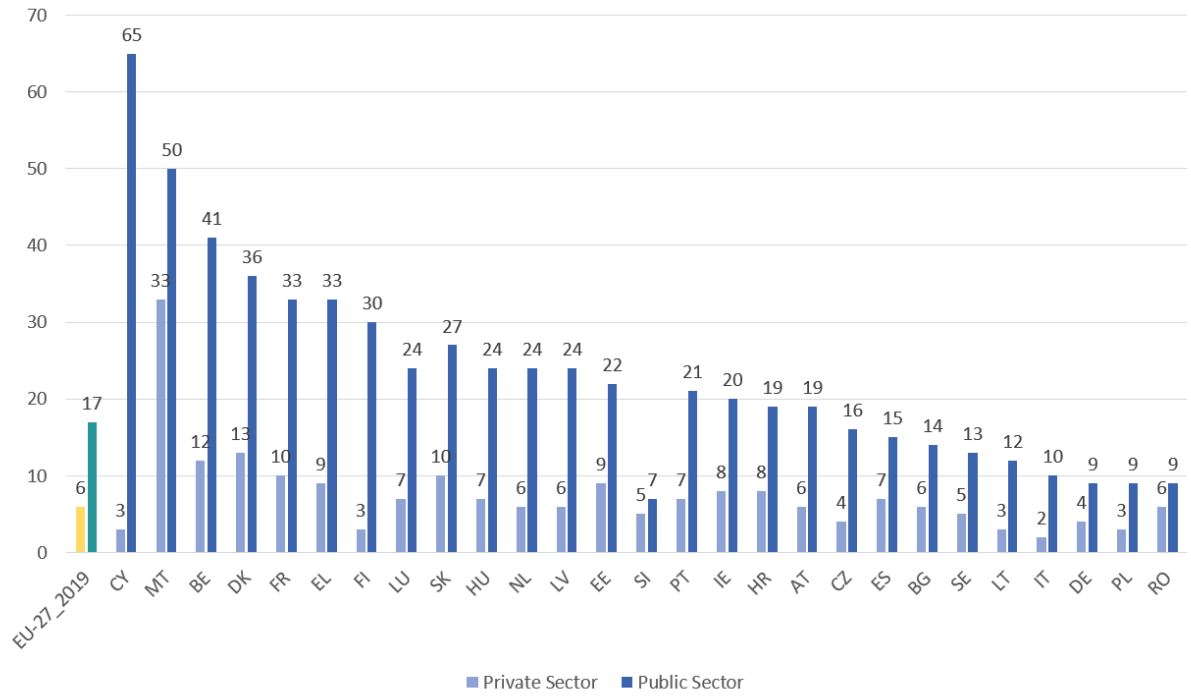

Figure 6: EU-27 countries willingness to share facial images to public and private authorities – Source: europa.eu

Based on most of the reviewed articles, most of the worldwide companies have taken steps to comply with GDPR and only a couple of months after the GDPR came into effect international companies were already paying attention to GDPR standards on personal data use. Many international companies took actions to comply with GDPR [38] while many of them have spent millions to become GDPR compliant and there are millions in major GDPR fines on international companies. Additionally, billions have been invested so far on GDPR compliance by companies in global level as GDPR applicability to international companies is a factor that can lead to penalties and fines when affecting EU's residents PII and many are making the investment to ensure they are not hit by sharper costs in the future. Since the compliance date for the regulation, EU data protection agencies have claimed millions in major GDPR penalties and fines.

Following the Enforcement Tracker [34] the below reproduced chart Figure 7 gives an overview of reported fines and penalties which data protection authorities within the EU have imposed so far. Spain out of the Eu-27 countries, leads the list of numbers of fines

per country by a large margin, followed by Italy and Romania, while Sweeden has the minimum total number of GDPR fines 24 in total.

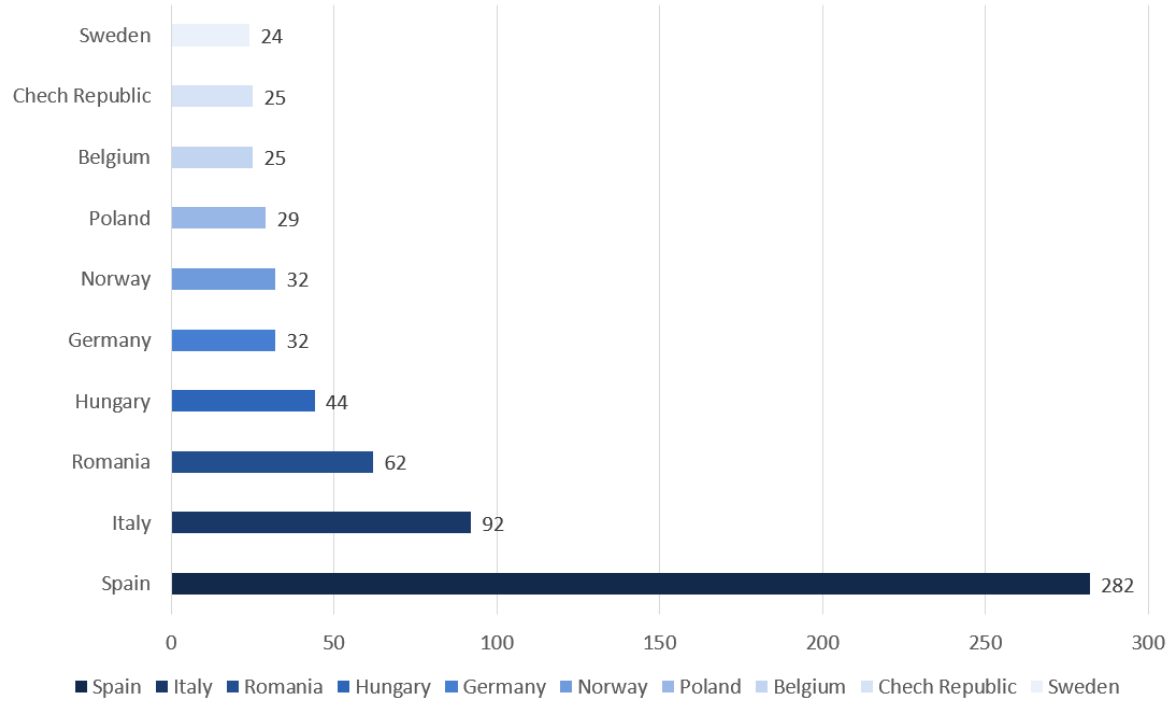

Figure 7: EU-27 countries by total number of GDPR fines – Source: Enforcement Tracker

The below reproduced [34] Table 3 shows how many fines and what sum of fines have been imposed per type of GDPR violation to date.

Table 3: Fines by type of violation – Source: Enforcement Tracker

Type of violation	Sum of Fines
Non-compliance with general data processing principles	€ 781,847,864 (at 165 fines)
Insufficient fulfilment of information obligations	€ 234,938,895 (at 56 fines)
Insufficient legal basis for data processing	€ 176,162,312 (at 278 fines)
Insufficient technical and organizational measures to ensure information security	€ 67,619,319 (at 165 fines)

Insufficient fulfilment of data subjects' rights	€ 16,195,825 (at 73 fines)
Insufficient fulfilment of data breach notification obligations	€ 1,284,091 (at 20 fines)
Lack of appointment of data protection officer	€ 219,000 (at 7 fines)
Insufficient cooperation with supervisory authority	€ 207,679 (at 32 fines)
Insufficient data processing agreement	€ 93,580 (at 4 fines)
Unknown	€ 500 (at 1 fines)

Finally, the following Figure 8 (reproduced pie) represent statistics according to GDPR fines by different industries. The statistics show the number of fines that have been imposed to date in each sector. We will notice that sector exposure is highest in the industries: commerce and media, telecoms, and broadcasting. The second sector includes digital media and platforms with a high "risky" processing of PII.[39]

Note: Only fines with valid information on the amount of the fine and on the corresponding sector are considered.

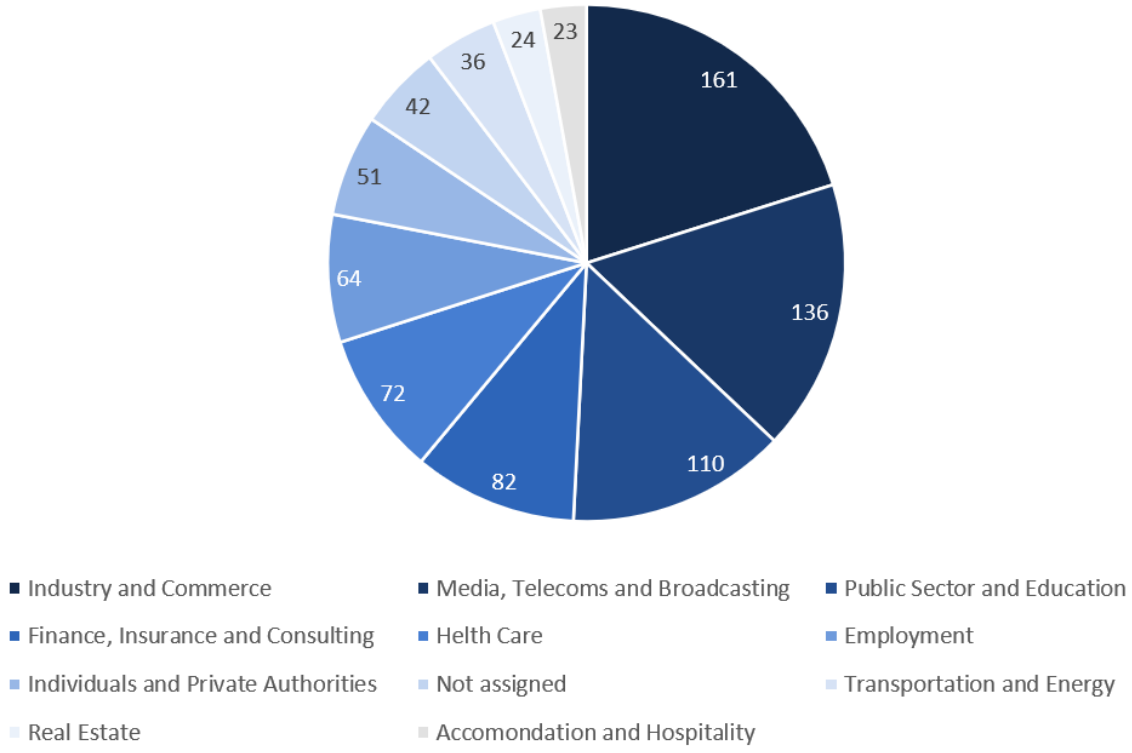

Figure 8: Total number of fines by sectors – Source: Enforcement Tracker

5. CONCLUSION AND OUTLOOK

The GDPR is clearly having an effect, but both private companies and the regulating representatives have been slow to adapt to the changes. Achieving GDPR compliance may sound challenging, but it makes the business more efficient, competitive, and secure. GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the EU. The new regulation has brought about many opportunities for differentiation, strategic advantage, and innovation in a highly competitive marketplace.

Under GDPR the law asks any organization to make good faith effort to allow EU people control how their data is used and who has access to it. To accelerate this, if requested you must be prepared to provide them transparently and openly with the information, they need to allow them to understand how their data is collected and used. EU provides many resources to help such as the GDPR compliance checklist to ensure your organization is meeting GDPR standards. The essential components of keeping your organization safe are quite straightforward, for either beginning now by the assessment, educating more people, or even expanding towards a cybersecurity short – long term plan.

Even in the EU, the post GDPR statistics show that many companies do not fully understand or do not know how to implement the GDPR. However, the amount of money being spent, as shown by the GDPR compliance statistics, shows that companies are clearly taking efforts seriously. When it comes to GDPR enforcement, there have been several cases and massive fines for major companies. However, the number of cases is still low. The penalties might be high but compared to the percentage of companies that are reportedly not GDPR compliant, we could expect the volume to be much higher in the GDPR statistics in the upcoming years.

The upcoming years are set to be a focused-on privacy protection regulation as several notable privacy laws will begin enforcement, with several others falling in line to the new international standard set by the GDPR. Cross-border transfers are likely to be one of the big compliance issues being tackled by legislative bodies and data protection authorities to ensure a regularization and normalization of data transfers between countries. The maximum GDPR fine for failing to comply is €20m, although some of the key points and best practices are summarized below:

1. Update privacy notices.

2. Prepare to delete customer data.
3. Prepare for data access requests.
4. Build a data protection culture.
5. Identify personal data you hold.
6. Use secure email.
7. Prepare a plan for data breaches.

Hopefully, this view of the GDPR has helped you understand the impact of this regulation. Finally, as stated in the beginning of this thesis the aim is to create awareness. I would like to remind the reader once more that there are lots of provisions in the GDPR that apply only in rare instances, which would be counterproductive to cover here. It may have created an appetite to you to become more compliant or reconsider some factors either as a controller, as a processor, or personal data. However, this document is not in any way considered as a legal advice. You should check with a lawyer to make sure you or your organization fully comply with the GDPR. Finally, it is highly recommended you consider speaking with an attorney specialized in GDPR compliance who can apply the law to your specific circumstances.

6. ABBREVIATIONS - ACRONYMS

UOA	University of Athens
GDPR	General Data Protection Regulation
ΕΚΠΑ	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
EU	European Union
ΕΕ	Ευρωπαϊκή Ένωση
DPA	Data Protection Act
ECJ	European Court of Justice
EC	European Commission
DPO	Data Protection Officer
DSR	Data Subject Request
DSR	Data Subject Request
DPC	Data Protection Coordinator
SMEs	Small and Medium-Sized Enterprises
US	United States of America – also known as USA
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
EEA	European Economic Area
ALISE	Association For Library Collections and Technical Services
PII	Personally Identifiable Information
FRA	European Union Agency for Fundamental Rights
SME	Small and medium-sized enterprise
EDPB	European Data Protection Board
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
DPIA	Data Protection Impact Assessment
5G	Fifth Generation
HIPAA	Health Insurance Portability and Accountability Act
eMBB	Enhanced mobile broadband

REFERENCES

[1] What is GDPR, the EU's new data protection law? - GDPR.eu https://gdpr.eu/what-is-gdpr , 2021
[2] GDPR Archives - GDPR.eu https://gdpr.eu/tag/gdpr , 2021
[3] GDPR history | Sourcing-international https://sourcing-international.org/news/article/a-brief-history-of-data-protection-how-did-it-all-start , 2021
[4] Decretum Gratiani | Wikipedia: https://en.wikipedia.org/wiki/Decretum_Gratiani , 2021
[5] Right to privacy https://en.wikipedia.org/wiki/Right_to_privacy , 2021
[6] Data Protection Act 2018 | Wikipedia https://en.wikipedia.org/wiki/Data_Protection_Act_2018 , 2021
[7] What is the Data Protection Directive? The Predecessor to the GDPR: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr , 2021
[8] International Safe Harbor Privacy Principles: https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles#:~:text=The%20International%20Safe%20Harbor%20Privacy,disclosing%20or%20losing%20personal%20information , 2021
[9] GDPR history | EDPS.Europa https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en , 2021
[10] EU-US Privacy Shield https://en.wikipedia.org/wiki/EU%E2%80%93US_Privacy_Shield , 2021
[11] GDPR Territorial scope Art. 3: https://gdpr.eu/article-3-requirements-of-handling-personal-data-of-subjects-in-the-union , 2021
[12] Does the GDPR apply to companies outside of the EU: https://gdpr.eu/companies-outside-of-europe , 2021
[13] What are the GDPR fine | GDPR EU: https://gdpr.eu/fines , 2021
[14] EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG , 2021
[15] What is GDPR, the EU's new data protection law? - GDPR.eu (europa.eu): https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en , 2021
[16] GDPR compliance checklist - GDPR.eu https://gdpr.eu/checklist/ , 2021
[17] Data Protection Officer (DPO) | European Data Protection Supervisor (europa.eu) https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en , 2021
[18] Fines / Penalties | General Data Protection Regulation (GDPR) (gdpr-info.eu) https://gdpr-info.eu/issues/fines-penalties/ , 2021
[19] Technology company - Wikipedia https://en.wikipedia.org/wiki/Technology_company, 2021
[20] 5G, explained | MIT Sloan https://mitsloan.mit.edu/ideas-made-to-matter/5g-explained, 2020
[21] Enhanced Mobile Broadband — 5G Innovation for consumers? - Qualcomm Developer Network: https://developer.qualcomm.com/blog/enhanced-mobile-broadband-5g-innovation-consumers , 2021
[22] European Cybersecurity Month 2020: Time for clarity on 5G, security and privacy in the "new normal" | European Data Protection Supervisor (europa.eu) https://edps.europa.eu/press-publications/press-news/blog/european-cybersecurity-month-2020-time-clarity-5g-security-and_en
[23] GDPR Interference With Next Generation 5G and IoT Networks | IEEE Journals & Magazine | IEEE Xplore https://ieeexplore.ieee.org/document/9110555
[24] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence - Think Tank (europa.eu) https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530 , 2020
[25] Technology firms vie for billions in data-analytics contracts | The Economist https://www.economist.com/business/2019/09/05/technology-firms-vie-for-billions-in-data-analytics-contracts, 2019
[26] EPRS_STU(2020)641530_EN.pdf (europa.eu): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf , 2021
[27] Privacy and Data Protection Policy (uoa.gr): https://en.uoa.gr/fileadmin/user_upload/main_uoa_images/to_panepisthmio/Data_Protection_Policy_EKPA_en.pdf , 2019
[28] What are the main aspects of the General Data Protection Regulation (GDPR) that a public administration should be aware of? | European Commission (europa.eu) https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en, 2021

[29] What are the main aspects of the General Data Protection Regulation (GDPR) that a public administration should be aware of? | European Commission (deloitte.com) https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-in-the-public-sector.html , 2021
[30] GDPR is for Public Sector Organizations Too | AWS Public Sector Blog (amazon.com): https://aws.amazon.com/blogs/publicsector/gdpr-is-for-public-sector-organizations-too/ , 2021
[31] Ecommerce in Europe - Ecommerce News https://ecommercenews.eu/ecommerce-in-europe/#:~:text=E-SHOPPERS%20%E2%80%93%20Data%20from%20Eurostat%20shows%20that%2032,percent%20ordered%20from%20sellers%20from%20other%20EU%20countries, 2021
[32] Legal regulations for e-commerce | Internal Market, Industry, Entrepreneurship and SMEs (europa.eu) https://ec.europa.eu/growth/sectors/tourism/business-portal/understanding-legislation/legal-regulations-e-commerce_en , 2021
[33] Your rights matter: data protection and privacy (europa.eu): https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf , 2021
[34] Enforcement Tracker https://www.enforcementtracker.com/, 2021
[35] Brexit | European Commission (europa.eu) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en , 2020
[36] UK to overhaul privacy rules in post-Brexit departure from GDPR | GDPR | The Guardian https://www.theguardian.com/technology/2021/aug/26/uk-to-overhaul-privacy-rules-in-post-brexit-departure-from-gdpr, 2021
[37] Press corner | European Commission (europa.eu) https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166 , 2020
[38] How Tech Culture Has Changed Since The GDPR (forbes.com) https://www.forbes.com/sites/julianvigo/2019/05/05/how-tech-culture-has-changed-since-the-gdpr/, 2019
[39] Executive summary | GDPR Enforcement Tracker Report | CMS: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/executive-summary2 , 2021