# GDPR & DATA PRIVACY: IMPACT OF DATA PROTECTION IN IRISH SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)

Research dissertation presented in partial fulfilment of the requirements

for the degree of

**MSc in International Business and Law**

Griffith College Dublin

Dissertation Supervisor: **Sana Khan**

**FALAYI PRETTY OLAWUNMI**

29th May 2020

## Candidate Declaration

Candidate Name: FALAYI PRETTY OLAWUNMI

I certify that the dissertation entitled:

**"GDPR & Data Privacy: Impact Of Data Protection in Irish Small and Medium-sized Enterprises (SMEs)"** submitted for the degree of: MSc in International Business and Law is a result of my personal effort and that where reference is made to the work of others, due acknowledgment is given.

Candidate signature: FALAYI PRETTY OLAWUNMI

Date: 29th May 2020

Supervisor Name: SANA KHAN

Supervisor signature:

Date:

## Acknowledgements

I would love appreciate God Almighty for granting me the strength and grace to complete this dissertation. He is my divine source that guided me throughout this dissertation. I would like to acknowledge my parents Dr. & Mrs. O.H. Falayi and my siblings for their immense financial support, prayers, love and giving me this opportunity, may God keep you to enjoy the fruits of your labour. Thank you Mummy and Daddy!

I also acknowledge my number one supporter, critic, other half and forever love, my husband Dr. Oluwaseun Omosehin for your unwavering support, love, and prayers, I love you. I certainly acknowledge my parents in love Pastor & Pastor (Mrs.) Omosehin for their continuous love and prayers, may God continue to strengthen them immensely.

I acknowledge my friends and classmates in MSc International Business and Law and all my other friends in Griffith College Dublin and Nigeria, my immense appreciation to you all for your encouragement and contribution towards my dissertation.

I also acknowledge my supervisor Sana Khan for her constant guidance and supervision towards the success of this dissertation. Thank you, Sana!

## Abstract

Data privacy and protection is a concept which is developing due to the fast-paced evolution of information technology. The substantial reliance on technology especially due to the COVID-19 pandemic has peaked considerably. However, data protection laws such as the General Data Protection Regulation (GDPR) is enforced to issue penalties in the event of any data breaches. Since the enforcement of the GDPR, all businesses have been mandated to implement the guidelines into their operations. However, the focus for the GDPR implementation and compliance have been majorly on large companies who are high regulators of data collection, processing, harvesting and storage. These large companies have contributed to a series of data breaches and violation of data privacy and protection laws put in place to curb such occurrences.

The question therein lies about the state of implementation and compliance of small and medium sized businesses in Ireland. There is minimal attention on Irish SMEs to implement and comply with the GDPR. This study focuses on the impact, challenges and compliance of Irish SMEs in relation to data privacy and protection. It explores the importance of cyber and digital security to these businesses in relation to securing the personal data of their customers, employees and the business. It also portrays the opinions of the Irish SMEs about the General Data Protection Regulations and its relevance to their business operational standards. This study also presents the data analysis and findings derived from the interviews granted by willing Irish business representatives, managers and owners. It shares their perspectives and what they have experienced with the GDPR implementation and compliance. These perspectives were critically examined and evaluated for the purpose of this study.

## Table of Contents

## List of Figures

# CHAPTER ONE

## 1. INTRODUCTION

### 1.1 OVERVIEW

Over three decades have elapsed since the of initial communications were disseminated over a growing global network, currently known as *the Internet*. During that period, a minority of the general population anticipated the Internet's expansive growth and constant intrusion into our private, social, and professional lives. The internet has created the possibility for many voices and expanded their reach, its decentralized power has also threatened the governing authorities and they have introduced measures to control this anarchic network (Spinello, 2006, p.1).

Small and medium sized businesses are influencing the international business environment and constitute a significant part of the backbone of the EU economy. They promote competitiveness, and investments of the Digital Single Market (DSM). SMEs are consistently dependent on Information technology (IT) networks, systems, and applications to maintain an online presence and provide online services to their customers. They invest in the services of third party technology companies/experts to establish their own technology infrastructure such as Internet of Things (IoT) applications and cloud computing services (European Union and Agency for Network and Information Security, 2016). Due to this SMEs have access to collect, process, and store the data of their customers as well as continuous use of this data in their daily business operations.

The General Data Protection Regulation (GDPR) is a set of data protection rules for all registered companies, organizations and businesses operating in the EU, wherever they are based. It is the law (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and rescinding Directive 95/46/EC (General Data Protection Regulation). It was adopted in April 2016 and implemented as of May 2018, it replaced the 1995 Data Protection Directive (European Union, 2019). Before the GDPR was implemented, several small and medium-sized businesses did not have the resources or expertise to contract the qualified personnel to handle and fully reorganize their business operations in adapting to the data protection standards. The precedence set out for implementing the GDPR in small and medium-sized businesses were high and complex (Jackson, 2018). The embedding of the GDPR regulations requires proactive planning that

accommodates the business operations of small and medium-sized Irish businesses (Goddard, 2017). This research explores the extent of GDPR since its adoption on data privacy, protection, compliance, technology and the negative or positive impact in small and medium-sized Irish businesses (SMEs). The General Data Protection Regulations (GDPR) highlights several definitions in its articles and some of which are being used contextually in this research include:

- **Personal data** is any information that relates to an identifiable or identified natural individual (i.e. data subject), this identifiable natural individual can be identified directly or indirectly, distinctly by reference to an identifier such as a name, identification number, location data, an online identifier, or more than one distinct factor to physical, psychological, , economic, genetic, mental, social and cultural identity of that natural individual.
- **Profiling** is any set up of automated processing of personal data comprising of the use of personal data to assess certain personal characteristics relating to a natural person, in particular to evaluate or predict aspects concerning that natural individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Processing** is an operation or series of operations that is conducted on personal data or on collections of personal data, either or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, distribution or otherwise making available, alignment or combination, restriction, deletion or destruction.

- A **Controller** is the natural or legal individual, public authority, agency or other body, alone or collaborating with others, that determines the motives and means of the processing of personal data; where the motives and means of such processing are determined by Union or Member State law, the controller or the distinct criteria for its nomination may be provided for by Union or Member State law
- A **Processor** is a natural or legal individual, public authority, agency, or other body which processes personal data on behalf of the controller
- **Consent** of the data subject is any freely given, distinct, informed and unequivocal indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, indicates agreement to the processing of personal data relating to him or her
- **Personal data breach** is a violation of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- **Genetic data** is personal data pertaining to the inherited or acquired genetic features of a natural individual which offers unique information about the physiology or the health of that natural individual and result, distinctly from an analysis of a biological sample from the natural individual in question.
- **Biometric data** is personal data resulting from distinct technical processing relating to the physical, physiological, or behavioural features of a natural individual, which allow or affirm the unique identification of that natural individual, such as facial images or other biometric data.

- **Enterprise** is a natural or legal individual involved in an economic activity, disregarding its legal form, including partnerships or associations regularly involved in an economic activity.

(GDPR.EU, 2018).

## 1.2 RESEARCH PURPOSE

The purpose of this study is focused on small and medium-sized Irish firms/businesses as an integral part of the economy striving to grow their businesses with the use of technology and innovation such as web and online applications, planners, social media platforms, cloud storage including a plethora of continuously sprouting and evolving platforms. The background of the General Data Protection Regulation (GDPR) and other related technology concepts are examined to determine how small and medium-sized Irish businesses cope with ethics and compliance issues while exploring if these issues contribute a regulatory burden to their business operations.

Their opinions about GDPR, its implementation and how it impacts data privacy, protection, and cybersecurity in their business operations. These opinions from the selected small and medium-sized Irish businesses will give insight to how the implementation of the GDPR has impacted their business operations and if the impact has been a positive or negative reinforcement to the business. It also gives insight to the level of compliance and ethics employed to ensure their customer data is protected. While portraying their opinions via interviews conducted with the representatives of the selected small and medium-sized Irish businesses.

The research also studies the various roles technology and innovation play in these businesses and its significant contribution to growth in their business activities. Technology and innovation have evolved overtime and improved the means of data collection via several platforms. The phenomenon of data collection and privacy has allowed for easier communication and processes in different sectors of business and society, these technological processes has evolved to help the development of small-medium sized businesses and allowed entrepreneurs to grow their businesses with the aid of web and online applications that help the businesses grow and evolve with the trends steadily.

## 1.3 SIGNIFICANCE OF THE STUDY

The essence of this study is to examine the impact of GDPR, data privacy and protection on small and medium-sized Irish businesses. In this study I would closely examine the GDPR and some of its proponents (information technology and innovation). Taking into cognisance the data breach scandals that have emerged such as the Cambridge Analytica data breach in 2018 and more recently the data breach

that developed during the COVID-19 pandemic with Zoom Video communications in 2020. Considering these notable data breaches and their implications on its consumers despite the implementation of data regulations, it has become more imperative to also assess how GDPR, since its inception has been affecting small and medium-sized Irish businesses. Usually the focus of data breaches is mainly on the big corporations or multi-national companies, this study would unveil the importance of the GDPR and the indicated issues by highlighting the struggles of the other players in the economy while eliciting its impact on the consumers.

One of the objectives of the General Data Protection Regulation is to refine and improve how businesses view and control the individual data of EU nationals. It aims to regulate how data is collected and controlled to improve cybersecurity in the European Community by putting consequences of non-compliance in place (Sirur *et al.*, 2018). The role of small and medium-sized businesses in Ireland cannot be overlooked when it comes to the services they offer and the technology they use to operate their businesses. The General Data Protection Regulation are a set of regulations to be adhered to by every sector of business in the European Community whether small, medium or large and it is important to take into cognizance the impact that these regulations have on SMEs in Ireland. Data protection is currently one of the most discussed and debated topics in information technology and innovation, cybersecurity is also another subject matter that is relevant to data protection. The role of information technology and innovation in the society today cannot be underestimated therefore it is vital importance to study a sample of Irish SMEs and their opinions about the impact of GDPR and data protection to their businesses. It is also quite important to this research to discern the role of cybersecurity and data protection in different aspects of their business operations as well.

This study would be exploring empirical literature from different disciplines such as data protection, privacy, retention, the General Data Protection Regulations, regulatory burden, cybersecurity, and Small/medium sized enterprises in Ireland.

### 1.4 RESEARCH OBJECTIVES

The main objectives of this study are:

1. To examine the impact of the General Data Protection Regulation on Irish SMEs.
2. Evaluate compliance of Irish SMEs in ensuring data protection and privacy of their customers.
3. To explore the challenges Irish SMEs experienced or are still experiencing with implementing the General Data Protection Regulations in their business

This research question extracted from the objectives above is **'What are the impacts of the General Data Protection Regulations, Data Privacy and protection on Irish SMEs?'.**

### 1.5 STRUCTURE OF THE STUDY

The structure of this study is comprised of five parts and outlined below:

Chapter One is the introductory section that gives an overview of the study, purpose of the research, significance of the study, research objectives that lead to the research question and the structure of the study.

Chapter Two portrays a deeper insight to the study by providing the literature review of previous journals, papers, articles that addresses the GDPR, technology, innovation, cybersecurity, data protection and privacy and the governing bodies in charge of ensuring proper compliance. This chapter also has the conceptual framework of the study.

Chapter Three of this study is the research strategy and methodology that gives the detailed explanation of the research philosophy and approach. It also highlights the method of primary data collection and the approach used for data analysis of the study.

Chapter Four describes the presentation and discussion of findings discovered during the study. The primary data collected has been analysed and interpreted to depict the connection between the literature review, conceptual framework, and findings.

Chapter Five concludes the study by focusing on the research implications, limitations, contributions, reflections, conclusions and recommendations for practice and future research.

# CHAPTER TWO

## 2. LITERATURE REVIEW

### 2.0 OVERVIEW

The evolution of technology has gone through various phases from the discovery of the internet, inception of social media, artificial intelligence, Internet of Things (IoT) and cloud technology. These factors have breached the communication gap with technological devices such as computers, smartphones, and smart devices subsequently turning the world into a global village. Individuals are continuously evolving, creating new ways to flow and comply with technological trends. Naturally, there are the downside effects of technology that trigger the implementation of policies to curb the damage done or limit other negative reoccurrences. However, studies have shown that the build-up tends to be ignored and overlooked until a drastic negative event occurs to trigger these principles and policies to be set up and enforced. This raises the question about the impact of the regulations set up for businesses. Indubitably, more challenges would arise as technology continues to evolve therefore it is crucial to consider the compliance of how businesses integrate data protection into their operations.

The effect of cyber-attacks on databases regardless of the business size is also crucial to highlight and understand the initiatives that businesses adopt to protect data and information stored in their database (Usman *et al.*, 2019, p. 5). Security and privacy of data are especially important for proper management, storage, and protection of data in businesses. Technology has provided a platform for various applications varying from low, medium, and high standards of security to be used by businesses. The question therefore arising is if the business has the capability to adopt the technology best suited for their business in terms of cybersecurity and data protection (Wilner, 2018, p. 309). This research will highlight the studies that have touched on the various subjects of the General Data Protection Regulation, data protection, privacy, cybersecurity, and how the small and medium-sized Irish business players are adapting from the implementation of the regulation to recent times. Data and information privacy encompass the emerging relationship between businesses, technology, artificial intelligence (AI), cyber and digital security. In other words, the business world of today has no option than to use technology in more ways than one to run a business. Whether it is using hardware such as computers, laptops, IT rooms

or software applications like the internet, websites, cloud storage, could computing, and company database that is used in its daily operations. Any business regardless of its size deals with data and information that requires security levels of access and protection from loss, damage or attacks (Wilner, 2018, p. 312).

Using the case of the political "Cambridge Analytica Scandal" 2018 that caused a major technology breach and caused a major ruckus, especially in the European Union. According to an article in The Guardian (International Edition, 2019), the after-effects of the scandal has brought about promises of improving the data privacy and protection of its users on Facebook, WhatsApp messenger and Instagram. However, the critics from privacy experts is that the improvement has little to do with protecting privacy and everything to do with protecting market share (Wong, 2019). It raises a concern if the largest players in the tech world can barely handle this kind of data breach then what the small businesses who also handle data collection and storage on different levels from their local customers.

The outbreak of COVID-19 and its development into a global pandemic has ushered further concerns that has made organisations implement extraordinary measures to safeguard employees, customers, and others against the posed health threat. Due to these measures, organizations have created applications to collect and process additional data about display of the virus symptoms, health status within a household, results of COVID-19 tests and the different locations these individuals have visited since the pandemic outbreak for contact tracing. This additional data being collected are classified as personal data or special categories of personal data (SCD) and subject to strict European Union (EU) compliance requirements imposed by GDPR (El-Leithy, 2020). A data protection impact assessment (DPIA) should be considered before any personal data or SCD is collected and processed. A data protection impact assessment (DPIA) is a process that was created to identify and reduce the risks associated with data collection and processing. This documentation informs the organization about any changes that are required in data protection compliance such as records of processing activities, privacy notices, etc. The GDPR mandates that organizations engage a DPIA if there is high risk associated to the data rights and freedom of individuals. This guide provided by data protection regulators suggest that a DPIA should be carried out where data processing activity involves genetic, tracking and/or data. Where DPIA is not obligatory organizations should endeavour to ensure all risks are identified and reduced (European Union, 2019).

### 2.1 Data Privacy and Protection

Enormous amounts of personal data are generated daily and most times this data is processed without value for privacy. Technology and innovation are the bane of the world's current daily cycle, even the minuscule details of personal data like using the alarm settings on a smartphone documents the sleep pattern of an individual (Sharma, 2019, p. 5). Other examples of personal data being stored are customized playlists on music apps, dating apps, banking apps, card payments/swipes, twitter posts, online/social media newsfeed, taking pictures in locations, and weather forecasts. Even the use of taxi apps to transport from one place to another records previous locations visited and ordering your favourite coffee from the shop leaves a digital footprint. An immeasurable amount of personal data is generated every second per minute in a day we use or rely on technology and most times the data is collected or processed with or without awareness or permission (Sharma, 2019, p. 5).

Privacy can be defined as a state of being alone, safeguarded from intrusion, liberty from public scrutiny, ability to make important decisions as a right, freedom of thought or authority over one's body or information (Kaan, and Ho, 2013). As individuals we have the inherent desire to share information, but at the same time we value our privacy or at least value the freedom and control to decide with whom or when to share information. Private information is shared personally and professionally in distinct conditions and a certain level of trust. Privacy is not a new phenomenon, however in this era of technology and innovation the ease of information circulation, enables anyone with a smartphone, tablet or laptop become an identifiable or anonymous virtual publisher. Technology and innovation provide the freedom of individual opinion and seamless communication with commercial services that provide immense comfort to our daily lives (Sharma, 2019, p. 15).

According to Sharma (2019), in 1960 a tort law scholar William Prosser outlined four main privacy torts which were based on cases in Warren and Brandeis article. The four main privacy torts are:

- Public disclosure of private facts- This describes disclosing the private issues of an individual that is not for public knowledge and considered highly impudent by the individual concerned.
- Publicity and false light- This means creating a false impression (false light) in disclosing private issues of an individual that is highly impudent and with little or no regard to the inaccuracy of the information disclosed.

- Intrusion upon seclusion- Deliberate trespassing into the private and secluded issues or business in a way that is highly impudent to a rational individual.
- Appropriation- Deliberate use of an individual's image or personality for personal advantage.

These privacy torts are the bedrock for the violation of personal privacy rights and following legal measures (William Prosser, 1960 cited in Sharma, 2019 p. 25). The EU Convention on Human Rights (ECHR) also echo fundamental human rights which are the ***right to a private life:*** which means that no individual should be subject to arbitrary intrusion into his/her private issues, family, correspondence or suffer any attacks to his/her reputation and ***freedom of speech and expression*** which is the right to convey one's perspective without any intervention and the ability to seek, communicate, and receive information through any media setting aside any limits or boundaries (Sharma, 2019, p. 35)

Data privacy is a concept that developed in the late twentieth century with the evolution of the internet and information technology. The parameters of disclosing information depends on the relationship we have (formal and informal) and how much trust we have in those associations (Sharma, 2019, p. 20). This means that there is a fiduciary duty from the entities with whom information or personal data is shared with across all platforms. In situations like this, sharing information is required and we innately trust the data collectors with personal data. In this technological era, an expansive framework should be created to ensure the release, sharing and use of personal data is discreet and transparent. Hence the laws created and enforced against preconceived and illegal use of personal data (Sharma, 2019, p. 40). Plausibly, it is still quite easy to obtain and distribute personal data despite the regulations that try to avert and penalize disclosure of personal data without the consent of the data subjects involved (Kaan, and Ho, 2013). A considerable portion of harm stems from inadequate implementation of proper data processing for authorized purposes. The evolution of technology is continuously developing new forms of potential threats that can emerge from the abuse of personal data. The reality of these threats being discussed under data privacy does not infer that the current countermeasures used to protect data breaches can be relied on to deter future threats (Leenes *et al.*, 2017).

The data protection law is based premise that it is realistic to separate information into personal and non-personal, and then to control the use of personal data in specified ways (Kaan, and Ho, 2013, p. 41). According to Recital 2 of the GDPR, *"the principles and regulations seeks to protect natural persons with regard to the*

*processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data"* (European Union, 2018). Despite data protection regulations or laws in these technological times, it is easy to obtain, share, store, transfer, publish, manipulate and mine large amounts of data causing devastating data breaches as seen over the years. A possible reason that data protection laws do not safeguard or prevent breach of data privacy is partially because it accommodates some parts of the European Convention of Human rights of ***transparency/openness*** and ***freedom of expression*** in public and business aspects. The accommodation of these rights occasionally compromises or limit the objectives of data protection regulations (Kaan, and Ho, 2013). Since the data breaches experienced by the Cambridge Analytica Scandal in 2018, the GDPR regulators have handed out numerous fines to organisations such as Facebook, Google, WhatsApp, among others. According to Article 97 of the GDPR, the European Commission is charged to release a public report on May 25, 2020 and every four years afterwards evaluating the GDPR, its progress, challenges experienced and review any reforms to be made due to any challenges (Kearney, 2019).

### 2.1.2 Digital Security, Cloud Computing, Secure Technology & Innovation

The attack on cloud-based applications and the hostile capabilities like data re-identification (also known de-anonymisation) apply increased pressure on secure innovation and proper data protection management. Technologies that provide obfuscation or anonymisation of data to assume the integrity of the data subject produce fragmentary protection against data breach. There are several alternate technologies that can be used to hack or bypass the firewalls set up to protect data linkage to the data subjects. Some organizations or businesses want to unlock the prospective value of data by regenerating it within the cloud and thereby developing a massive process of data integration (Munn *et al.*, 2019, p. 2). Technology has also introduced the innovation of cloud computing and artificial intelligence in data privacy. This cloud computing is a virtual domain where resources and applications are distributed on demand over the internet as services. It supplies a suitable on-demand network access to a shared pool of programmable computing resources that refer to network services, computing applications, software servers, software services, virtual servers, and other computing facilities (Sun *et al.*, 2014, p. 1).

The main software services considered in cloud computing are ***Platform as a service (PaaS), Software as a services (SaaS)*** and ***Infrastructure as a service (IaaS).*** These services are employed by cloud service providers for features that their users access

through web browsers. Cloud computing facilitates services to be consumed on demand. It has features such as extensive network access, independent location facility pooling, on-demand self-service, rapid resource elasticity, use-based pricing, and conversion of risk. The benefits of cloud computing continue to attract considerable interests from the scholastic research world and commercial world, its technology is fast changing the methods of the business world. Despite the attractive features of cloud computing technology and its applications, there are issues related to the storage and deployment of consumers and enterprise data. The fundamental issues include adopting high data security, data privacy, compliance, data protection, resource management, security and monitoring (Sun *et al.*, 2014, p. 3).

Artificial Intelligence (AI) has shown enormous potential and can analyse a substantial volume of data highlighting trends and insights that are being ignored or missed and providing recommendations on how to improve or update software for secure innovation. It is highly instrumental for proper storage of data, digital security and secure innovation, this means that AI can also detect any suspicious activity and alert the data analysts for further investigation. For this to be effective, data research analysts use other AIs as a ruse to test the effectiveness of the AI cyber-detection competencies and then develop new versions of malware that provide a stronger protection against cyber-attacks. The future of data privacy and secure innovation is more investment in Artificial Intelligence infrastructure because as technology evolves and alter its patterns so does the approach to ensuring better cybersecurity in innovation (Wilner, 2018, p. 314).

### 2.1.3 Data Protection in Ireland and the European Union

The conception of data privacy and protection legislation or laws in Europe was influenced by the European Convention on Human Rights (ECHR), the *right to a private life* in Article 12 and *the right to freedom of expression* in Article 19 were stated as the fundamentals of privacy as seen in previous literature above. The timeline for European data protection is outlined below:

- In the 1960s, there was the economic and technological advancements, increase in international trade, telecommunications and `the utilization of computers.
- In the 1970s the development of communication technology included the establishment of substantial banks of personal data and new opportunities for international data processing. There was also the dissension between international free trade and national privacy rights.

- Earlier in the 1980s two important data protection initiatives were launched, the Organization for Economic Cooperation and Development provided guidelines on the Protection of Privacy and Transborder flows of Personal data (OECD Guidelines). These guidelines focused on easing data flows and protecting personal data in a global economy, they were improved in 2013 to include data protection principles. The Council of Europe Convention also called Convention 108 was open for signatures in 1981 and became the first data protection tool for several European council member states. It was different from the OECD guidelines and needed signatories to petition the principles of Convention 108 in their domestic legislation. Difficulties with the Convention 108 were becoming visible in the late 1980s, only a few states endorsed it and applied a disintegrated approach.
- In 1990, the European Commission recommended the introduction of a dedicated directive. The Convention 108 principles were used as the bedrock for the EU Data Protection Directive (95/46/EC), the directive set out general data protection principles and requirements, necessitating EU member states to convert and implement them.
- The 2000s brought the Charter of Fundamental Rights of the EU proclaimed by European Union institutions. It is an inclusive collection of individuals' rights, including the fundamental right to the protection of personal data. Adopted in 2002 and revised in 2009, the EU Directive on Privacy and Electronic Communications (e-Privacy Directive) is legally binding on EU member states and mandates domestic implementation. Generally, the e-Privacy Directive pertains to processing of personal data through public automated communications services and networks in the EU. The EU Data Retention Directive (2006/24/EC) was adopted in 2006 and nullified in 2014 by the EU Court of Justice. In 2009, the Treaty of Lisbon came into force. Its focus is to reinforce and improve the core structures of the EU and to help it operate more efficiently. It gave the EU Charter of Fundamental Rights full legal authorization in the European Union.
- 2010s: The General Data Protection Regulation (GDPR) became a legislation in 2016. It replaces the Data Protection Directive and became enforceable from May 25, 2018. A public report is expected to be released on May 25, 2020 about the evaluation of the GDPR, its progress, challenges experienced and any reviews from the challenges.

(Khan, 2020).

Data protection in the European Union has required Member states to describe national provisions in a way that respects the minimum standards of data protection

when maintaining data. The European Union's objective to improve data privacy rights, area of freedom and data security of individuals is not a straightforward or simple process (Galli, 2016). Before the implementation of the General Data Protection Regulations, the Data Protection Directive were a set of directives that were set up for the purpose of data privacy and protection in the European Union. Some studies have reflected that the General Data Protection Regulation deemed as an upgrade from the previous data protection directives are not enough to deal with the continuous evolving technology (Galli, 2016).

### E-Privacy Regulation, Cookies and the GDPR

According to the European Data Protection Supervisor, the e-Privacy Directive 2009/136/EC is concerned with processing personal data and privacy protection in the electronic communications division. It is an amendment of the Directive 2002/58/EC. The e-Directive has provisions that cover processing of personal data and privacy protection including:

- Access to stored data
- Confidentiality of communications
- Security of networks and services
- Processing traffic and location data
- Security of network and services
- Calling line identification
- Unsolicited commercial communications (spam)
- Public subscriber directories

Other changes added include requirements for data breach notifications, extension to cover electronic tags, strengthened enforcement rules, etc. However, the new e-Privacy Regulation (EPR) is a replacement that broadens the scope and definitions of the e-Privacy Directive (EPD). In the European Union, a regulation is legally binding in the EU from the date it comes into effect while a directive must be integrated as a national law by EU countries (EDPS, 2020).

The e-Privacy Regulation is meant to replace the current e-Privacy Directive which is the current law on the regulation of cookies in the European Union. The e-Privacy regulation proposal for privacy and electronic communications seeks to augment trust and security in the Digital Single Market (DSM) as it improves the legal framework on e-Privacy (European Commission, 2017). Information technology services are rapidly evolving and developing, the European Commission started the major upgrade of the data protection structure (e-Privacy legislation) to align with General Data Protection Regulation (GDPR) (European Commission, 2017).

The e-Privacy regulation proposal was adopted in 2017 by the European commission, the proposal contains high level privacy rules which includes:

- **New players**: the privacy rules in future would also pertain to new players providing electronic and automated communications services such as WhatsApp, Facebook, Skype and others. This would make certain that these commercial services ensure the same level of confidentiality of communications as conventional telecommunication operators.
- **More effective enforcement**: the proper enforcement of the confidentiality laws in the regulation would be the duty of data protection authorities, already in charge of the rules under the General Data Protection Regulation.
- **Protection against spam**: the proposal prohibits unsolicited electronic communications via emails, SMS and automated calling machines. Depending on national legislation individuals would either be secured by default or be able to use a do-not-call list to prevent marketing phone calls. Marketing callers would need to display their phone number or use a unique pre-fix that indicates a marketing call.
- **Simpler rules on cookies**: the provision on cookies, which has resulted in a burden of consent requests for internet users would be streamlined. The new rule would be more user-friendly and browser settings would provide for a simple way to allow or reject tracking cookies and other identifiers. The proposal also defines that no consent is needed for non-privacy intrusive cookies improving internet experience (for example, remembering shopping cart history) or cookies used by a website to count the number of visitors.
- **Stronger rules**: all individuals and businesses in the European Union would benefit from the same level of protection of their electronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the European Union.
- **Communications content and metadata**: privacy is guaranteed for communications content and metadata, for example time of a call and location. Metadata have a high privacy element and is to be anonymised or permanently erased if users did not give their consent, except the data is needed for billing.
- **New business opportunities**: When consent is given for communications data - content and/or metadata - to be processed, traditional telecommunication operators would have more opportunities to supply supplementary services and to grow their businesses. For example, they could produce heat maps

> indicating the presence of people; these could help public authorities and transport companies when building new infrastructure projects.
>
> (European Commission, 2017).

The e-Privacy Regulation (EPR) was meant to be passed in 2018 during the period the GDPR was enforced and it seems there is a delay in its implementation. This is because the Permanent Representatives Committee of the European Union Council voted down its proposal in November 2019 (Beduschi, 2019).

Cookies are tiny content files that are placed on your device by websites while surfing the web. They are processed and stored by web browsers, they have become more rampant on all websites due to the e-Privacy and GDPR. On their own cookies are harmless and perform key tasks for websites and can be simply viewed and deleted. Nevertheless, cookies can cache a massive amount of data that can possibly be used to identify a natural individual without consent. They are the key tool that advertisers use to monitor visitors online activity, that way they can target extremely specific ads based on browsing history (Munn *et al.*, 2019, p. 10). A substantial amount of data cookies stored is considered as personal data in specific situations and are subject to GDPR principles. There are three different ways to categorise cookies through their origin, duration and purpose and they are outlined below:

**Origin**

- First-party cookies**-** Just as the name describes, first-party cookies are placed on an individual's device directly by the website they are visit.
- Third-party cookies- These are the cookies that are placed on an individual's device, not by the website they are visit, but by a third party for example an advertiser or an automated analytic system.

**Duration**

- Session cookies**-** These cookies are temporary and expire once an individual closes the browser or website (or once one's session ends).
- Persistent cookies**-** This group comprises of all cookies that remain on an individual's hard drive until they deleted, or the browser automatically deletes them, depending on the cookie's expiration date. All persistent cookies have an expiration date written into their code; however, their duration varies. According to the e-Privacy Directive, they should last no longer than 12 months, but in practice, they could remain on an individual's device much longer if it is not manually erased or cleared.

(Munn *et al.*, 2019, p. 12)

**Purpose**

- Strictly necessary cookies- These cookies are necessary for an individual to browse the website and use its features, such as accessing secure areas of the site. They are the cookies that permit online stores to hold an individual's items in the online shopping cart while one shops online. These cookies would generally be first-party session cookies. Although it is not required to gain consent for these cookies, what they do and why they are essential should be explained to the user.
- Marketing cookies- They are cookies that track a user's online activity to help advertisers deliver more related advertising or to restrict the number of times the user views an ad. These cookies can share that data with other organizations or advertisers. They are persistent cookies and almost mostly of third-party origin.
- Statistics cookies- They are also known as "performance cookies," these cookies collect data about how an individual visits a website, for example what pages were visited and which links were clicked on. None of this information can be used to identify an individual, it is all aggregated and, then anonymized. Their sole purpose is to enhance website functionalities. This includes cookies from third-party analytics services if the cookies are for the exclusive use of the owner of the website visited.
- Preferences cookies- They are also known as "functionality cookies," and these cookies permit a website to store choices the users have made in the past, like the language they prefer, what region are preferred for weather reports, or what the user name and password are so they can automatically log in.

(Munn *et al.*, 2019, p. 12)

The above mentioned are the major categories of cookies, nevertheless there are cookies that do not fit accurately into these categories or would be qualified for more than one category. The concerns or criticisms raised about the privacy risks that cookies pose are mostly about the third-party persistent advert cookies. These cookies store substantial amounts of data about users online activity, preferences, and locations. The chain of command about who could access these cookies' data are also quite complex and only heightens the possibility of abuse. Since the General Data Protection Regulation (GDPR) has been implemented, it is said to be the most exhaustive data protection legislation to be passed. However in all its 88 pages, cookies are only stated once in recital 30 (Online identifiers for profiling and identification), *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags…"* (Munn *et al.*, 2019).

Complying with the legislation that govern cookies under the GDPR and e-Privacy Directive a summary of the above stated include:

- Collect user consent before the use any cookies except strictly necessary cookies.
- Provide precise and exact information about the data each cookie tracks and its purpose in plain language before consent is received.
- Document and store consent received from users.
- Permit users to access your service even if they refuse to allow the use of certain cookies
- Make it as simple for users to withdraw their consent as it was for them to give the consent in the first place.

*Digital Rights Ireland* is a group that advocates for digital rights in Ireland and their court case *Digital Rights Ireland Ltd v Minister for Communication & Ors.* made headlines in May 2010. The case which was ruled in favour of *Digital Rights Ireland* for breach of Data Protection laws, EU law and Ireland's obligations under the European Convention of Human Rights (ECHR) (Digital Rights Ireland Ltd -v- Minister for Communication & Ors [2010] IEHC 221, 2010). This ignited arguments about data privacy, protection and retention in Ireland, in reference to the Data Retention Directive. However, its provisions were restricted to the activities of Internet Services Providers (ISPs) and did not control access to or use of data by the law enforcement authorities. At the time, it was revealed just how vague the former Data Retention Directive was and how it was being abused in Ireland by law enforcement. It also raised questions of compliance with data privacy rights and how retained data was being alleged to be used to acquit individuals suspected of serious crimes without using other means of surveillance, interception of communication and home search which could be more invasive as it refers to privacy rights. Usually law enforcement and government tend to place more value on the acquisition of substantial data evidence in handling serious crimes than protection of data privacy rights (Galli, 2016).

The awareness of data privacy and protection in Ireland has stimulated compliance with data protection regulations among all sectors from government, commercial and personal entities. The debate of data privacy and protection may not likely end soon because there is a need to adhere to the protection of human rights beyond the confines of the European Convention of Human Rights (ECHR). As it stands there is still room for improvement with compliance in data protection regulations in all sectors (Purtova, 2010).

### 2.1.4 Consumer Data Protection

As technology evolves, innovation advances in new methods of automated data capture, transference of visual, print media and the limits of personal privacy are challenged. The general populace no longer harbours reservations of their private

matters as they widely circulate and disclose videos, pictures, family history, private stories and other information across various social media networks and applications such as Instagram, WhatsApp, Facebook, Pinterest and other online platforms. In these times, privacy is no longer respected rather it is commoditized and an asset used by data collectors to generate massive revenue (Jardine, 2018). This technological era has organizations collecting and processing data as a necessity in their business operation and storing the data of their employees, contractors, affiliates and consumers or customers as the case maybe. Subsequently, the implementation of General Data Protection Regulation (GDPR) recommends that businesses should ensure consumers can use their data privacy rights. However, do the consumers have adequate knowledge of their data privacy rights and do the consumers know when a business is GDPR compliant? One of the GDPR objectives is to allow consumers control their personal data and this is achieved by businesses ensuring secure measures of data privacy and protection of their consumer data (Christian Kurtz *et al.*, 2018, p. 6). The GDPR clearly states the rights of consumers or individuals in *chapter 3 (Articles 12-23)*, a summary of these rights includes:

- The transparency about how data is being used
- Access to personal information if the owner asks for it
- The ability to request that data be deleted or corrected for accuracy
- The right to object to data processing and restrict processing
- The right to have their data provided in a standard format that can be transferred elsewhere.

(Christian Kurtz *et al.*, 2018, p. 7).

Recital 1 of the GDPR states, *"The protection of natural persons in relation to the processing of personal data is a fundamental right",* this sentence is the anchor of the regulation and a main objective striving to be achieved. In respect to digital rights, the GDPR standardizes various pre-existent rights and developed new rights for consumers (data subjects). It also develops a structure for answers to the questions below:

- What are the rights of data subjects?
- How is it explained to the consumers?
- How are the rights imposed?
- What is considered when it is being imposed?
- Under what conditions can the controllers derogate or reject to implement consumer rights?

The rapid increase in information technology makes mandating consumers data protection rights a primary responsibility for all data controllers. As stated, above

*chapter 3 (Articles 12-23)* includes the rights of data subjects (consumers) under GDPR. Controllers are obligated to follow the GDPR principles and comply with consumer rights in order to ensure data privacy, protection and increased security (Sharma, 2019, p. 55). Organizations and businesses continuously expand their efforts to collect, process and use consumer data, there is a growing concern (i.e. privacy issues) about how secure consumer data really is and the preventive measures to guard against data breaches. Data breaches intensify consumer perceptions of vulnerability and suggests that the business or organizations are not well equipped to secure consumer data due to security lapses. However, an organization's data use transparency and control offer consumers detailed information about how the business collects, processes, shares and stores their data. It also provides consumers insight about what information they give the business, how the information is being used and if any affiliates or partners have access to their data (Martin *et al.*, 2017).

In 2019, Ben Wolford conducted a series of twitter polls, to analyse how much consumers knew about their data privacy rights using the GDPR principles as depicted below:

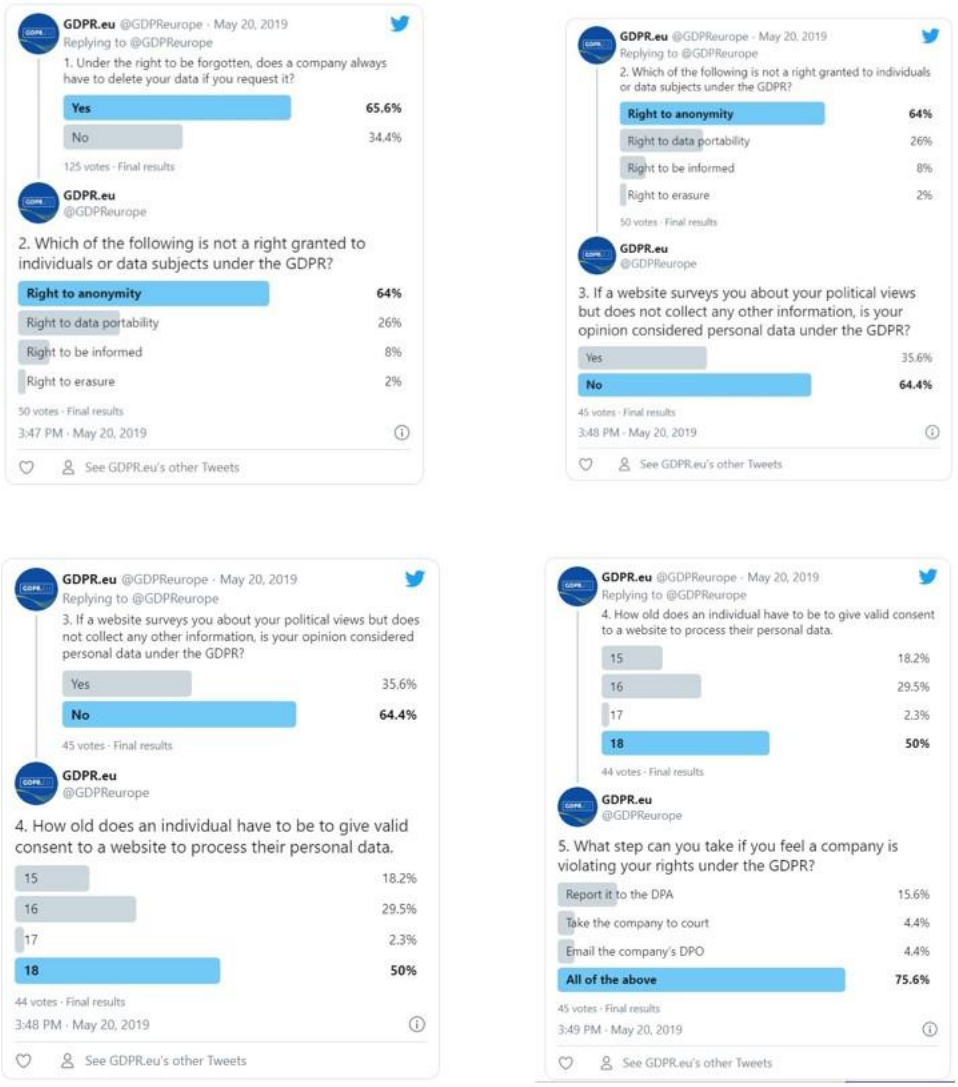



**Figure 1.1: Twitter polls: Do Consumers know their rights? (Ben Wolford, 2019)**

**(source: https://gdpr.eu/consumers-gdpr-data-privacy-rights/)**

Looking at the result of the polls, it seems that one post-GDPR implementation, several consumers and business owners still did not understand the law. The lack of awareness and knowledge among the consumers may partly be the reason SMEs do not prioritize GDPR compliance. Whereas data privacy, protection and security are very vital factors to developing a more secure cyberspace in the European Union (Ben Wolford, 2019).

### 2.2 General Data Protection Regulation (GDPR) and Cybersecurity

The General Data Protection Regulations expands the scope of data protection laws in the European Union to include all foreign businesses that handle data processing of EU residents, provide harmonization of data protection laws in the European Union and easing the process for non-European businesses to observe these regulations (Lindgren, 2018, p. 241). It constituted a change of how data collection is handled

and raised an awareness for businesses to take data privacy and protection much more seriously. However, it raises a concern about the compliance and proper implementation of these regulations in all businesses including small, medium, and large in the European community. The focus of this research is small and medium-sized Irish firms/businesses and would study the relevant literature, while highlighting the challenges that small and medium-sized Irish businesses have encountered.

Under the General Data Protection Regulation, personal data is referred to as any information pertaining to an 'identified' or 'identifiable' individual (a Data subject) and the GDPR grants privacy rights to data subjects (Loveday and Abraham, 2018). The General Data Protection Regulation gives permission to individuals to act against violation and national regulatory bodies the right to enforce fines on companies that are non-compliant. The possible impact of the implementation of the GDPR for companies or businesses that handle data collection or processing within the EU is evident. Data protection and privacy should be a company or firm's priority in order to reduce the risk of data breach and so that they comply with the GDPR guidelines and are able to continue business operations through data collection and processing (Loveday and Abraham, 2018). The GDPR also controls data management of businesses that determine the purpose and use of processing data (Controllers) and businesses that manage data on behalf of 'Controllers' (Processors). A few important requirements of Controllers and Processors under the GDPR include:

- Inform individuals of the use for which their data will be processed
- Limit processing to the use for which their data was collected except in specific conditions
- Store personal data securely
- Inform regulators and individuals in the event of any data breach

The GDPR additionally provides:

- Evident rights for individuals to require deletion of their personal data (especially if no longer necessary for the purpose it was collected), restrict the purpose and withdraw consent for processing the personal data
- Review consent as a basis of processing, with implicit consent unlikely to be adequate in most circumstances
- The GDPR also requires companies and businesses to report any breach to the affected individuals if there is a high risk of violating their rights and freedom.

(Loveday and Abraham, 2018).

The General Data Protection Regulation indicates pseudonymisation (i.e. artificial identifiers or pseudonyms) as a procedure that changes personal data in a way that the data result cannot be assigned to a specified data subject without the contribution of additional information. An example of this is encryption, it provides the authentic data as incomprehensible and it is irreversible without the access of the right decryption key. The General Data Protection Regulation stipulates that the additional information (i.e. the decryption key) be stored separately from the pseudonymised data. The recommendation of pseudonymisation is to decrease the risks to the data subjects and while aiding controllers and processors comply to the data protection regulations (Lindgren, 2018, p. 250).

Cybersecurity not only ensure the framework of data and information or safeguarding of the same. It also includes securing what we know and how we know it. It includes defending the probity of information and isolating realities from mistruths. Cyber-attacks or data breaches are often perceived as means to exfiltrate data, intellectual property and other information that is used by hackers for criminal activities or sold to the highest bidder (third party) (Wilner, 2018, p. 315). Another concern would be using the data for political propaganda which can be used for the motives of misinformation spread for strategic purposes. For example, the manipulation by Russia in the 2016 US presidential election is described to have used misinformation to influence pre-existing political, economic, and social divides within societies with the intention to threaten democracy. It is also perceived that Russia had targeted national elections in Europe (Wilner, 2018, p. 316). However, this research will study the state of cybersecurity in small and medium-sized Irish businesses and determine its importance to their business and its operations. This is because it seems, individuals or businesses with valuable digital data and information could be seen as targets for cyberattacks for example, if a ransomware or malware encrypts personal data on a computer, it prevents the victim from gaining access until a ransom is paid to the hacker (Lau *et al.*, 2018).

In this era of fast paced and evolving technology, there are high volumes of devices connected to the Internet. These devices aid to increase the performance of applications by sharing different computational and storage resources. The devices and connectivity need protection by using various cybersecurity technologies (Usman *et al.*, 2019, p. 12). Businesses utilise these devices, connections, and technology for their daily operations and most of these firms utilise different types of cybersecurity technology to safeguard their technology. Without proper cybersecurity these businesses no matter how small they seem are prone to hacks, cyber-attacks or data breaches which could jeopardize the data and storage they utilize in their daily

operations. The evolving technological applications used by businesses operate in real-time and depending on the business structure generate sensitive data. These applications require up to date protection from internal and external threats that can identify viruses, hacks and unauthorized access into their system (Usman *et al.*, 2019, p. 16). Cybercrime is swiftly evolving at the same pace with technology, it is recurrently difficult for regulations and legislations to catch up with the evolving security landscape. It results in outdated directives unfit for the purpose of curbing, controlling and managing the damage once it occurs. In business today, there is the misconception that compliance equals good business practice especially in relation to cybersecurity. The General Data Protection Regulation offers the opportunity to level the field and promote a better convergence between cybersecurity and compliance in business (Zerlang, 2017).

### 2.2.1 GDPR and Cybersecurity in Irish SMEs

The goal of a businesses is to make profit and provide quality services to its customers. The business then uses the profits realised to expand its operations and achieve other set goals which fits the business in question. Business owners must consider several internal and external factors that would affect the business and comply with these factors to run the business. Customers are also vital in the sustenance of a business and it is important that businesses provide quality service that endears its customers so as to keep them coming back. In this era of technology, businesses utilise different technological tools, hardware and software are incorporated into their business processes. Cybersecurity is essential to secure stored data in the cloud and daily updates are needed to protect against the threats of cyber-attacks while safeguarding key network-based systems (Usman *et al.*, 2019, p. 20).
As discussed in the previous sections about GDPR and Cybersecurity, this research seeks to expatiate on the impact of the General Data Protection Regulations and Cybersecurity on small and medium-sized enterprises in Ireland. In doing so, it will examine relevant literature which will aid this research and streamline its focus on the positive and negative impact experienced. SMEs are at risk of cyberattacks on their businesses if there is no adequate or up to date protection to wade off potential attacks. Imagine if the IP (Internet Protocol) of a laundry business got stolen by a hacker, this creates the possibility of pilfering personal data of the individuals that patronize the business and damages the image of the business especially in terms of issues with compliance of the General Data Protection Regulations (Opitz, 2018, p. 4). Inevitably, the business would need to adhere strictly to the regulations and pay a hefty fine if found wanting in terms of compliance and this could also ruin the image of the business. Cybersecurity should be treated and accounted for like any other

business risk, measures should be taken to mitigate and get insured against cyberattacks. Cyber insurance policies should be considered as added protection especially for businesses that handle or process customer data and payment information (e.g. debit or credit card details) (Opitz, 2018, p. 5). The General Data Protection Regulation is impressing upon businesses in Ireland to adhere to the regulation and be compliant by putting adequate measures in place and so as not be a victims of data breach (Jackson, 2018).

The General Data Protection Regulation does not place too much emphasis on data processing and information for empirical research and statistical motives. It is deemed to be more concerned with local, national, international, and foreign businesses that operate or process the data and information of the European Union residents. The implementation of the regulations has contributed to an increased workload for all sizes of businesses, departments, and employees, especially the workload of small and medium-sized Irish businesses. This increased workload is to ensure that current and obsolete data are properly secured or deleted from the business database (Lindgren, 2018, p. 245). For example, a local pharmacy store that uses a Customer Relationship Management (CRM) software to store customer data, prescriptions, habits and tastes in different products enables them to improve customer services, avoid and record customer complaints on their database whilst providing service to customer daily. They would have a sizeable amount of the elderly and special needs population as their regular customers. This population would have expectations of being provided quality services due to the pharmacy's knowledge, expertise, and other auxiliary services provided. Considering the operational hours, productivity level of the staff and the goal to continuously improve the pharmacy's services so as to keep up with their clientele demands. Data registration and processing would usually be handled by the staff with the basic training to collect customer data. However, the implementation of the General Data Protection Regulations requires that training and increased workload which reduces the productivity levels of staff and the effect on customer service delivery could decrease sales and patronage (Lindgren, 2018, p. 252). The point to drive home from this example is that the General Data Protection Regulations in one way or another affects the process of how small and medium-sized businesses handle their business operations and provide customer satisfaction. Especially in terms of expenses, workforce, culture, business processes and operations (Lindgren, 2018, p. 254).

### 2.3 General Data Protection Regulation (GDPR) Implementation & Compliance: Regulatory Burden?

Since the implementation of the General Data Protection Regulation (GDPR), there has been a significant change with how businesses handle their consumer data. However, the implementation of GDPR in different sectors across organizations and businesses is handled at different paces. This is dependent on the resources that a business possesses to transition or upgrade its technological facilities for total GDPR compliance. Most SMEs do not possess the finances or human resources to employ the IT applications or solutions for data privacy and protection. In several cases, most SMEs are dependent on using end-to-end encrypted services that secures the business's data and limits access to only the business owner (Mortleman, 2018). There are some technical measures that a business sets up to ensure there is standard for being GDPR compliant and they are:

- Employing an assigned and well-trained team to deal with consumer requests. The team would be licensed to implement GDPR and report to the Data Protection Officer (DPO) or team lead.
- Requests would be classified according to levels of priority and rectify execution of these requests.
- A standard response would be set out and given to consumers in accordance with the GDPR principles.
- Processing code of ethics would be authorized to manage specific consumer requests and objections. The authorized code of ethics sets the standard criteria of how consumer requests are handled.
- A standard protocol of processing activity should be set up for data breach and the steps to inform the consumers involved.
- Any unusual or controversial requests should be communicated and handled directly by the Data Protection Officer
- All automated procedures should be subject to routine maintenance and systematic upgrade

(Sharma, 2019, p. 76).

The implementation of GDPR in the EU has most businesses reviewing their digital security and third-party data processing agreements to ensure data privacy and protection of their consumers. In addition to the technical measures above, *Chapter 4 (Articles 24-43)* of the GDPR provides the responsibilities of all data controllers and processors. Although compliance with the GDPR is not unequivocal, businesses still need to apply the rules of GDPR encryption, security and standard GDPR agreement for data processing with the affiliates of a business (Matzner *et al.*, 2016).

These GDPR compliance steps are quite cumbersome but they are very essential to prevent the fines or penalties that could be issued due to non-compliance (Matzner *et al.*, 2016).

A survey conducted by GDPR.EU in May 2018 on 716 SMEs in France, Spain, the United Kingdom, and Ireland to determine compliance since GDPR implementation revealed the following information:

- About 36% of the SMEs that participated in the survey are really GDPR compliant while most of the GDPR decision makers believe they are completely GDPR compliant.
- As regards *Article 12* of the GDPR i.e. transparent information, communication, and procedure for the exercise of data subject rights: 44% "completely agreed" that their business clearly inform the consumers about their data processes, 33% "somewhat agreed", while 9% were "neutral".
- As regards obtaining consent from the data subjects and lawful processing *Articles 6 & 7* of the GDPR, 44% of the survey respondents were not too confident about obtaining consent or could establish lawful reasons before using consumer data.
- Responses to *Article 32* of the GDPR about processing security revealed that several of the survey respondents were unclear, oblivious, or used contractors for compliance, 22% indicated that they did not use any technical measure to protect their consumer data, while a few indicated they understood and were compliant with encryption, pseudonymization and anonymization.
- 86% of the survey respondents indicated that it is vital to be GDPR compliant, while some respondents revealed other reasons such as ***because it is the law, its good business to protect consumer data, they did not want to be fined,*** and some indicated ***they believed in the right of data privacy.***

(Ben Wolford, 2019).

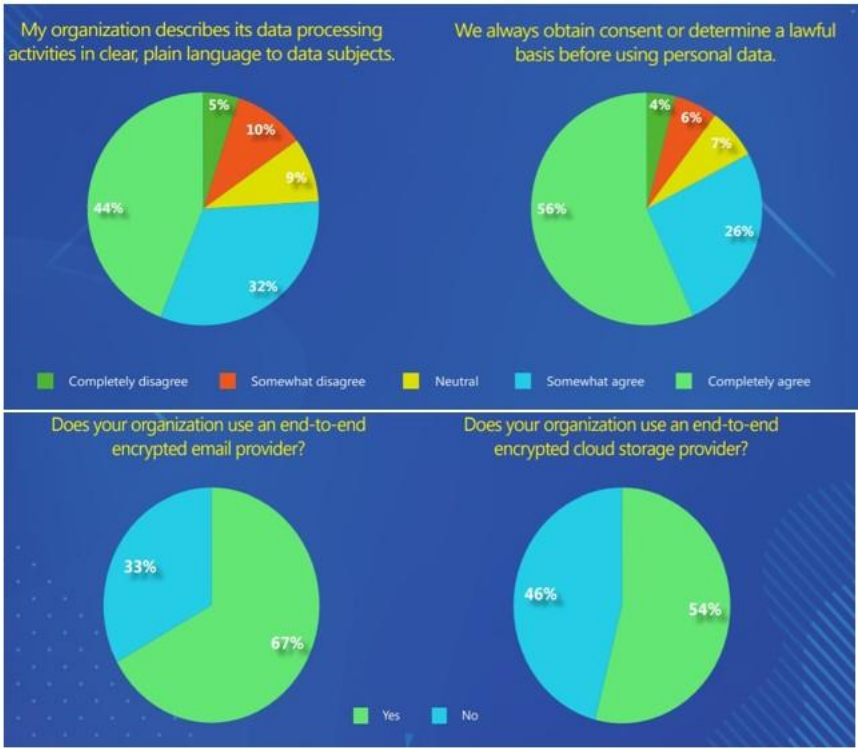



Figure 1.2: Millions of small businesses aren't GDPR compliant, our survey finds (Ben Wolford, 2019). (source: https://gdpr.eu/2019-small-business-survey/)

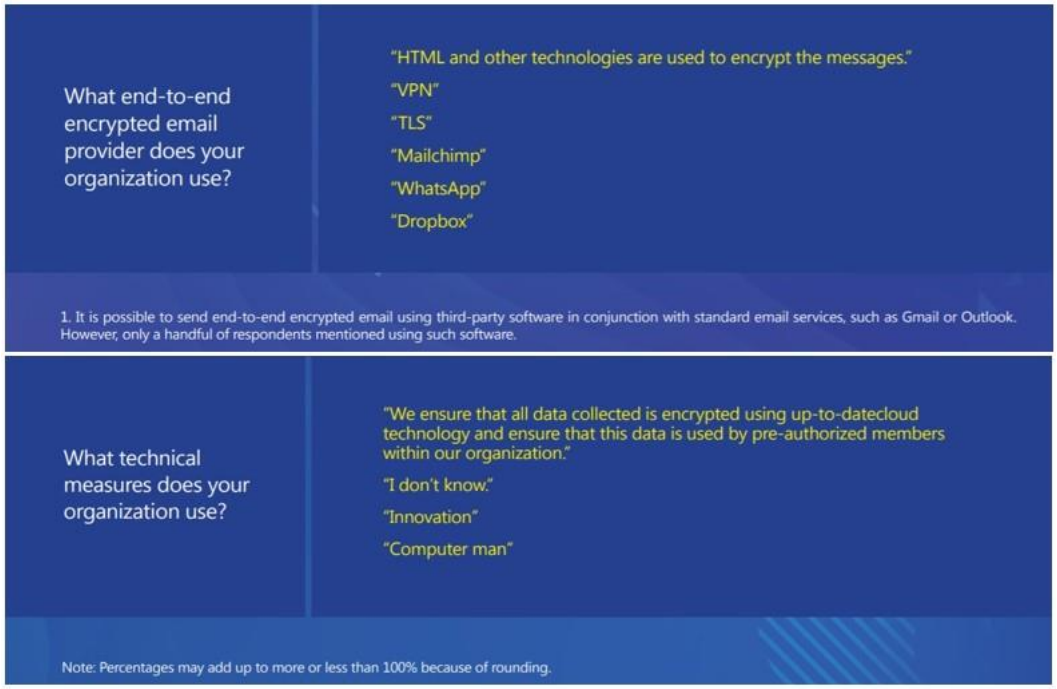



Figure 1.3: Millions of small businesses aren't GDPR compliant, our survey finds (Ben Wolford, 2019). (source: https://gdpr.eu/2019-small-business-survey/).

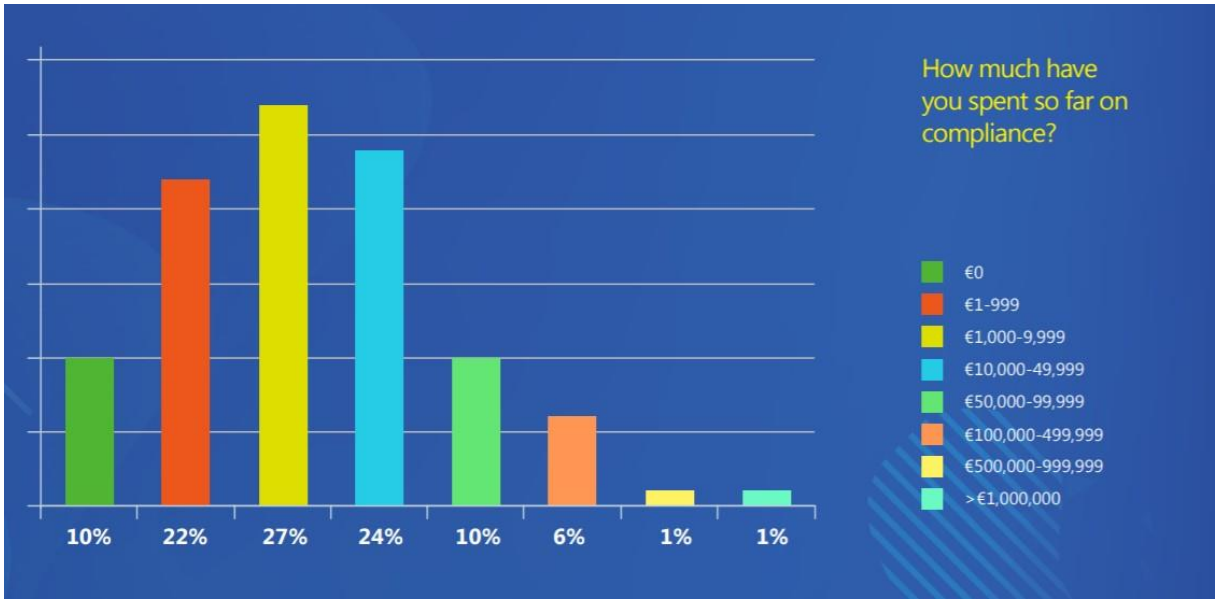



**Figure 1.4: Millions of small businesses aren't GDPR compliant, our survey finds (Ben Wolford, 2019). (source: https://gdpr.eu/2019-small-business-survey/).**

The survey report reveals compliance of the GDPR from the perspective of small and medium-sized businesses, a year after its implementation in the European Union. These SMEs have faced significant issues with GDPR compliance due to their limited financial budgets. However, they cannot afford the GDPR penalty and therefore they need to adhere to the GDPR principles of data privacy and protection (Ben Wolford, 2019). Unquestionably, to ensure compliance with the GDPR principles could prove to be a herculean task for any business. Data privacy and protection is highly essential in this fast-paced and evolving era of technology, complying to the GDPR could ensure that a business protects its consumer's data and privacy (Sharma, 2019, p. 88).

### 2.3.1 Regulatory Bodies in Ireland and the European Union

In the European Union, there are regulatory bodies that ensure all member states align and implement the data protection legislation that is the GDPR. The regulatory body for data protection in the European Union following the GDPR implementation is the European Data Protection Supervisor (EDPS). The European Data Protection Supervisor (EDPS) oversees EU institutions and bodies to ensures strict compliance and respect of consumer's right to privacy during the processing of their personal data. It was set up in 2004 and its location is in Brussels, Belgium (EDPS, 2016). The EDPS has two main supporting entities namely: **supervision and enforcement** which appraises data protection compliance of EU bodies and institutions and **policy and consultation** which counsels EU legislators on data protection affairs in different policy areas and new legislative proposals. The EDPS also ensures that EU institutions and

bodies do not process an individual's personal data such as political opinions, race or ethnic origin, trade-union membership, religious views or philosophical views. They are also not to process health or sexual orientation except for healthcare reasons and even then it must be done by a health care professional or other persons that adhere strictly to data privacy or secrecy (EDPS, 2016). The duties of the EDPS include:

- Oversee all new technologies that influence data protection.
- Manage enquiries and handle complaints.
- Supervise processing of personal data in the European Union's administration and ensure compliance with data privacy legislation.
- Counsel EU bodies and institutions on all facets of processing personal data and its associated rules, policies and legislation.
- Collaborate with the national officials of European Union member states to ensure uniformity in data privacy and protection.

(EDPS, 2016).

The Data Protection Commission (DPC) (An Coimisiún um Chosaint Sonraí in Irish) is the national independent authority in Ireland that manages the sustenance of the fundamental right of individuals in the European Union (EU) to protect their personal data. Consequently, the DPC is the Irish supervisory authority in charge of monitoring the application of the GDPR (Regulation (EU) 2016/679). The mission statement for the DPC is to *safeguard data protection rights by driving compliance through guidance, supervision, and enforcement* (DPC, 2019). The core duties of the DPC, to enforce the GDPR and the Data Protection Act 2018, that gives further implementation to the GDPR in Ireland, are:

- Manage inquiries and investigations regarding violations of data protection legislation and ensures enforcement action where necessary.
- Stimulate awareness amongst residents of the public of their data subject rights and have their personal information protected under the laws of data protection.
- Investigate complaints from individuals in relation to potential violations of data protection law.
- Convey improved awareness and compliance with data protection legislation to data controllers and processors legislation via the publication of high-quality guidance, proactive engagement with public and private sector enterprises and organizations.

- Consultations with organisations to aid in recognising risks to personal data protection and provide guidance of best practice methods to mitigate against those risks
- Collaborate with (which also involves sharing information with) other data protection authorities and function as Lead Supervisory Authority at EU level for organisations that have their main EU establishment in Ireland.

(DPC, 2019).

The DPC acts as administrative authority for personal-data processing under several key legal frameworks. These include the General Data Protection Regulation (GDPR), Data Protection Act 2018, Law Enforcement Directive (Directive 2016/680, as substituted in Ireland under the Data Protection Act 2018), Data Protection Act 1988 and 2003, and the 2011 "e-Privacy Regulations" S.I. No. 336 of 2011 of the European Communities (Electronic Communications Networks and Services) (Privacy And Electronic Communications) Regulations 2011) (DPC, 2019).

These legislations apply to the processing of personal data by institutions with law-enforcement responsibilities in the context of the safeguarding, prevention, investigation, detection, or prosecution of criminal offences or execution of criminal fines and penalties. The DPC also executes certain supervisory and enforcement roles in relation to the processing of personal data in the context of electronic communications under the e-Privacy Regulations (S.I. No. 336 of 2011) (DPC, 2019).

## 2.4 CONCEPTUAL FRAMEWORK

According to Miles and Huberman (1994), a conceptual framework is a visual or written result that explains graphically or in descriptive form, the key concepts, variables or factors in the main research and their assumed relationships (Cardoso *et al.*, 2014). The conceptual framework of this study was designed by identifying the key concepts, connecting the variables, and establishing a relationship based on preceding literature. The key concepts in this study has also been a useful guide to maintain the focus of the study.

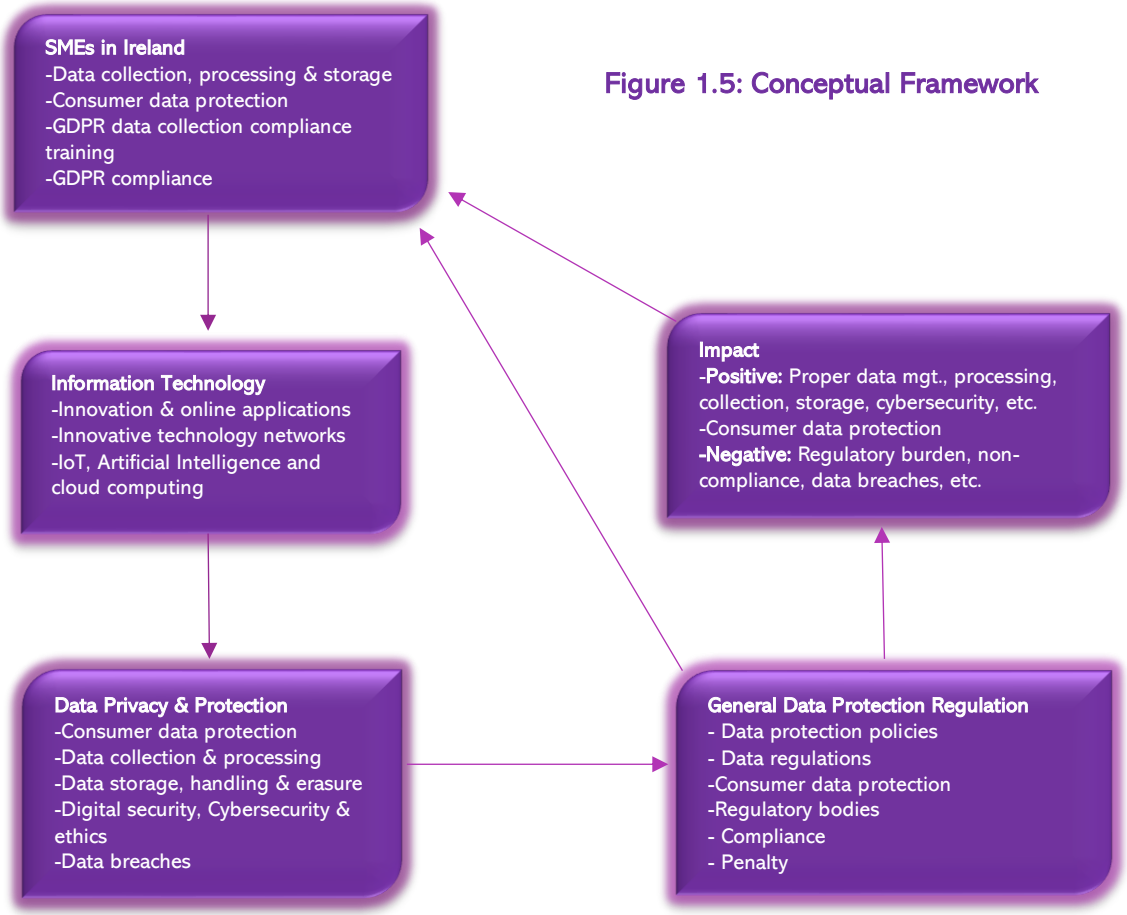



Figure 1.5: Conceptual Framework

The conceptual framework provided above shows the influences and relationships between all the key concepts, the outcome and it's resultant negative and positive impact on Irish SMEs. The conceptual framework also details the evolution of Information technology and innovation, its use by Irish SMEs for data collection, processing and storage. The fact that SMEs are considerably reliant on technology leads to the concern of data privacy and protection which entails consumer data protection, the data being collected, processed, stored or erased. It also deals with the data breaches that occur due to lack of adequate cybersecurity and absence of proper cyber ethics. The relationship between all the key variables and their underlying influences/issues give an outcome to the General Data Protection Regulation (GDPR). It also enumerates the policies, regulations implemented, its regulatory bodies, ensuring compliance and penalty for non-compliance. This outcome branches out to the underlying impact of GDPR on small and medium-sized Irish businesses. The positive impact of GDPR includes constituting guidelines for proper data collection, processing, and storage. Another upside is the increased cybersecurity which protects consumer data and prevent data breaches. The negative impact includes viewing the GDPR as a regulatory burden as it requires these businesses to invest in high tech applications or infrastructure to facilitate the

implementation of the data regulations. In addition, another downside to the GDPR implementation is that due to the size of these businesses, they tend to be overlooked while the focus of implementation is on the large organisations. This could also lead to data breaches from these businesses if they are continuously overlooked. It is imperative for these businesses to be compliant to the GDPR so as to prevent further breach of consumer data.

## 2.5 CONCLUSION

The literature reviewed in this chapter portrays the concept of GDPR and data privacy and the importance it places on proper compliance and implementation in small and medium-sized businesses in the Irish economy. It is also noteworthy that there are numerous topics related to this study such as consumer data protection, online data privacy, cybersecurity, cyber ethics, and digital security which are very essential to data privacy and protection. However, the key concepts of this research were explored and discussed extensively to depict the relationship as portrayed in the conceptual framework diagram. The intention of this research is to examine the GDPR implementation measured against data privacy and protection and when analysed highlights the impact on small and medium-sized Irish businesses.

# CHAPTER THREE

## 3. RESEARCH METHODOLOGY AND DESIGN

### 3.1 Overview

This section of the study provides a detailed discussion of the methodology, philosophy, and approach of the research. The research methodology is vital as it explains the data collection techniques, it influences the validity and reliability implemented during the study. It also depicts the nature of data collection, data analysis and the research questions examined. The research methodology also aids to understand the research philosophy and its application on the key concepts in the research undertaken. This research is a descriptive study using the interpretivist philosophy and a deductive approach. Semi-structured interviews were constructed and used to collect primary qualitative data that would be analysed through a discourse analysis.

### 3.2 Research Philosophy and Approach

Research philosophy can be defined as structure of beliefs and assumptions as it concerns the development of knowledge. The research philosophy aid to understand the research questions, methodology and interpret the potential findings (Saunders *et al.*, 2015, p.124). The philosophy adopted reflects the assumptions/opinions developed by the researcher and his/her understanding of the world.

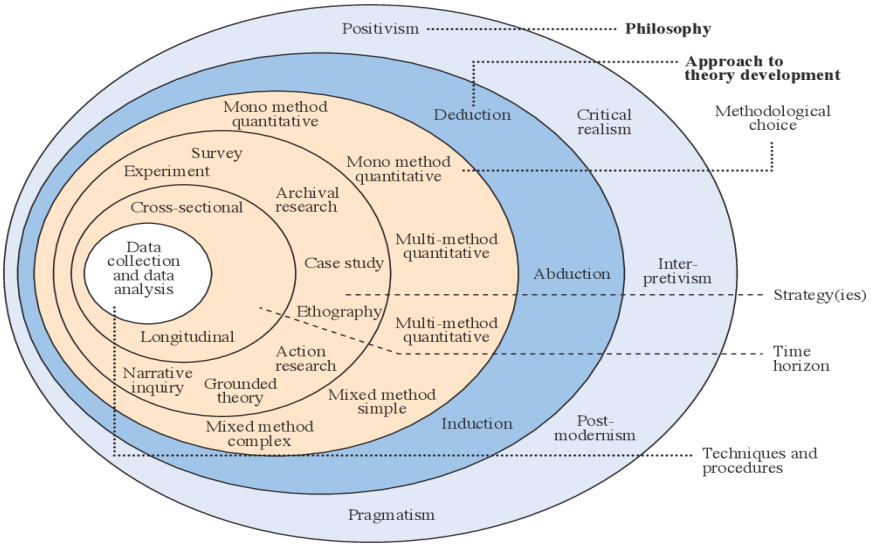



Figure 1.6: Research Onion (Saunders, Lewis & Thornhill, 2015, p. 124)

As seen in the diagram above, there are different forms of research philosophies that describes research strategies and approaches. The five main philosophies include:

1. **Positivism-** This is a theory that describes the evolution of human societies and created set of recommendations for investigating an inquiry. (Brown and Baker, 2007, p. 34). A positivist concentrates on scientific empiricist methods to uncover pure data and facts unaffected by human examination or bias. This philosophy requires the researcher to be objective, independent and use general theories against measures to certify or attest the hypothesis. The positivist is also required to be detached, neutral and use universal laws to depict the phenomenon of the research (Saunders *et al.*, 2015, p. 136).
2. **Realism-** The realist accepts the bias affected by the human interaction, culture, and societal structure. The researcher is objective and attempts to reduce bias and misconception. Realism is related to epistemology which translates to the representation of a situation or reality is described as what you see is what you get (Saunders *et al.*, 2015, p.136). A realist views a situation is real when it shows visible or material results (Brown and Baker, 2007, p. 53).

   Saunders et al., (2015) further discussed that there are two types of realism and they are:

   **Direct realism** also simple empirical scientific realism is the belief that one's experience through our senses depicts the world realistically and as stated earlier what you see is what you get while **Critical realism** explains that what one sees or experiences in underlying patterns of reality shape discernible events. A critical realist believes what we sense or observe cannot be completely relied upon (Saunders *et al.*, 2015).
3. **Interpretivism-** is a philosophy that signifies that humans are distinct from physical situations because meanings are created. It is also related to epistemology like positivism and realism. An interpretivist believes that different individuals from diverse cultural backgrounds, diverse situations and at different times make unrelated meanings, thereby they form and experience diverse social realities. It also believes that substantial insight into humanity is misplaced if the complexity is minimised to a series of general laws. An interpretivist researcher collects meaningful data from its participants and develops new, substantial understandings and evaluation of social spheres and settings (Saunders *et al.*, 2015, p. 140).
4. **Postmodernism-** A postmodernist researcher believes that any sense of order is temporary and baseless, ascribing more importance to the role of language.

He/she dismisses modern objectivity, realist ontology of things and instead highlights the disorderly primary of flux, change, movement, and elasticity. The philosophy embraces the role of language and influence of relations that query the welcomed ways of thinking instead voicing the alternate marginalized views (Saunders *et al.*, 2015, p. 141).

5. **Pragmatism-** This philosophy aims to harmonize subjectivism and objectivism, values and facts, explicit and rigorous knowledge, and distinct experiences in context. It considers concepts, ideas, theories, research findings and hypotheses in non-abstract form relaying in parts that they portray as tools of thoughts and actions. This is done in terms of their viable repercussions in distinct contexts. A pragmatist starts the research with a problem and presents realistic solutions that inform future practice (Saunders *et al.*, 2015, p. 143).

In the research onion diagram above, there are two main approaches under the research philosophies, and they are- **the Deductive approach** which uses a developed theoretical framework and is tested by empirical observation from the general to the specific. It is an approach that gives the basis of presentation to present laws, anticipates the phenomena, forecast their incidence and allows them to be controlled (Saunders *et al.*, 2019, p. 153). However, **the Inductive approach** engages a familiar premise to generate untested conclusions. It generalises from the specific to the general, the data collected in an inductive research is used to explore a situation, and develop a conceptual framework based on the identification of themes and patterns. A research that adopts the inductive approach is particularly concerned with the conditions in which the events occur (Saunders *et al.*, 2019, p. 155).

The interpretivist philosophy will be adopted for this study because I strongly believe that individuals are different and unique in their perspectives or beliefs based on their diverse cultural/societal realities encountered. Another reason for choosing the interpretivist philosophy for this research is data privacy and protection concerns everyone (myself inclusive) as data subjects, previously my knowledge about GDPR was superficial. This research has deepened my knowledge about GDPR and the importance of data privacy and protection, the data to be collected would also provide insight to how my personal data (as a consumer) is being protected within the European Union.

This study is aimed to be descriptive to obtain information about the impact of GDPR, data privacy and protection. I would also employ a deductive approach to test the data collected and interpret the specific outcomes to produce concrete results. A

discourse analysis would be used to portray perspectives of the Irish SMEs business representatives that were interviewed for the purpose of this research. Their perspectives/opinions would be analysed and interpreted to elucidate a conclusion against the key concepts related to this study.

### 3.3 Research Strategy

A research strategy is used to determine the method and type of data collection. There are different research strategies namely surveys, interviews, case studies, grounded theories, experiments, observations, etc. and they can be grouped under quantitative and qualitative data. The research strategy chosen would determine the data collection and the research design used to support the study such as explanatory, exploratory, analytical or descriptive (Saunders *et al.*, 2019, p. 178).

This research is a descriptive study and the research strategy for data collection to be used are semi-structured Interviews. A research interview is a driven conversation between two or more individuals, where the interviewer asks incisive and straightforward questions while listening attentively to the interviewee's responses. Most times there is an established level of rapport between both parties and an interviewer is required to listen carefully to the interviewee to pick up points of interest, clarify and affirm meanings. The use of interviews is used to collect substantial and reliable data that are appropriate to the research objective(s) and question(s) (Saunders *et al.*, 2019, p. 435).

As earlier stated, I would be conducting interviews with semi-structured questions that are aligned with my research objectives and question. The perspectives gained from the interviewees would provide a deeper understanding about how Irish SMEs view GDPR, data privacy and protection. It would also further explore compliance, positive and negative impact while providing further insights into the challenges encountered with GDPR implementation on their businesses. The phrases and words used by the interviewees would be analysed against the key concepts and discussed extensively.

### 3.4 Collection of Primary Data

The data to be sourced for this research would include primary and secondary data such as interviews, academic journals, peer reviewed journals, articles, books, and other academic online resources. The use of interviews would enable an in-depth analysis with the view to develop findings about the study. The theory would be developed through the analysis of words and phrases examined about how these businesses view GDPR, data privacy and protection. The diverse responses from these

Irish SMEs would provide the valid qualitative data needed to develop findings and discuss possible patterns essential in drawing valid conclusions.

### 3.4.1 Sources

As mentioned initially, this is a deductive study and it requires the collection of qualitative data and the means of primary data collection is semi-structured interviews. The interview would be conducted with already prepared semi-structured questions developed using the research question and objectives. The resulting responses will be analysed using the key concepts of this study. However, as the interviewer I have created room for potential relative opinions that could be obtained from the interviewee's responses which are connected to the study. Due to the method of primary data collection being in-depth semi-structured interviews and time consuming, I plan to conduct 4-6 interviews with personnel in small and medium-sized Irish businesses. As stated, secondary data collection for preceding literature is obtained from academic journals, articles, books, peer reviewed journals and other academic online resources.

### 3.4.2 Access and Ethical Issues

The primary data collection for this study being semi-structured interviews highlights some issues that were encountered in the data collection process. The initial issues include but is not limited to ease of access to interviewees who were willing to participate as a show of goodwill with the knowledge that there is little or nothing to be gained in return. I also encountered a lot of rejections and interviewees that pulled out at the last minute after initially agreeing to take part in the interview due to personal reasons or their busy schedules. Other issues encountered are time constraints and sincere responses as the in-depth semi-structured interview has questions that involves at least 10-20 minutes of the interviewees time taken out of their busy schedule or lunch break and some interviewees were wary to supply sincere responses to the questions due to the sensitivity of GDPR as a topic.

Interestingly, the above issues were further escalated with the development of the COVID-19 pandemic (scientifically known as Coronavirus and nicknamed "Miss Rona") which held the world hostage and introduced significant changes in the normal routine of doing face-to-face interviews due to social distance rules adopted by the National Public Health Emergency team (NPHET) and the Irish government as preventive measures aimed at flattening the curve of COVID-19 pandemic. During these challenging times, there is a significant increase in the reliance on information technology and access restrictions due to the lockdown measures. However, the

interviews were conducted via phone or online interviews once I was able to gain access to and obtain consent from the interviewees.

As regards to ethics, I ensured that all the interviewees read, understood and signed a plain language statement and Informed consent form, they were informed about the main purpose of the research and their voluntary involvement. I also ensured they were aware that the interview was recorded for educational research purposes only. The interviewees were also ensured about anonymity and strict confidentiality according to the code of ethics and GDPR guidelines. As such the names and personal details of the interviewees would be coded to protect the data subjects.

### 3.5 Approach to Data Analysis

The data collected for this study would be analysed through discourse analysis using the words obtained in the interviews. The process of analysis would be done by recording the interviews conducted and transcribing the audio recordings into written format. The audio transcripts would be analysed against the research themes and patterns to discover similar features and determine a discourse analysis about the study (Saunders *et al.*, 2019, p. 438).

The discourse analysis would be conducted with the aid of previous discourse analysis notes. An overall examination would be conducted on the interviewees responses and essential parts that are directly connected to the key concepts would be selected including the way these responses were constructed. The essential parts of the interviews would be selected for in-depth analysis concentrating on their distinct relation to the research objectives and key concepts of the study (Saunders *et al.*, 2019, p. 441).

### 3.6 Conclusion

The methodology and design of a research cannot be exaggerated, it aids the researcher to develop a structured format, appropriate selection of the research philosophy and approach to guide the study. It enables and enhances the study in being precise, concise, and meaningful about decisions in data collection and analysis. This study has employed a structured format to provide well-developed findings that are aligned with the research objectives. It also provides conclusions that would contribute to formulating a solid bedrock for further improvements in GDPR, data privacy and protection.

# CHAPTER FOUR

## 4. PRESENTATION AND DISCUSSION OF FINDINGS

### 4.1 Overview

As mentioned in the previous chapter, the primary source of the data used for this study is Interviews and the data will be analysed using a discourse analysis. There is no generally accepted approach to carrying out a discourse analysis, I would be making use of previous discourse analysis as stated in the methodology section for this study to critically analyse the key concepts.

The primary data collected for this study was sourced from different small and medium-sized Irish businesses. I reached out to about 17 different businesses that met the criteria for this study and are directly involved with data collection, processing and handling. At first, there were several positive responses but due to the COVID-19 pandemic some businesses stopped responding, while others declined and pulled out at the last minute. Overall, I was only able to conduct 4 interviews with willing participants, they consented to participating by signing a plain language statement and consent form. The participants were also aware and consented to the interview recording for educational purposes. The interviews were transcribed and shown in the appendices of this study.

Data privacy, protection and the General Data Privacy Regulation which are the main focus of this study are used to determine how the GDPR guidelines have impacted these businesses since its implementation, the challenges encountered and their personal perspectives of the guidelines.

To analyse the data collected and contributing to the findings discussed, the key concepts were critically examined against certain responses from the participant interviews which are related to the research question and objectives. These responses are highlighted in the code book and related to the themes used for the discourse analysis.

A discourse analysis uses expressive phrases, certain words and expressions to interpret a conversation putting into consideration the situation in which the communication exchange occurs and the diverse cultures or backgrounds (Canepari, 2015). A discourse can be described as a precise way of communicating and knowing an aspect of the world. There are several arguments and perspectives about how a

discourse analysis is done. However, the fundamental perspective of language being coordinated and its translations are vital to give meaning to the discourse being analysed (Jørgensen and Phillips, 2002).

The key concepts to be used for this discourse analysis include **compliance, data privacy & protection, regulatory burden, data breach, cybersecurity, positive impact, negative impact, access and storage.** These concepts were key phrases used during the interviews with the respondents and the significance of this phrases were essential to arrive at the findings for this study. In discussing the findings for this study, it is pertinent to mention the research objectives and question which was used as the research guide. The research objectives are:

1. To examine the impact of the General Data Protection Regulation on Irish SMEs.
2. Evaluate compliance of Irish SMEs in ensuring data protection and privacy of their customers.
3. To explore the challenges Irish SMEs experienced or are still experiencing with implementing the General Data Protection Regulations in their business

The research question as stated in the first chapter is **'What are the impacts of the General Data Protection Regulations, Data Privacy and protection on Irish SMEs?'**

## 4.2 Findings

The findings presented in this study were measured and analysed against the key concepts studied in the literature review. The concepts were developed using the research objectives and question to indicate the impact of the GDPR, data privacy and protection on Irish SMEs.

### 4.2.1 To examine the impact of the General Data Protection Regulation on Irish SMEs.

In considering the objective stated above, the finding discovered was analysed through certain phrases used by the participants. It was discovered that the GDPR does have positive and negative impacts on the small and medium-sized Irish businesses that participated in the interviews. To highlight the different impact findings, the theme "**Impact: Positive and Negative"** was used in the code book found in the appendices. The impacts were also highlighted in the interviewees responses and colour coded as **Positive** (green) and **Negative** (purple) as identified in the appendices of this study.

As stated above, there are indeed positive and negative impacts of the GDPR and all four interviewees gave different responses about how the GDPR has affected their

businesses. As seen in the responses given by interviewee 1,2,3 and 4 in the appendices. Further analysis from the interviewees shows that the positive impact of the GDPR as enumerated by interviewees 1,3 and 4 are good initiative, increased security, sensitivity and cautiousness to data privacy. Other positives include using the GDPR guidelines to re-access data storage, prioritizing data privacy and protection of their customers data. The negative impact of the GDPR as itemized in the responses given from interviewees 2,3 and 4 are its effects on their employee hiring process, difficulty in implementation, financial impact and disruption of business operations in trying to accommodate consumer needs while adhering to the GDPR guidelines.

These findings reveal that the General Data Protection Regulation is vital to protecting the personal data of not only the consumers but also the employees and the businesses. In analysing the data, it shows that the GDPR provisions are a good initiative in data privacy and protection. Although the impact on Irish SMEs differ based on the sizes of the business and the positive impact outweigh the negative impact it is obvious that Irish SMEs would still need more time adjusting to the GDPR guidelines.

#### 4.2.2 Evaluate compliance of Irish SMEs in ensuring data protection and privacy of their customers.

The findings for this objective revealed the level of compliance by these SMEs interviewed. It portrayed that all businesses are compliant based on their resources and business operational standards. The indication for this can be found under the themes Compliance and Data privacy and protection colour coded as pink and brown in the appendices. It was discovered that every business adheres to the operational standards of the labour union they function under and they maintain that standard in their business operations. These businesses also utilize their available resources in order to implement the GDPR guidelines in protecting their customers personal data.

Interviewees 1 and 2 stated that they were GDPR compliant, evaluating the interview and the size of their business, it shows that they considered their businesses GDPR compliant based on the resources utilized in implementing the guidelines to their operations. They also inculcated additional measures such as including the GDPR guidelines for customer data protection into their employee contracts and employing the use of concealing customer names or card details when they patronize the business. Interviewees 3 and 4 stated they were under certain business operational standards maintained by their unions. This means that these businesses are under the obligations to uphold the standards of the unions they represent to be GDPR compliant. It shows that there are procedures and protocols to make sure that the

businesses were not only reliant on their initiative and the strength of their resources to implement the GDPR guidelines for data privacy and protection of their customers. They also acknowledge the importance of data privacy and protection of their customers data and making it imperative for them to maintain the standards in that respect.

Overall, the analysis shows that Irish SMEs are GDPR compliant based on different circumstances, business resources available and business operational standards. The presence of labour unions or organizational entities ensure that the businesses functioning under them maintain the standards of GDPR compliance. Their union or organizational entities have internal standards that businesses functioning under them must uphold, including external provisions such as the GDPR. In evaluating their compliance towards data privacy and protection of customers personal data, Irish SMEs understand the importance of customer data privacy and protection and they employ the GDPR guidelines to ensure they are compliant.

#### 4.2.3 To explore the challenges Irish SMEs experienced or are still experiencing with implementing the General Data Protection Regulations in their business.

The findings for this objective identified that Irish SMEs experienced and are still experiencing challenges implementing the GDPR in their businesses. In the analysis of this objective, the evidence can be found under the theme **Challenges** colour coded in orange. All interviewees highlighted the challenges they experience with GDPR implementation in their business operations. Interviewee 1 stated that they experienced challenges with access to video surveillance, prior to the GDPR guidelines there was ease of access to video surveillance. After the GDPR guidelines were implemented the business has to limit access to video surveillance and also ensure upgraded security which proved to be a bit challenging. Interviewee 2 explained that the main challenge the business faces is with hiring staff, compliance with the GDPR guidelines for recruitment hinders the business owner from obtaining the some of the essential information needed from the potential employee. The interviewee also stated that the GDPR guidelines apply to the business and the employee, also getting information may prove a bit difficult because as a business owner you are limited from obtaining some personal information about the potential employee.

Interviewee 3 stated the business had to change their approach in order to be compliant with the GDPR guidelines and it has not been an easy process. This means that the business is still experiencing challenges with implementing the GDPR into the business. Despite the business operational standards that need to be upheld it has not and is not an easy implementation process due to the size of the business.

Interviewee 4 described some challenges faced in implementing the GDPR guidelines due to the nature of the business. The interviewee explained that how long the business has been in existence prior to GDPR, they had quite a volume of data stored. After the implementation of the GDPR guidelines, they were faced with a large volume of work as they had to re-assess, recategorize and re-catalogue the data they previously stored and the new data they currently possess. Another challenge they faced was that due to the old records which were over 50 years old, they had to curb all the excess and re-process it into a different category which took quite some time to achieve.

Overall, the analysis shows that Irish SMEs have encountered quite a lot of challenges and still encounter challenges implementing the GDPR guidelines into their business operations. It also shows that the GDPR guidelines is a process which would take some time for Irish SMEs to implement seamlessly. The occasional challenges will still arise in future during the course of daily operations.

## 4.3 Discussion

As discussed in the conceptual framework section in chapter 2, the key concepts of this study were used to analyse the primary data collected via interviews. In this section, I would be discussing the key concepts used as themes that were analysed against certain phrases from the interviews. The themes analysed against the data include **data privacy & protection, compliance, regulatory burden, data breach, cybersecurity, positive impact, negative impact, access and storage.** These themes were deducted from the conceptual framework of this study, which also outlined in the literature review. In the discussion of each theme, the relevance of the theme to the core of this study is conveyed and this proves that the General Data Protection Regulation, data privacy and protection have significant impact on small and medium-sized Irish businesses.

### 4.3.1 DATA PRIVACY AND PROTECTION

This key concept is a major theme in this study, in the literature review it was discussed extensively and linked to the GDPR. It can also be seen under the theme **Data privacy & protection** colour coded in brown as depicted in certain phrases from the opinions of the interviewees. In the data analysis, it was discovered that data privacy and protection is indeed important to SMEs especially in protecting their customers, employees and businesses. Although implementing the GDPR guidelines cannot be said to be a seamless process, these businesses believe in the right to privacy. Interviewee 1 indicated that employees had to sign contracts in line with the GDPR guidelines besides the usual employment contracts. It can also be noted that it

is no longer allowed to give out personal information of employees even though the inquirer is familiar with the employee in question. For Interviewee 2 despite not having much of an opinion, there are measures in place to ensure data privacy and protection for its customers. He also mentioned that the GDPR guidelines is a safety net for the business and its employees.

Interviewee 3 explained that due the nature of the business, all its employees sign a confidentiality agreement and that breach of this agreement results in immediate contract termination. The interviewee also stated that data privacy and protection is the cornerstone of the business and the protection of their customers personal data is treated with the utmost priority. Interviewee 4 stated that data protection is the entirety of the business and protection of the customers data is essential, requiring top security. Overall, this proves that data privacy and protection is vital in any business regardless of its size or business operations. These SMEs interface with data in different ways on a daily basis and it can be seen that they understand the importance of data privacy and protection for their customers, employees and the business as a whole.

### 4.3.2 CYBER SECURITY, DIGITAL SECURITY, DATA ACESS AND STORAGE

In analysing these concepts, they were measured against certain phrases in the interview and the phrases were deducted through questions regarding cybersecurity, data access and storage for the business. The analysis of the data revealed that cybersecurity and digital security are vital to proper data protection, it also proves that Irish SMEs are quite reliant on information technology and innovation by employing the use of cybersecurity software and upgraded digital security measures in order to secure its data. As regarding data access and storage, the data analysis portrayed that Irish SMEs have to limit data access and upgrade storage putting the data in secure locations and using technological devices to back up the data in the cloud. The evidence of this can be viewed in the code book (interviewee responses) under the themes **Cybersecurity & Digital security** colour coded in blue and **Data access & storage** colour coded in turquoise.

In the data analysis, Interviewee 1 stated that since the GDPR guidelines have been implemented, only the top management personnel are authorized access to sensitive data. It was also detected that a software has been installed to help with cybersecurity and administer different levels of access between the employees and top management personnel of the business. Interviewee 2 simply revealed that there was a secure software and physical secure storage in place with limited access to only the business owner.

In analysing the data from Interviewees 3 and 4, it was discovered that these businesses had higher cyber and digital security installed for their businesses. Being high data regulators, the use of anti-virus, high-tech cybersecurity and cybersecurity insurance are used to protect their data. It was also seen that access to sensitive data within the businesses was dependent on the employees job rank. These businesses also ensure that there is a secure password system and levels of authorization to access sensitive data. This proves that Irish SMEs are particularly cautious about the measures they use to secure their data while ensuring that they are adhering to the GDPR guidelines.

### 4.3.3 COMPLIANCE AND REGULATORY BURDEN

The data analysis for this concept are seen in the second finding above, Irish SMEs are GDPR compliant based on the business size, its resources and business operational standards. It also proves as discussed in the literature review, that the GDPR provisions is seen as a regulatory burden on Irish SMEs. This is because these businesses have had to change their business operations to be compliant with the GDPR guidelines which was no difficult process, requiring utilization of several resources for proper implementation to avoid fines or penalties.

The data was analysed using interview responses against the themes **Compliance** with colour coded in pink and **Regulatory Burden** colour coded in yellow as seen in the code book under appendices. Subsequently, all businesses indicated their compliance with the GDPR guidelines to the best of their abilities. This means that being GDPR compliant as Interviewee 1 stated is to ensure that the employees sign contracts with GDPR guidelines and implementing the GDPR provisions into the business which required upgrading their system to ensure compliance. As stated previously, interviewees 3 and 4 under these themes are under labour unions or organizations which maintain internal business operational standards and the GDPR guidelines to ensure compliance. The presence of the union or sanctioning bodies is an added measure on these businesses to uphold the standards expected and be GDPR compliant. However, the GDPR proved to be a regulatory burden for these businesses as well, this is because they had to re-access, re-process and erase the data they previously stored. It was also discovered that there are high expectations on these businesses to be up to date on GDPR compliance.

### 4.3.4 IMPACT AND CHALLENGES

In discussing both concepts, the data was analysed using interview responses against the themes as stated above. However, it was discovered that Irish SMEs have experienced significant impact (positive and negative), they encountered challenges

and still encounter challenges in implementing the GDPR guidelines into their businesses. The evidence for this can be found in the interview responses (under the appendix section) and highlighted in the code book under the themes **Impact:** Positive and Negative colour coded in green and purple respectively and under Challenges colour coded in orange.

As evidenced, the data analysed against the themes indicates the positive impact of the GDPR implementation for all the interviewees as a good initiative, promoting increased awareness, sense of responsibility, sensitivity and cautiousness towards data privacy and protection in their business operations. However, there are also some negative impacts that were highlighted from interviewees 2,3 and 4 such as the GDPR not being easy to implement, affecting the daily business operations and financial impact. These businesses highlighted the above as the downside to the GDPR implementation on their businesses.

As regards the challenges encountered and still being encountered by these businesses. Interviewees 1 and 2 stated that there were challenges to restricted placement of surveillance (CCTV), restricted access to the surveillance footage, issues with getting relevant information during employee recruitment and significant financial investment. Interviewees 3 and 4 indicated their challenges with the GDPR implementation as change of business approach to be GDPR compliant and significant financial investment. As discussed in the literature review, this proves that Irish SMEs do incur significant financial impact to acquire the resources needed to implement the GDPR, maintain compliance and avoid penalties.

### 4.4 Conclusion

As seen in the findings outlined above, it can be implied that the General Data Protection Regulation is quite essential in its role to ensure data privacy and protection in all facets of business. There are different approaches which a business can take to ensure proper implementation of GDPR guidelines. Although as proven there should be more focus placed on Irish SMEs to ensure adequate implementation of the GDPR guidelines, businesses should also be monitored to ascertain that they are maintaining the standards of data privacy and protection.

This study also proves that data breaches do occur in Irish SMEs, even though not on the scale experienced in international businesses like Facebook and Google. The interview was also constructed to decipher if any of the businesses had ever encountered a data breach, as seen under the theme Data breach colour coded as red in the code book (under the appendix). Interviewee 4 indicated that the business had experienced what was described as **"an extremely minor"** data breach, which

proves that regardless of the business size a data breach can still occur if the adequate security measures are not implemented. Interviewee 4 further described that although the data breach was minor, it was a wake-up call to tighten up, upgrade the security measures and invest in cybersecurity insurance as previously discussed in the literature review.

Further analysis of the data collected for this study shows that Irish SMEs are still in the **"learning phase"** of GDPR implementation and compliance. There is indeed the increased awareness for data privacy and protection both on the consumers and the businesses, however Irish SMEs should receive the adequate support required to ease the regulatory burden and reduce the challenges encountered in their business operational standards. The General Data Protection Regulation regulatory body in Ireland should engineer this support as this would instil a better sense of transparency and responsibility on Irish SMEs.

In conclusion, this study has proven its objectives and proven that the GDPR, data privacy and protection do impact Irish SMEs in diverse ways depending on several factors. It is possible for Irish SMEs to be GDPR compliant as seen in the findings, also data privacy and protection is highly essential for the protection of consumers and businesses. Consumers should also be aware about their rights to data privacy and protection especially since we all contribute to the emerging digital footprint.

# CHAPTER FIVE

## 5. CONCLUDING THOUGHTS ON RESEARCH CONTRIBUTION, ITS LIMITATIONS, RECOMMENDATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

### 5.1 Summary and Implications of Findings for the Research Questions

In summary of the above, it is implied by this study that Irish small and medium-sized enterprises/businesses deserve to be paid more attention by the Data Protection Commission (DPC). This is because the focus on large organizations leaves room for complacency in compliance and implementation with the General Data Protection Regulation in Irish SMEs. While it inevitably takes time to fully adopt the GDPR guidelines into every facet of business, it is imperative that a data protection audit needs to be conducted on Irish SMEs especially independent business not under sanctioning bodies or unions. This is because an independent business is prone to non-compliance or partial compliance with the GDPR, which leaves the data processed or collected by the business vulnerable or prone to cyber-attacks. Although the perceived opinion is that Irish SMEs are not a major concern, there is still a lot of work to be done to ensure that the GDPR guidelines are strictly complied with by all.

This study also reveals that the GDPR guidelines warrants improvement to provide allowances for SMEs who do not have the adequate resources to comply. As seen in this study, most Irish SMEs are still in the learning and implementation phase and as the economy expands more SMEs are bound to be established. Considering the digital footprint generated on a daily basis and the fact that information technology continually introduces innovation, the world is more reliant on technology especially since the COVID-19 pandemic shook the world to its core.

### 5.2 Contributions and Limitations of the Research

In view of the literature review and findings of this study, it is proven that the GDPR, data privacy and protection still need to be properly enforced in all businesses. It also shows the monopolized focus on large organizations should be widened to include Irish SMEs. The broadening of the GDPR compliance focus would prevent or at least ensure that Irish SMEs are prepared for the possibility of cyber-attacks or data breaches. Data breach or cyber-attack of any kind on personal data is an infringement of data privacy rights, therefore it is imperative to protect the privacy of all.

The main limitation of this research was getting willing interviewees to participate in the interview for this study. Due to the pandemic and the sensitivity of GDPR, data privacy and protection, 4 out of 17 granted an interview to contribute to this study. The inability to access a sizeable number of interviewees limited the study's ability to probe into more detailed analysis from diverse businesses and their opinions about the GDPR, data privacy and protection. However, this study can only assume that the findings are to be accepted and used to guide further research as needed.

### 5.3 Recommendations for Practice

The first recommendations for practice are directed towards the data protection regulatory body in Ireland. The Data Protection Commission should perform an audit to determine the stage of implementation and compliance of the General Data Protection Regulation in Irish SMEs. This will further strengthen the objectives of the DPC in deciding a supportive approach to guiding these businesses in the right direction towards maintaining the data privacy and protection standards. It is also recommended that the DPC collaborate and gears its support towards sanctioning bodies and unions of Irish SMEs to ensure consistency and standard compliance with the GDPR. It is also important that support towards cybersecurity insurance for Irish SMEs be subsidized to allow the smallest businesses afford the services of cybersecurity insurance.

The second set of recommendations are directed towards Irish SMEs, I applaud the efforts of these businesses that have improved their business operational standards and upgraded their technological systems to be GDPR compliant. However, there is still a lot of room for improvement as regards the areas cybersecurity, data access and storage. It is understandable that these businesses can only utilize the resources they possess, it is therefore imperative to invest in the cybersecurity or digital security software that would protect data access and storage against cyber-attacks and data breach.

Lastly as regards the consumers I recommend that, it is imperative to know your rights for data privacy. Embarking on this research has deepen my knowledge about my rights to data privacy and protection. This study has broadened my knowledge and opened my mind to the amount of data being processed daily and even my contribution to it. Being aware of your rights to data privacy and protection increases ones sense of responsibility and cautiousness of distributing one's data on different online and physical platforms.

### 5.4 Recommendations for Further Research

In recommending further research, I would suggest that more Irish SMEs be evaluated to gain a deeper insight into the concept of data privacy and protection. It would also further contribute to general knowledge about the opinions of Irish SMEs towards the GDPR, data privacy, protection, data management and other related concepts. I would also recommend that an in-depth analysis on consumer knowledge to data privacy and protection be carried out to educate consumers about their rights and how to curb excessive data distribution.

### 5.5 Final Conclusion and Reflections

Conclusively, the importance of data privacy, protection and compliance with the General Data Protection Regulation cannot be underestimated. It is imperative that there is need to drive awareness and knowledge about data privacy and protection. Knowledge should not be limited to the elite, everyone deserves a right to privacy and should be protected as such. In the words of Interviewee 3, *"there's always a superior force out there that can get personal data if they want…*". As stated earlier, the pandemic has created a substantial reliance on information technology and innovation, which continues to evolve and provide the world with numerous pathways in increasing our digital footprint. Taking into consideration the entire study, the importance of being conscious about the sensitivity of the data we provide cannot be overestimated.

## REFERENCES


Ashford, W. (2016) 'Organisations Make Data Protection an Investment Priority Ahead of GDPR'. *Computer Weekly*, pp. 4–6. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=114602126&site=ehost-live (Accessed: 14 December 2019).

Beduschi, A. (2019) 'Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights'. *Big Data & Society*, 6(2), p. 2053951719855091. DOI: 10.1177/2053951719855091.

Ben Wolford (2019) *Do Consumers Know Their GDPR Data Privacy Rights? GDPR.eu*. Available at: https://gdpr.eu/consumers-gdpr-data-privacy-rights/ (Accessed: 17 May 2020).

Ben Wolford (2019) *Millions of Small Businesses Aren't GDPR Compliant, Our Survey Finds*. *GDPR.eu*. Available at: https://gdpr.eu/2019-small-business-survey/ (Accessed: 17 May 2020).

Brown, B.J. and Baker, S. (2007) *Philosophies of Research into Higher Education.* [Ebook] Bloomsbury Publishing. Available at: Available at: https://www.perlego.com/book/805633/philosophies-of-research-into-higher-education (Accessed: 6 May 2020).

Canepari, M. (2015) *An Introduction to Discourse Analysis and Translation Studies.* [Ebook] EDUCatt. Available at: Available at: https://www.perlego.com/book/1084888/an-introduction-to-discourse-analysis-and-translation-studies (Accessed: 22 May 2020).

Cardoso, J., Lopes, R. and Poels, G. (2014) 'Conceptual Frameworks'. *SpringerBriefs in Computer Science*, (9783319108124), pp. 15–33. DOI: 10.1007/978-3-319-10813-1_2.

Christian Kurtz, U. of H., Martin Semmann, U. of H. and Tilo BÃ\Phmann, U. of H. (2018) 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors'. *INFORMATION SYSTEMS SECURITY AND PRIVACY (SIGSEC)*, p. 10. Available at: https://aisel.aisnet.org/amcis2018/Security/Presentations/36/.

Digital Rights Ireland Ltd -v- Minister for Communication & Ors [2010] IEHC 221. (2010) (2006 3785 P) *Digital Rights Ireland Ltd -v- Minister for Communication & Ors [2010] IEHC 221*. Available at: http://www.bailii.org/ie/cases/IEHC/2010/H221.html (Accessed: 12 December 2019).

DPC (2019) 'Data Protection Commission Annual Report 25 May-31 December 2018'. Available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf (Accessed: 18 May 2020).

EDPS. (2020) *EPrivacy Directive*. *European Data Protection Supervisor - European Data Protection Supervisor*. Available at: https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en (Accessed: 16 May 2020).

EDPS. (2016) *European Data Protection Supervisor (EDPS). European Union*. Available at: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en (Accessed: 18 May 2020).

El-Leithy, K. (2020) *COVID-19 and Data Protection Compliance | White & Case LLP. White & Case LLP*. Available at: https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance (Accessed: 5 May 2020).

European Commission. (2017) *Proposal for an EPrivacy Regulation. Shaping Europe's digital future - European Commission*. Available at: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (Accessed: 17 May 2020).

European Union (2019) *EU DATA PROTECTION RULES*. Available at: https://ec.europa.eu/commission/sites/beta-political/files/eu_data_protection_rules_-_main_takeways_for_the_future.pdf (Accessed: 20 October 2019).

European Union. (2018) 'Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation – GDPR)'. *International and European Labour Law*, 2014(October 1995), pp. 958–981. DOI: 10.5771/9783845266190-974.

European Union and Agency for Network and Information Security (2016) *Guidelines for SMEs on the Security of Personal Data Processing.* Available at: http://dx.publications.europa.eu/10.2824/867415 (Accessed: 30 April 2020).

Galli, F. (2016) 'Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions'. *Maastricht Journal of European and Comparative Law*, 23(3), pp. 460–477. DOI: 10.1177/1023263X1602300305.

GDPR.EU. (2018) *Art. 4 GDPR - Definitions. GDPR.eu*. Available at: https://gdpr.eu/article-4-definitions/ (Accessed: 12 May 2020).

Jackson, O. (2018) 'Many Small Firms Are Still Unprepared for GDPR'. *International Financial Law Review*, pp. 1–1.

Jardine, E. (2018) 'Privacy, Censorship, Data Breaches and Internet Freedom: The Drivers of Support and Opposition to Dark Web Technologies'. *New Media & Society*, 20(8), pp. 2824–2843. DOI: 10.1177/1461444817733134.

Jørgensen, M.W. and Phillips, LJ. (2002) *Discourse Analysis as Theory and Method.* SAGE Publications [Ebook] Available at: Available at: https://www.perlego.com/book/861080/discourse-analysis-as-theory-and-method (Accessed: 22 May 2020).

Kaan, T. S. and Ho, C. W. (2013) *Genetic Privacy: An Evaluation of The Ethical and Legal Landscape: An Evaluation of the Ethical and Legal Landscape.* [Ebook] Imperial College Press. Available at: Available at: https://www.perlego.com/book/839770/genetic-privacy-an-evaluation-of-the-ethical-and-legal-landscape (Accessed: 12 May 2020).

Kearney, S. (2019) 'Gdpr: Privacy Considerations for the Digital Single Market'. *Journal of Internet Law*, 22(8), pp. 16–21. Available at:

http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=134619099&site=ehost-live (Accessed: 12 December 2019).

Lau, N. *et al.* (2018) 'Human Factors in Cybersecurity – Perspectives from Industries'. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), pp. 139–143. DOI: 10.1177/1541931218621032.

Leenes, R. *et al.* (2017) *Data Protection and Privacy: The Age of Intelligent Machines.* [Ebook] Bloomsbury Publishing Available at: Available at: https://www.perlego.com/book/809079/data-protection-and-privacy (Accessed: 12 May 2020).

Lindgren, P. (2018) 'GDPR Regulation Impact on Different Business Models and Businesses'. *Journal of Multi Business Model Innovation and Technology*, 4(3), pp. 241–254. DOI: 10.13052/jmbmit2245-456x.434.

Loveday, C. and Abraham, R. (2018) 'The General Data Protection Regulation - Another Key Compliance Area for Global Business'. *Defense Counsel Journal*, 85(3), pp. 1–16. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=130846678&site=ehost-live (Accessed: 12 December 2019).

Martin, K.D., Borah, A. and Palmatier, R.W. (2017) 'Data Privacy: Effects on Customer and Firm Performance'. *Journal of Marketing*, 81(1), pp. 36–58. DOI: 10.1509/jm.15.0497.

Matzner, T. *et al.* (2016) 'Do-It-Yourself Data Protection—Empowerment or Burden?' In Gutwirth, S. Leenes, R.and De Hert, P. (eds.) *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Law, Governance and Technology Series. Dordrecht: Springer Netherlands, pp. 277–305. DOI: 10.1007/978-94-017-7376-8_11.

Mortleman, J. (2018) 'Why GDPR Is Great for SMEs'. *Computer Weekly*, pp. 17–21. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=127389473&site=ehost-live (Accessed: 14 December 2019).

Munn, L., Hristova, T. and Magee, L. (2019) 'Clouded Data: Privacy and the Promise of Encryption'. *Big Data and Society*, 6(1), pp. 1–16. DOI: 10.1177/2053951719848781.

Opitz, E.L. (2018) 'Cybersecurity for the Board of Directors of Small and Midsized Businesses'. *Board Leadership*, 2018(159), pp. 4–5. DOI: 10.1002/bl.30115.

Saunders, M., Lewis, P. and Thornhill, A. (2015) 'Understanding Research Philosophies and Approaches'. *Research Methods for Business Students*, 4, pp. 106–135.

Saunders, M. N.K., Thornhill, A. and Lewis, P. (2019) *Research Methods for Business Students.* 8th ed. [Ebook] Pearson Available at: Available at: https://www.perlego.com/book/971477/research-methods-for-business-students (Accessed: 8 May 2020).

Sharma, S. (2019) *Data Privacy and GDPR Handbook*. [Ebook] Wiley Available at: Available at: https://www.perlego.com/book/1323927/data-privacy-and-gdpr-handbook (Accessed: 9 May 2020).

Sirur, S., Nurse, J.R.C. and Webb, H. (2018) 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 88–95. DOI: 10.1145/3267357.3267368.

Spinello, R.A. (2006) *Cyberethics: Morality and Law in Cyberspace*. revised. Jones & Bartlett Learning Available at: https://books.google.ie/books?id=NEyg1T9-dD0C&printsec=frontcover&dq=cyber+ethics&hl=en&sa=X&ved=0ahUKEwi25JnUnonpAhWgSxUIHe8TAB0Q6AEIKDAA#v=onepage&q=cyber%20ethics&f=false (Accessed: 27 April 2020).

Sun, Y. *et al.* (2014) 'Data Security and Privacy in Cloud Computing'. *International Journal of Distributed Sensor Networks*, 10(7), p. 190-903. DOI: 10.1155/2014/190903.

Usman, M. *et al.* (2019) 'A Survey on Representation Learning Efforts in Cybersecurity Domain'. *ACM Computing Surveys*, 52(6), pp. 1–28. DOI: 10.1145/3331174.

Wilner, A.S. (2018) 'Cybersecurity and Its Discontents: Artificial Intelligence, the Internet of Things, and Digital Misinformation'. *International Journal*, 73(2), pp. 308–316. DOI: 10.1177/0020702018782496.

Wong, J.C. (2019) *The Cambridge Analytica Scandal Changed the World – but It Didn't Change Facebook*. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (Accessed: 18 October 2019).

Zerlang, J. (2017) 'GDPR: A Milestone in Convergence for Cyber-Security and Compliance'. *Network Security*, 2017(6), pp. 8–11. DOI: 10.1016/S1353-4858(17)30060-0.

# APPENDICES

## Appendix A – INTERVIEW QUESTIONS

**Preliminary questions:**

i. This interview is solely for educational research purposes.

ii. Do you understand the plain language statement and consent form?

iii. Do I have your consent to record this interview?

iv. Your responses and information provided will be recorded, coded, and remain strictly confidential as stated in the consent form you signed.

**INTERVIEW QUESTIONS**

1. Could you kindly state your role and what your business specialises in?
2. What does data privacy and protection mean to you and the business?
3. How does your work relate to GDPR, data privacy & protection and would you say the business is GDPR compliant?
4. Would you describe the implementation of GDPR as a regulation burden on the business?
5. What effects has GDPR had on the business since its implementation and does it interfere with the business daily operations?
6. What significant challenges has the business encountered with GDPR implementation?
7. How does the business protect its customers data?
8. What is your opinion about GDPR, data privacy and protection?
9. Has the business experienced any data breach and what measures does the business have to prevent any data breach?

## Appendix B – CODE BOOK

The code book illustrated below presents the themes that were used in the analysis, interpretation and findings of the primary data collected for this study.

| THEMES | MEANING | COLOUR | INTERVIEW QUOTE (PRIMARY DATA COLLECTED) | ANALYZED IMPLICATION |
|---|---|---|---|---|
| Data Privacy & Protection | The right to total control of one's personal information and the right for one's data to be protected |  | "people like to maintain a large degree of privacy and confidentiality around us and on a daily basis, we deal with a lot of items and materials that we consider confidential you know" - Interviewee 3 | All individuals have a right to privacy and it is imperative that their data is protected. The business understands the value of data privacy and protection for its customers. |
| Compliance | Conforming with the regulation or laws |  | "we already had the fidelity and secrecy bond in place since the 1960s. That's an annual declaration that you will make sure to maintain the secrecy of information and with the annual training all employees and volunteers have to acknowledge it during the exam at the end of the training. They have to pass it the exam and ensure that their knowledge is up to date and with the annual policy everyone has to read and sign it in respect of the standards. We also have annual refreshers, so they know the data protection standards and are published for members. In the monthly staff meeting there's an auditing board for IT and physical security that's | Steps taken to comply with the General Data Protection Guidelines (GDPR) indicates that this business follows the standards of the GDPR in its business operational standards. |

| | | | | |
|---|---|---|---|---|
| | | | done so if there's any unauthorized access it would be raised by the compliance officer"- Interviewee 4 | |
| Challenges | Challenges encountered by Irish SMEs with implementing GDPR |  | "All staff hiring had to go through the official process in line with the GDPR guidelines for data collection and processing. It has been helpful but it's also a struggle sometimes as well trying to get the relative information that you need". - Interviewee 2 | The challenges encountered/still being encountered by implementing the GDPR guidelines into the business. |
| Positive Impact | The positive impact of the GDPR guidelines since its enforcement |  | "Without permission or a warrant, you cannot get access to the store's surveillance. Also, personal information is no longer given to anyone, they need permission to collect personal information whereas before if someone asked for someone's personal information you could give it to them. Now we're more aware about the sensitivity and cautious about it"- Interviewee1 | Although Irish SMEs face challenges with GDPR implementation, it has created an increased sense of responsibility and security. |
| Negative Impact | The negative impact of the GDPR guidelines since its enforcement |  | "This obviously had a financial impact we had to set money aside and we weren't prepared to do that project at the time" -Interviewee 4 | There is a substantial financial impact on Irish SMEs to ensure GDPR compliance, their resources are limited due to the business size and the annual income/budget. |
| Data Access & Storage | The system put in place for data storage and who has access to the data |  | "it is stored, passworded and backed up on a system that only management has access. We also have a similar system in our common work area downstairs but there's different levels | There is a system in place to store sensitive data and limited access for different roles in the business. This shows an increased sense of security towards data protection. |

| | | | | |
|---|---|---|---|---|
| | | | of access. The general staff have limited access to certain parts in the system while the top management has full access to the sensitive data stored in the back office" - Interviewee 1 | |
| Regulatory burden | The toll experienced in complying with the GDPR guidelines |  | "I think because we are such high regulators, its actually much of an extra burden because our standards, the expectations of central bank and the DPC on us are especially high so we already had a DPO, annual staff compliance policy, mandatory data protection training, statement to members about how their data is being used and data protection in our SLAs. It has been quite a burden on us especially in the aspect of accuracy because credit unions are around for a long time and they started in volunteerism, a lot of our data have been kept longer than necessary" – Interviewee 4 | The GDPR is seen as a regulatory burden because of the provisions Irish SMEs need to comply with to avoid penalties or fines. |
| Cyber & Digital security | The technological software or resources placed to secure data |  | "It's still a work in progress with getting the right anti-virus software for cybersecurity and having a secure network. I think that any pharmacy in this country would fail to have to GDPR security compliance anti-virus software. We're more proactive about it"- Interviewee 3 | Irish SMEs are still learning to install the right cyber and digital security in place, however there's an awareness about it. |
| Data Breach | Violation of security leading to |  | "Yea we've had some data breaches in the past and after that we | Irish SMEs do experience data breaches. Hence the data protection regulatory |

| | | | | |
|---|---|---|---|---|
| | the unlawful loss of stored or processed data | | put all the measures, verification controls and securities in place. The breaches that we've had are extremely minor, we don't have any large scale of data breach" - Interviewee 4 | body in Ireland should place more focus on Irish SMEs. |

As seen below are the samples extracted from the interviews conducted (primary data collected). The themes are coded into different colours as stated in Chapter 4 of this study.

**Summary keywords** (All interviews) **-** data privacy and protection, impact, compliance, GDPR guidelines, significant challenges, personal data, sensitive data, information, cybersecurity, data breach, regulatory burden, consumer data, data access and storage.

## Appendix C- Interview 1

**Speakers** – Interviewer and Respondent (Interviewee)

00:01 **Interviewer:** I will start by saying that this interview is solely for research purposes. Your information and personal data is strictly confidential and not to be distributed anywhere else.

0:00:15 **Respondent:** Ok

00:17 **Interviewer:** Did you understand the plain language statement and consent form stating your voluntary participation for this interview?

00:23 **Respondent:** Yes, I do.

00:24 **Interviewer:** Could you kindly state your role and what your business specializes in?

00:33 **Respondent:** I am the manageress of the business and wife of the owner it is a family business that deals with groceries and essential items. We sell a bit of everything and I manage the store and staff to make sure our shelves are properly stocked and the store runs as it should.

00:56 **Interviewer:** Ok, so what does data privacy and protection mean to you and the business?

01:19 **Respondent:** Initially, anyone could easily gain access to someone's identity by walking into the store and asking for video footage from the camera surveillance of a specific day and time, that person could get it without any issues but now things are different you need to get permission to do that, we are very cautious. Without permission or a warrant, you cannot get access to the store's surveillance. Also, personal information is no longer given to anyone, they need permission to collect personal information whereas before if someone asked for someone's personal information you could give it to them. Now we're more aware about the sensitivity and cautious about it.

01:55 **Interviewer:** What kind of personal information and whose personal information were you referring to exactly?

02:00 **Respondent:** I was referring to giving out staff telephone numbers before now if someone knew a staff by name, they could get their telephone number but now we do not give out such personal information even if they know the staff in question. They need permission to get the staff's personal information.

02:35 **Interviewer:** How does your work relate to GDPR, data privacy and protection and would you say your business is GDPR complaint?

02:46 **Respondent:** I wouldn't know too much about its relation because my husband handles that aspect but we make sure that the business is up to date on compliance with GDPR. All the files containing any personal information or sensitive data is being stored properly then again, my husband handles that part and is right up on it.

03:07 **Interviewer:** Would you describe the implementation of GDPR as a regulatory burden on the business?

03:29 **Respondent:** Maybe at the start it was trying to implement it and upgrade our system but now you can appreciate why and what the GDPR is trying to achieve. At the moment, we just work with the regulations and implement them.

03:43 **Interviewer:** What effects has GDPR had on the business since its implementation and does it interfere with the business daily operations?

03:54 **Respondent:** My husband would know more about that, I'm not sure but he has made sure to follow the rules by the book and he's also made sure we're aware and used to it. I don't think it makes too much of a difference now on the daily operations of the business.

04:15 **Interviewer:** What significant challenges has the business encountered with GDPR implementation?

04:29 **Respondent:** The challenges were with the video footage from camera surveillance, we were used to being able to have access to it easily but now it's different. Access to video footage is limited and also being more careful with staff documentation and contracts everything needs to be signed and stored securely.

05:17 **Interviewer:** Do you know if there's a software used for the data storage and who has access to it?

05:24 **R:** Yes, it is stored, passworded and backed up on a system that only management has access. We also have a similar system in our common work area downstairs but there's different levels of access. The general staff have limited access to certain parts in the system while the top management has full access to the sensitive data stored in the back office.

05:41 **Interviewer:** What is your opinion about GDPR, data privacy and protection?

05:46 **Respondent:** It is a good initiative and it's there to protect people and their identity. I think it's good.

06:01 **Interviewer:** Has the business experienced any data breach and what measures does the business have to prevent any data breach?

06:04 **Respondent:** No, we haven't experienced any data breach. The back office were all sensitive data is stored and has limited access, only the top management are authorized to sensitive data. There's no reason for general staff to go into the back office at all, the staff also sign contracts that state GDPR and data privacy guidelines at the start of their employment. I am not 100% sure what it says in the contracts because I married into the business but I know the staff sign contracts with guidelines in it.

## Appendix D- Interview 2

**Speakers** – Interviewer and Respondent (Interviewee)

00:01 **Interviewer:** Just to confirm that this interview is solely for educational purposes, its being recorded and you are voluntarily participating in it as stated in the plain language statement and consent form?

00:05 **Respondent:** Yes, I am.

00:07 **Interviewer:** Could you please state what your role is and what your business specializes in?

00:11 **Respondent:** I am the owner of the business and its specializes in the hospitality industry.

00:17 **Interviewer:** What does data privacy and protection mean to you and the business?

00:24 **Respondent:** For me, it's a safety net really as such especially on my employees and personally when people are looking for information about us.

00:35 **Interviewer**: How does your work relate GDPR, data privacy and protection and would you say your business is GDPR complaint?

00:39 **Respondent:** More in the hiring aspect than anything else...errm if someone locally here was looking for a job and I know where they came from, I can't ask them questions without them being aware of the purpose or reason I am asking the questions. As for the business, we are GDPR compliant to the best of my abilities so far.

01:05 **Interviewer:** What effects has the GDPR had on the business since its implementation and does it interfere with its daily operations?

01:13 **Respondent:** So, we're newly opened since March this year, so it hasn't really been a big issue for me or the business yet.

01:20 **Interviewer:** When you newly opened what steps did you have to put in place to ensure GDPR compliance?

01:26 **Respondent:** First of all, our camera systems that were initially set up downstairs can't be in place anymore. All staff hiring had to go through the official process in line with the GDPR guidelines for data collection and processing. It has been helpful but it's also a struggle sometimes as well trying to get the relative information that you need.

01:49 **Interviewer:** When you say struggles could be more specific please?

01:53 **Respondent:** For example, as I said earlier about my hiring, getting direct answers from my employees I can't dig too deep and they're under the GDPR guidelines as I am. Former employees would also be one of my major struggles as such because they are under the same guidelines.

02:20 **Interviewer:** How does your business protect its customers data?

02:22 **Respondent:** So, for example when they place an order with us it doesn't show the customer's name and when it's on the credit card payment, it blanks out... I think 12 of the 16 numbers that we do over a purchase. Yea, so it's completely safe for our customers.

02:39 **Interviewer:** For your employees do you have a secure system or software technology for data storage?

02:47 **Respondent:** We have indeed by hand and then we have a secure computer software.

02:54 **Interviewer:** By hand is it locked somewhere safe and who has access to it? Does every employee have access?

02:59 **Respondent:** No, just me. I am the only one that has access to it.

03:01 **Interviewer:** What is your opinion about GDPR, data privacy and protection?

03:16 **Respondent:** Errrmm... I don't really have an opinion on it as such, it's just a case of its necessary now more than anything else you know.

03:17 **Interviewer:** Has your business experienced any data breach?

03:18 **Respondent:** No.

03:19 **Interviewer:** Do you have any preventive measures against any data breach?

03:23 **Respondent:** At the moment I don't to be quite honest, I'm still learning the ropes inside, it's a learning process and GDPR is not very easy to implement... errrm, so we're still in the learning aspect of it.

## Appendix E- Interview 3

**Speakers** – Interviewer and Respondent (Interviewee)

00:01 **Interviewer:** This interview is solely for educational purposes, do you understand the plain language statement and consent to voluntarily participate in this recorded interview?

00:16 **Respondent:** I do indeed.

00:18 **Interviewer:** Your information, name and responses are strictly confidential and will not be shared even after the completion of this research.

00:27 **Respondent:** That's fair enough.

00:28 **Interviewer:** Could you kindly state your role and what your business specializes in?

00:32 **Respondent:** This business is a pharmacy and it specializes in healthcare. I am the owner and superintendent pharmacist of this pharmacy.

00:46 **Interviewer:** What does data privacy and protection mean to you and the business?

00:50 **Respondent:** Well... Data privacy and protection has always been the cornerstone of a pharmacy, confidentiality, people's prescriptions and medical data has always been treated with the utmost respect. It is always confidential and stays within the four walls of any pharmacy business, errm... that has always been the way you know, it means a lot and it means everything to the customers as well you know.

01:28 **Interviewer:** How does your work relate to GDPR, data privacy & protection?

01:33 **Respondent:** Well we receive prescriptions and we have a daily conversation with people in relation to their own private well-being, relating to their own medical history, medication they are using. So, people like to maintain a large degree of privacy and confidentiality around us and on a daily basis, we deal with a lot of items and materials that we consider confidential you know. It's vital to our daily role.

02:26 **Interviewer:** Would you say the business is GDPR compliant?

02:30 **Respondent:** Well errm... GDPR compliance we do our best to follow the guidelines from our sanctioning bodies the PSI (Pharmaceutical Society of Ireland) and the Irish Pharmacy Union, so, they give guidelines on how to maintain and effectuate GDPR compliance. We implement the guidelines as best as we can.

02:53 **Interviewer:** What effects has GDPR had on the business since its implementation and does it interfere with the business daily operations? Would you describe it as a regulatory burden?

03:02 **Respondent:** Yes I suppose it does, we've had to review how we deal with customers coming through the shop door, like 99% of customers have no issue

with talking about medicine or items that can be audible to others, in that kind of case they have no real fear of someone overhearing what medicine they're on or if they want to order a specific prescription. It's a very small percentage with people who have a problem with taking an order over the counter but we have those customers. So, we've had to change how we can maybe question people at the counter be less audible or a bit more private. It does affect the running of the pharmacy sometimes trying to do that we don't have the space to accommodate everyone. So yes, we have changed our approach to maintain GDPR compliance, it hasn't been an easy process entirely.

04:33 **Interviewer:** As regards to your customers data and storage, who has access to it?

04:44 **Respondent:** Everyone who works in a pharmacy has to sign a confidentiality agreement, that's part and parcel of any part of the pharmacy the staff works in. Be that the Clarins counter, the front shop counter it doesn't matter where you work in the pharmacy you going to be in receipt of confidential information whether you like it or not. Everyone signs up the confidential agreement when they start employment, any breach of that agreement results in immediate contract termination. That's part of the contract that an employee signs, now everyone in this pharmacy has to sign the agreement because that's the nature of the business. In relation to prescriptions in every working environment, you have different levels of activity like you have the shop floor, the pharmacy area, prescription area, blister packs area... Different people work in different areas and as a result of that they have working access to a different parts of the pharmacy. Generally, staff working on the shop floor would have no reason to involve themselves in the prescription area and that would depend on the training and how they progress to different levels and get experience then you have the pharmacist who will always have access to prescriptions that need to be done, technicians and dispensary staff who may not be qualified but have been working in the dispensary for years, they also have access to prescriptions that's never been a problem before and it isn't a problem now. Yea that's how access works in this pharmacy.

06:54 **Interviewer:** What significant challenges has the business encountered with GDPR implementation?

07:05 **Respondent:** Errm.... No with GDPR guidelines, the computers are password protected only members of staff are able to access the dispensing software or email system. It's still a work in progress with getting the right anti-virus software for cybersecurity and having a secure network. I think that any pharmacy in this country would fail to have to GDPR security compliance anti-virus software. We're more proactive about it but not all pharmacies have that, I think pharmacies are doing our best and it takes time and the guidelines change. So, until it finalizes and settles down into something they can home in on and say this is the way it has to be, we are all learning.

08:21 **Interviewer:** How does the business protect its customers data?

08:25 **Respondent:** We have a secure software that is passworded and not all the staff have access to customers sensitive information, only the pharmacist and myself.

08:30 **Interviewer:** What is your opinion about GDPR, data privacy and protection?

08:32 **R:** Well I acknowledge that data privacy and protection are important. I think that for our pharmacy and any pharmacy these records kept have always been confidential. I think its larger companies that harvest personal data, I think that law needs to focus on that side of things because they are using and harvesting personal data. Pharmacies like us we maintain personal data, we don't harvest or use it. You know it's like those companies that are using and abusing the system that's where the focus needs to be for them to get rid of the problem.

09:29 **Interviewer:** Has the business experienced any data breach and what measures does the business have to prevent any data breach?

09:30 **Respondent:** No, we would never have had any data breach, well at least not that I know of then again there are computer hackers out there who have superior knowledge about computers than I ever will. It's possible this has happened in many government entities that have been hacked and their personal data has been harvested. They haven't been able to prevent it, so to say that it hasn't happened in pharmacies or doctor surgeries around the country would be naive to think that hasn't happened. I would say that you do your best, get your anti-virus and security software in place and maintain your own in-house security system. After that then you can do no more because *there's always a superior force out there that can get personal data if they want* (laughs).

10:46 **Interviewer:** Thank you very much for taking time out for this.

10:52 **Respondent:** No problem at all. Thank you for asking me.

## Appendix F- Interview 4

**Speakers** – Interviewer and Respondent (Interviewee)

00:01 **Interviewer:** This interview is solely for educational purposes. Did you understand the plain language statement and consent from that was sent to you?

00:24 **Respondent:** Yes, I did.

00:26 **Interviewer:** Do you agree to have this interview recorded? The responses and your information provided will be coded and strictly confidential as stated in the consent form.

00:36 **Respondent:** Yup.

00:38 **Interviewer:** Could you kindly state your role and what your business specializes in?

00:46 **Respondent:** The business is a credit union and it specializes in retail banking and financial services in the community. My role is the assistant manager, risk manager, compliance officer, data protection officer and training liaison officer.

01:05 **Interviewer:** What does data privacy and protection mean to you and the business?

01:11 **Respondent:** Data protection is very important and part of my work ethic. It's almost the entirety of the business because we deal with a lot of private data. The data is the most valuable thing we have, it's held with the highest regard and it's our top priority to ensure top security for it and things like that.

01:37 **Interviewer:** How does your work relate to GDPR, data privacy & protection and would you say the business is GDPR compliant?

01:49 **Respondent:** Yea so as my role being a data protection officer, I am responsible to make sure that the data procedures are complied with the restrictions and requirements that are in place, so everyone is compliant with them. The other things that we have to do obviously is to give a privacy notice to our members, we make sure that all information is that is being processed are under required, registered interest or they have given consent and we have to rely that same information on our website as well. The other part of my work is that anytime we introduce a new process, or we change processes in regard to data, I have to do a DPIA on it that has to go to the board for review. Ultimately the board is responsible for all actions in the credit union must be informed on a frequent basis from the DPO about our data protection. Along with that all employees have to do an annual data protection and privacy training and sign a fidelity and secrecy bond. Our data related policies have to be reviewed and approved by the board and for any breaches as well, we have a response plan and our cybersecurity insurance, all our technology and stuff like that. All our SLAs have protection in them as well and I'm also registered with the DPC on behalf of the credit union to report any breaches that have happened on our members data.

03:34 **Interviewer:** Would you describe the implementation of GDPR as a regulation burden on the business?

03:46 **Respondent:** I think because we are such high regulators, its actually much of an extra burden because our standards, the expectations of central bank and the DPC on us are especially high so we already had a DPO, annual staff compliance policy, mandatory data protection training, statement to members about how their data is being used and data protection in our SLAs. It has been quite a burden on us especially in the aspect of accuracy because credit unions are around for a long time and they started in volunteerism, a lot of our data have been kept longer than necessary. Although it actually helps the operational side for us to use the regulations as a guiding tool to curb a lot of excess data we don't need anymore.

04:56 **Interviewer:** What effects has GDPR had on the business since its implementation and does it interfere with the business daily operations?

05:06 **Respondent:** I suppose the implementation means that all members of staff even though we have the annual security and confidential declaration anyway for the credit union act. Also, I think daily its more highlighted and on a high level of priority, whereas

maybe before AML (Anti-Money Laundering) was at number 1 for our daily operations. Data protection and privacy is on par with that, so we're always conscious of who were talking to, when we're talking to you and its definitely affect the daily operations of the staff downstairs that work at the counter. We have tightened up our security and given them a better sense of consistency. Everyone is in committing the same, everything is in black and white now. So, it does interfere with the daily business operations.

06:11 **Interviewer:** What significant challenges has the business encountered with GDPR implementation?

06:18 **Respondent:** The biggest challenge we'd have would be the volume of work to reassess and curb all the data we had because our organization is over 50 years old. So, a lot of our records would have been the old mentality, which was created years ago, we had to go through the records re-categorize, re-process and re-catalogue everything. This obviously had a financial impact we had to set money aside and we weren't prepared to do that project at the time. It had a financial impact even though it was an investment and we have an extra third-party data protection provider that we use, that manages and stores data for us.

07:24 **Interviewer:** How does the business protect its customers data? And also, in terms of access and who controls the access?

07:38 **Respondent:** The customer data is seen as the crown jewel within the organization, so we have several layers of security including IT, physical security, and other layers. There's not one access to any data, you'd have to get through at least 4 verification steps to access any personal data and even at that its peers depending on your role within the credit union you can access different types of data. Then obviously as an employee move through their access levels will change, if you're promoted from your last role your access will change accordingly.

08:32 **Interviewer:** Do the employees sign a GDPR compliance contract as data controllers and processors?

08:34 **Respondent:** Yea how that works is because we already had the fidelity and secrecy bond in place since the 1960s. That's an annual declaration that you will make sure to maintain the secrecy of information and with the annual training all employees and volunteers have to acknowledge it during the exam at the end of the training. They have to pass it the exam and ensure that their knowledge is up to date and with the annual policy everyone has to read and sign it in respect of the standards. We also have annual refreshers, so they know the data protection standards and are published for members. In the monthly staff meeting there's an auditing board for IT and physical security that's done so if there's any unauthorized access it would be raised by the compliance officer which would be me as well then I would update it at the staff meeting and it would be dealt with.

09:50 **Interviewer:** What is your opinion about GDPR, data privacy and protection?

09:56 **Respondent:** I think in my role it's great because it makes it more black and white. It makes it more newsworthy, so it's easier for me to raise concerns and bring it to the board because everyone now knows about GDPR whereas before that data protection wasn't very important. It wasn't making news headlines all the time and wasn't in the mind of the board. Now everyone understands GDPR and values data protection, it's gives black and white instructions, there's no more interpretation it is the principles that are put in place. It kind of gives a consistency not only in our organization but on our labour, organization are making sure that all credit unions are maintaining one distinct level.

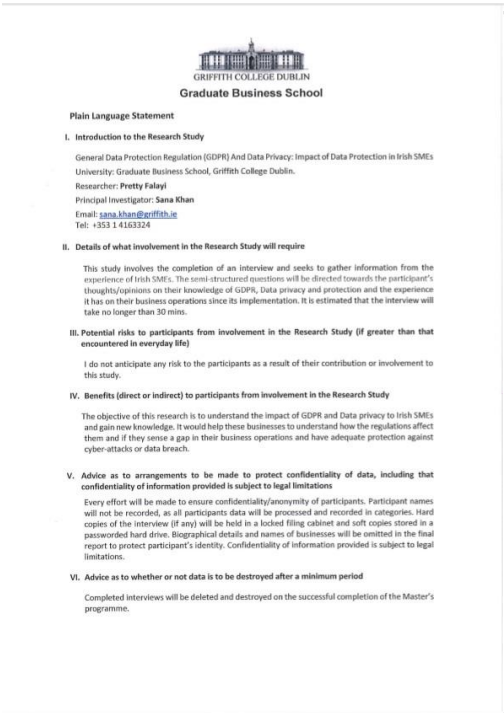
10:48 **Interviewer:** Has the business experienced any data breach and what measures does the business have to prevent any data breach?

11:03 **Respondent:** Yea we've had some data breaches in the past and after that we put all the measures, verification controls and securities in place. The breaches that we've had are extremely minor, we don't have any large scale of data breach. There's the control room where no one would personally be able to access or hack. So, what we've done is training and updated our procedures, before any data goes out, we have a second pair of eyes look at it so it's not just one person handling sensitive data. Obviously going with the lessons learned, anytime something goes wrong even though it's not an actual data breach. We have a lessons learned register, we register it and then start testing it to find the root cause and then we go about fixing it.

12:25 **Interviewer:** Thank you so much for taking time out of your busy schedule for this.

12:34 **R:** No worries at all.

## Appendix G- Sample Plain language Statement & Consent Form



GRIFFITH COLLEGE DUBLIN

**Graduate Business School**

**Plain Language Statement**

**I. Introduction to the Research Study**

General Data Protection Regulation (GDPR) And Data Privacy: Impact of Data Protection in Irish SMEs
University: Graduate Business School, Griffith College Dublin.
Researcher: **Pretty Falayi**
Principal Investigator: **Sana Khan**
Email: sana.khan@griffith.ie
Tel: +353 1 4163324

**II. Details of what involvement in the Research Study will require**

This study involves the completion of an interview and seeks to gather information from the experience of Irish SMEs. The semi-structured questions will be directed towards the participant's thoughts/opinions on their knowledge of GDPR, Data privacy and protection and the experience it has on their business operations since its implementation. It is estimated that the interview will take no longer than 30 mins.

**III. Potential risks to participants from involvement in the Research Study (if greater than that encountered in everyday life)**

I do not anticipate any risk to the participants as a result of their contribution or involvement to this study.

**IV. Benefits (direct or indirect) to participants from involvement in the Research Study**

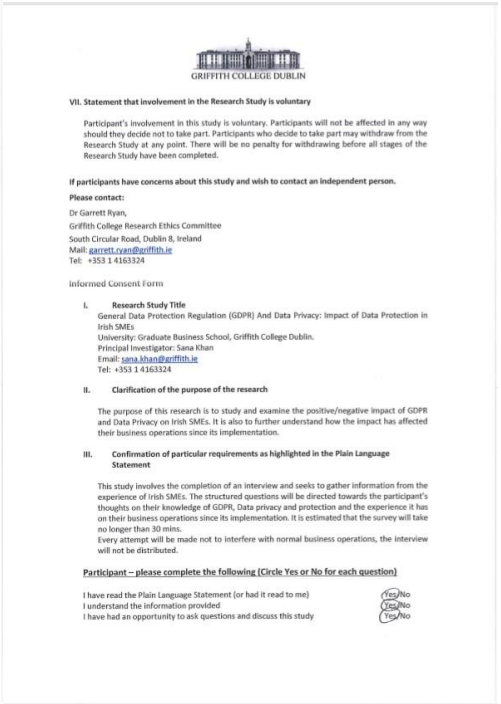
The objective of this research is to understand the impact of GDPR and Data privacy to Irish SMEs and gain new knowledge. It would help these businesses to understand how the regulations affect them and if they sense a gap in their business operations and have adequate protection against cyber-attacks or data breach.

**V. Advice as to arrangements to be made to protect confidentiality of data, including that confidentiality of information provided is subject to legal limitations**

Every effort will be made to ensure confidentiality/anonymity of participants. Participant names will not be recorded, as all participants data will be processed and recorded in categories. Hard copies of the interview (if any) will be held in a locked filing cabinet and soft copies stored in a passworded hard drive. Biographical details and names of businesses will be omitted in the final report to protect participant's identity. Confidentiality of information provided is subject to legal limitations.

**VI. Advice as to whether or not data is to be destroyed after a minimum period**

Completed interviews will be deleted and destroyed on the successful completion of the Master's programme.



GRIFFITH COLLEGE DUBLIN

**VII. Statement that involvement in the Research Study is voluntary**

Participant's involvement in this study is voluntary. Participants will not be affected in any way should they decide not to take part. Participants who decide to take part may withdraw from the Research Study at any point. There will be no penalty for withdrawing before all stages of the Research Study have been completed.

**If participants have concerns about this study and wish to contact an independent person.**

**Please contact:**

Dr Garrett Ryan,
Griffith College Research Ethics Committee
South Circular Road, Dublin 8, Ireland
Mail: garrett.ryan@griffith.ie
Tel: +353 1 4163324

Informed Consent Form

I. **Research Study Title**
General Data Protection Regulation (GDPR) And Data Privacy: Impact of Data Protection in Irish SMEs
University: Graduate Business School, Griffith College Dublin.
Principal Investigator: Sana Khan
Email: sana.khan@griffith.ie
Tel: +353 1 4163324

II. **Clarification of the purpose of the research**

The purpose of this research is to study and examine the positive/negative impact of GDPR and Data Privacy on Irish SMEs. It is also to further understand how the impact has affected their business operations since its implementation.

III. **Confirmation of particular requirements as highlighted in the Plain Language Statement**

This study involves the completion of an interview and seeks to gather information from the experience of Irish SMEs. The structured questions will be directed towards the participant's thoughts on their knowledge of GDPR, Data privacy and protection and the experience it has on their business operations since its implementation. It is estimated that the survey will take no longer than 30 mins.
Every attempt will be made not to interfere with normal business operations, the interview will not be distributed.

**Participant – please complete the following (Circle Yes or No for each question)**

I have read the Plain Language Statement (or had it read to me) Yes No
I understand the information provided Yes No
I have had an opportunity to ask questions and discuss this study Yes No

GRIFFITH COLLEGE DUBLIN

I have received satisfactory answers to all my questions (Yes/No)
I am aware that my interview will be audiotaped (Yes/No)

**IV. Confirmation that involvement in the Research Study is voluntary**

Participant's involvement in this study is voluntary. Participants will not be affected in any way should they decide not to take part. Participants who decide to take part may withdraw from the Research Study at any point. There will be no penalty for withdrawing before all stages of the Research Study have been completed.

**V. Advice as to arrangements to be made to protect confidentiality of data, including that confidentiality of information provided is subject to legal limitations**

Every effort will be made to ensure confidentiality/anonymity of participants. Participant names will not be recorded, as all participants data will be processed and recorded in categories. Hard copies of the interview (if any) will be held in a locked filing cabinet and soft copies stored in a passworded hard drive. Biographical details and names of businesses will be omitted in the final report to protect participant's identity. Confidentiality of information provided is subject to legal limitations.

**VI. Signature:**

I have read and understood the information in this form. My questions and concerns have been answered by the researchers, and I have a copy of this consent form. Therefore, I consent to take part in this research project.

**Participants Signature:** [redacted]

**Name in Block Capitals:** [redacted]

**Witness:** [redacted]

**Date:** 15/6/2020