A study of the GDPR impact on the EU SMEs and their competitive advantage

SYED, HASSAN I.

Professor Vincent English
Name of Approving Faculty Member
For Approval

Student Name: Syed Hassan
Student Country: Canada
Program: DBA
Course Code or Name: DBA
Doctoral Supervisor: Professor Vincent English

This document uses ☒ US English (for spelling, punctuation rules and formatting of references). Rule of Style used: APA6 (footnotes). End Notes have been used for footnotes and to generate the bibliography.
Note: This document is in US A4 format

GDPR IMPACT ON THE EU SMEs

by

SYED HASSAN, I.
DBA, UNINETTUNO, ITALY
PhD, PÔLE UNIVERSITAIRE EUCLIDE
LLM PÔLE UNIVERSITAIRE EUCLIDE
GRADUATE DIPLOMA, BPP UNIVERSITY, UK
GRADUTE DIPLOMA, UNINETTUNO
LLB (HONS), BPP UNIVERSITY, UK
P.E, P.ENG, ASCE USA

Presented to the Faculty of Business Studies (UNINETTUNO University)
School of Economics & Business Studies
in Partial Fulfilment
of the Requirements
for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION (DBA)

UNINETTUNO | INTERNATIONAL TELEMATIC UNIVERSITY
SCHOOL OF ECONOMICS & BUSINESS STUDIES
www.uninettunouniversity.net

Nov 2024

DECLARATION

I, Syed Hassan I., hereby declare that this thesis entitled "**Impact of GDPR on EU SMEs**" is my own original work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material. All quoted materials are duly cited and acknowledged.

This thesis has been solely submitted to the Università Telematica Internazionale UNINETTUNO. This thesis has been approved and accepted for the award of Doctor of Business Administration through from the University's DBA Programe in the year 2024.

Signed this 3rd day of December, in the year 2024. This is a truthful declaration and attestation.

Syed Hassan I.
Canada

ACKNOWLEDGMENT

Graduate studies especially doctoral studies demand discipline, focus, determination and finally, supervisors, who can keep the students going. I am fortunate to have Professor Vincent as my supervisor. His gracious support and extremely knowledgeable guidance have been the driving force behind all my endeavours. His sense of humour and the ability to motivate the cohort has been a blessing. I would not have been able to complete this journey without his ardent support. I am forever in his debt. Last but not least, I want to acknowledge my loving family, without their support, I would not have persevered. Thank you all.

ABSTRACT

22 million EU SMEs form 70% of all EU businesses and employ 90% of the EU workforce. The emergence of personal data as the most valuable commodity started with converting global economies into digital economies since the advent of the *World Wide Web*. The services offered by the smallest legal businesses to the largest multinational corporations rely on accessing, storing, and processing consumer data. Artificial Intelligence (AI), 5G and the Internet of Things (IoT) etc., create opacity about the actual ownership of data. Data aggregation and identifying consumer behaviour through their data for customised web-based services in now a norm. The monetizing of consumer data at all levels has changed the face of technology innovations. This applies to *B2C* and *B2B* technology landscape. Tech giants like Google, Apple, Amazon, Microsoft, etc. lead the global stock values.

The technology products offered by these tech giants are technology variants based on mass consumer data. New secondary markets have emerged within the global data value chain, such as Blockchain. Financial Derivatives packaged on the stored volume of personal data valued on consent are traded on the global financial markets. Such vast and complex uses of personal data have raised serious concerns from regulators to consumers alike.

The Trillion-dollar data-driven global economy faces challenges. EU law has been at the forefront of protecting a natural person's data as a fundamental right. United States law treats personal data as a property right and affords different protections but not as a fundamental right. The different legislative approaches to natural person data created tensions between the two most prominent players in the US$4.8 trillion data markets. On the 25th of May 2018, enforcement of the EU General Data Protection Regulation (GDPR) ushered in a new era of business law that has a transnational effect within the EU-27 and has international reach. Within EU-27, the 22 million EU SMEs face the challenge of implementing and complying with GDPR as a legal obligation. There is no opt-out for these EU SMEs. The essence of GDPR is the personal data protection of natural persons. Its scope, however, is purely business. Thus, all EU businesses will have to comply with GDPR.

Since EU SMEs form 90% of the EU's business incorporations and employ 96% of the EU's workforce. The business and legal implications due to compliance with GDPR are huge. GDPR also raises the stakes for their competitiveness and business modelling going forward. Global companies are still exploring the impact of GDPR due to its international reach and the steep fines associated with any GDPR breaches internationally concerning the use of EU residents' data. This research aims to study the impact of GDPR on EU SMEs. This research aims to find the GDPR impacts on the competitiveness of the EU SMEs within the global digital economy.

TABLE OF CONTENTS

CONTENTS

1) INTRODUCTION

a) Background

This research is about the impact of the European Union (EU) General Data Protection Regulation (GDPR) on the EU SMEs. The research seeks to answer questions related to the GDPR's impact on SMEs due to their mandatory compliance with GDPR. Those questions relate to the cost of compliance, challenges faced by the SMEs for compliance and the overall competitiveness of SMEs post-compliance. The competitiveness question directly speaks to the SMEs having business strategies related to the GDPR.

GDPR came into force on May 25th, 2018, as an EU-wide data protection legislation that carried stiff penalties for potential violations. Scant research has emerged about the impact of GDPR on EU SMEs. This research aims to study the impact of GDPR impact on the competitive advantage of EU SMEs. The availability of limited research and data about the impact of GDPR on EU SMEs poses challenges for this research. The researcher aims to mitigate this challenge by using Pollfish as a platform to collect data for this research and collaborate with EU data collection agencies that are conducting their research on EU GDPR roll out through their various programs.

The 21st-century business is all about data. Data drives the direct digital economy business based on ICTs valued at US$4.8 Trillion or 7% of the US$80 Trillion global GDP. (*GDP Growth (Annual %) | Data*, 2019) GDPR is considered the EU's legislative response to the growing business use of natural person data in industries across the globe. (Regulation, 2016) Limited research has emerged on its business implications for SMEs.(Brodin, 2019b) The internet giants such as Google, Microsoft, Facebook, and Amazon (GMFA) are at the top of the global digital value chain. Small and medium enterprises (SMEs) comprise the main body of the value chain. Figure 1 below shows the GDPR scope outside the EU.

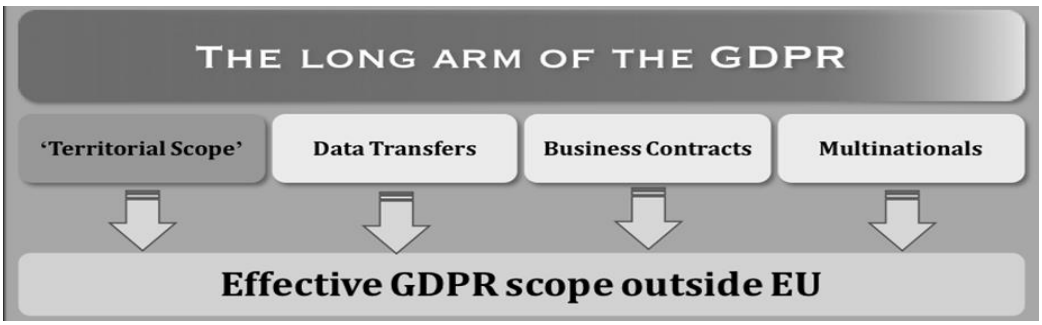


Figure 1-GDPR Scope

b) Research Aim & Objectives

This research aims to study the impact of GDPR compliance on EU SMEs for their competitive advantage. There is presently limited research published on GDPR's impact on EU SMEs. Therefore, this research is exploratory.

The aim of this research will be tested by:

- *Conducting* qualitative research of select literature and secondary data
- *Using* quantitative research based on online surveys conducted with 600 professionals from 50 EU SMEs directly impacted by GDPR. The surveys are blind and the pool of 600 participants was selected from an initial pool of 1500 participants by using a screening/reverse-validity question.

c) The Research Objectives:

Does compliance with GDPR increase the competitiveness of EU SMEs? In that:

- Does the GDPR negatively impact the EU SMEs' competitiveness?
- What is the level of GDPR compliance preparedness of EU SMEs?
- Does the GDPR increase the cost of doing business for SMEs?
- Has GDPR improved the privacy policies of EU SMEs?

d) Research Context

The Internet has given a new meaning to the monetization of data in all forms (Peter Buell Hirsch, 2019). Data is critical for SMEs as part of the global digital value chain. In Asia, 60 to 90 per cent of all businesses are SMEs. These SMEs employ 50 to 98 per cent of the working population. These SMEs contribute 35 to 70 per cent of Asia's total GDP. The Asian SMEs use European data. This links Asian SMEs to the EU data value chain.(Yoshino & Taghizadeh Hesary, 2016)

In 2016, the EU's SMEs linked to data business numbered around **255,000**. These numbers are expected to increase to **350,000 by 2020**. These SMEs employ 6.16 million Europeans as of 2016. The number of EU SME workers linked to data business will cross 10 million by 2020. The workforce growth rate has been 14% per year since 2012. These SMEs generated over US$60 billion in 2016. These revenues will cross US$120 billion by 2020. The data economy of the EU is over $350 Billion. US$ 230 billion of this EU data business is controlled by non-EU companies. Some of those companies are Amazon, Facebook, and Google. EU data business showed the highest growth of any one sector, averaging 5% per year since 2012. (EU DSM Report, 2017)

The future impact of GDPRs on the global data economy is an emerging area of business research. (Li et al., 2019) The crucial role of data in the worldwide economy is settled research. It is still not settled who owns the '*internet*' or the '*World Wide Web*'.(Goldsmith & Wu, 2018.) There is a growing global tussle for controlling the data business. Some examples are the French effort to tax tech giants, the US-China trade war, and US-China Huawei's 5G technology tussle. The impact of GDPR on global business and the compliance issues are shown in figure 2.

Figure 2: GDPR Compliance- EU SMEs (source: https://smedata.eu/)

Krasteva et al. (2015)(Krasteva et al., 2015) and Campbell et al. (2015)(Campbell et al., 2015) are the most recent research on regulatory compliance and its impact on technology firms. Both researchers present theories that regulatory compliance costs can create barriers to entry and may thus hurt innovation. Campbell et al. assert that regulatory compliance increases the cost of doing business. The adverse effects of such costs are more severe for SMEs. Krasteva et al. assert that increased regulatory compliance costs favour large and established firms. Their research supports our hypothesis that GDPR will have implications for EU SMEs. The legal context of GDPR underpins this research. The focus remains to study the business implications of GDPR.

e) The Research Hypothesis

A preliminary research model was created to conduct data sampling and derive constructs and variables to define a hypothesis model. The impact of GDPR on EU SMEs realises its aims by creating (some) competitive advantage through harmonization of SME business across Europe. The five GDPR principles, minimizing the use of personal data, the purpose limitation, confidentiality of data including storage, lawfully defined use of data and ensuring the integrity of data use are the foundation for the hypothesis model. The constructs are the variables which by definition have a negative construct when applied to the foundational principles of GDPR applied to EU SMEs. The dependent variable that emerges is the impact of GDPR on EU SMEs and their competitive advantage.

The hypothesis has been developed by testing the five core principles of GDPR with the independent variables. All independent variables are negative constructs for EU SMEs in terms of their application. The independent variable when assumed as negative constructs, when applied to the dependent variable provides the ground for the hypothesis..

‘**This thesis hypothesises that : GDPR will adversely impact the EU SMEs and increase their cost of doing business and positively impact by improving the data protection and consequently win the favour of EU consumer confidence**. ’

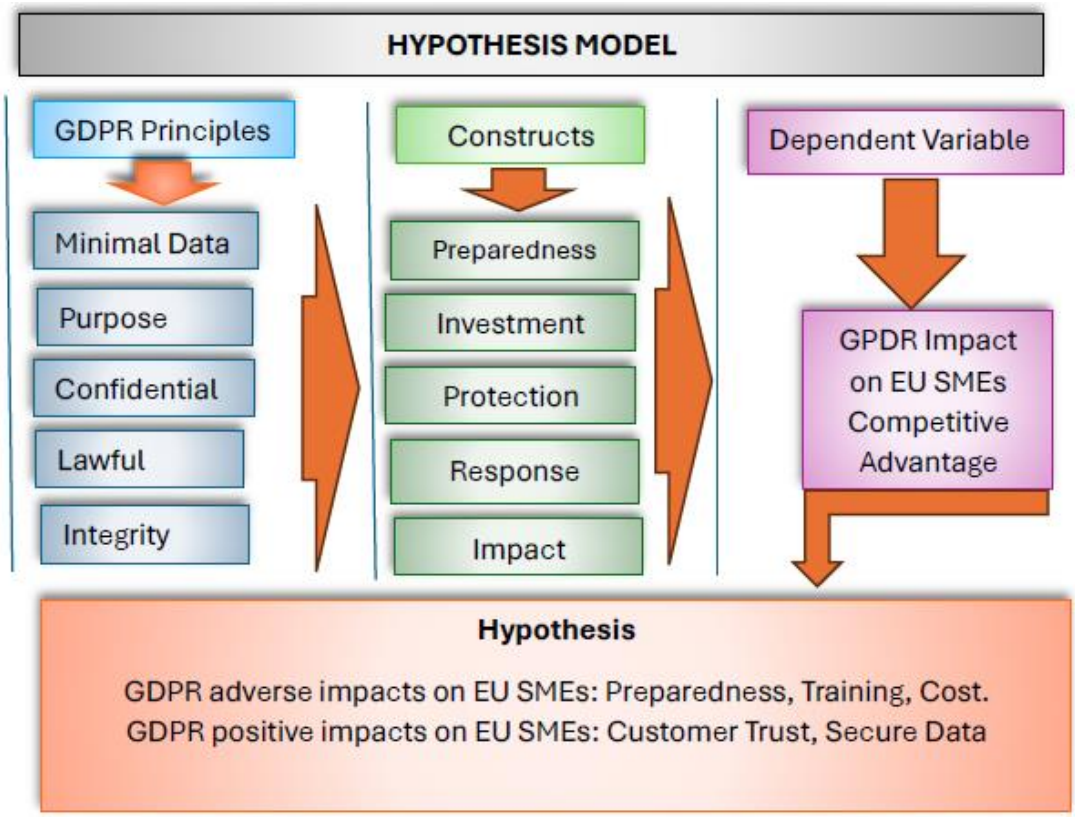


Figure- Hypothesis Model

The hypothesis model in the figure above needs to be tested. To prove this hypothesis, the researcher intends to collect data across the EU-27 from EU SMEs and support the analysis with statistical data interpretation and literature review.

To disprove this hypothesis, the researcher will critically examine the statistical analysis for errors and opposing literature review.

The hypothesis will be tested through methodological quantitative analysis of collected data.

The research questions have been framed to examine for statistical analysis:

- Collect data only from EU SMEs and discard data from SMEs outside the EU-27. Since the UK has left the EU, any data collected from the UK will be used as the control group.
- Frame a question that would allow opposite coding to remove any false data collected.
- Statistical analysis based on independent variables such as age, income, nationality, sector of professional work, level of work within the sector etc.
- Statistical analysis for the focused area of the hypothesis that projects GDPR and its impact on SME's competitive advantage, cost of doing business and regulatory fines for non-compliance.

f) Research Methodology

Business by its very nature, falls under the category of '*soft*' sciences. On the other hand, mathematics is termed as the '*Queen of science'.* Mathematics is, therefore, in the quantifiable category of '*hard*' sciences. The social sciences evolved through the emancipation of philosophical constructs while the 'hard' sciences matured through increased quantification.

The knowledge of business also relies heavily on hard mathematical science. This mix of business soft and hard sciences results in evolving business paradigms. Business paradigms are the *informed* and *sophisticated* views of human construct. (Guba & Lincoln, 1994) The acceptance of paradigms is based on their *persuasiveness* and *utility* which requires *proof.* (Guba & Lincoln, 1994, p. 166) Mathematical data help in gleaning the proof. '*Qualitative*' and '*Quantitative*' are umbrella terms that describe the methods adopted for the research.(Anand et al., 2020, p. 1652) It has been argued that in business research, the question of *methods* is secondary to the question of *paradigm*s. (Guba & Lincoln, 1994, p. 101) GDPR business implications for EU SMEs are the paradigm in this research.

Context is paramount for research objectives examining business problems. Qualitative methods provide the contextual information to guide the business research context. The quantitative methods correct the disparities in the context and qualitative findings. Contemporary business research leans towards a '*Mixed Method'* approach to study business problems. The mixed method approach allows the integration and interpretation of quantitative and qualitative findings.(Tashakkori & Creswell, 2007)

The 'world-view' analysis of EU GDPR will be based on Pragmatism. Pragmatism helps connect induction with deduction, subjectivity with objectivity, and generality with context and develops research inter-subjectivity and transferability within various parts of the research. (D. L. Morgan, 2007)

The word '*methodology*' adds a dimension of *complexity* to the word '*method*'. The added dimension of complexity is the philosophical framework and fundamental assumptions that are formed by the researcher. The methodology framework drives the entire process of the research. The use of surveys, focus groups, interviews, historical data and literature are all part of the research design. The research design of this study is based on Creswell's (2003) conceptual and methodological mix methods. The conceptual and methodological mix method research design is shown in Figure 3 below.

	Qualitative	Quantitative
Conceptual	Narrative data Using inductive approach to understand and solve the research problem	Numerical data Using detective process to proof the research question
Methodological	Data are collected through participant observation and interviews Data are analyzed by coding scheme	Data are collected through surveys and check list Data are analyzed through descriptive and inferential statistic

Figure-3 Conceptual and Methodological Model of Creswell

Mixed method research is defined as research in which the theoretical assumptions guide the collection and analysis of data based on the mix of qualitative and quantitative methods in a single study, according to Creswell (2003). The combined effect of qualitative and quantitative methods improves the research outcomes. The combined approach has also been termed 'integrated', 'mixed', 'hybrid' and 'methodological triangulation approaches. (Parylo, 2012, p. 257) The mixed-method method is preferred in social sciences such as business research. Methodological triangulation will be used to connect the contextual theories with the qualitative and quantitative findings.

The mixed-method research in this study focuses on the business dimensions that underpin GDPR. The business implications of GDPR on EU SMEs remain the primary focus of this research. There are multiple dimensions of the business implications for SMEs due to GDPR. The effectiveness of the Mixed Method Approach is proven to tackle multiple dimensions in a single study for complex business problems. This research relies on Creswell's Mixed Method Approach (2012). The research will use the triangulation method to describe the logical relationship between the theoretical concepts and the quantitative and qualitative findings. The Erzberger and Kelle triangulation model (figure 4) will be used for the mixed-method research.(Kelle & Erzberger, 2003)

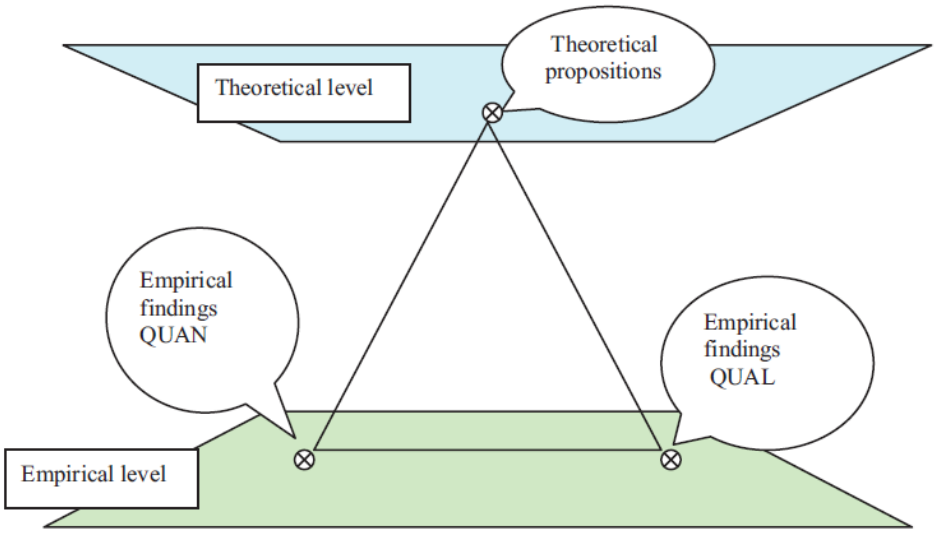


Figure 4: Triangulation for Findings in Mixed Methods Approach

g) Research Structure

There is an increasing demand for cost-effective and applied business research. These demands are driven by the business community's calls for moving away from theoretical research. The trend is to move towards research that can drive business policy and fulfil the practitioners' needs. This research is focused on the applied business implications of GDPR on EU SMEs. The research structure is explained in the figure below. This research started with defining the research problem and the formulation of research questions. The literature review on the topic guides the framing of the questions for the survey questionnaire.

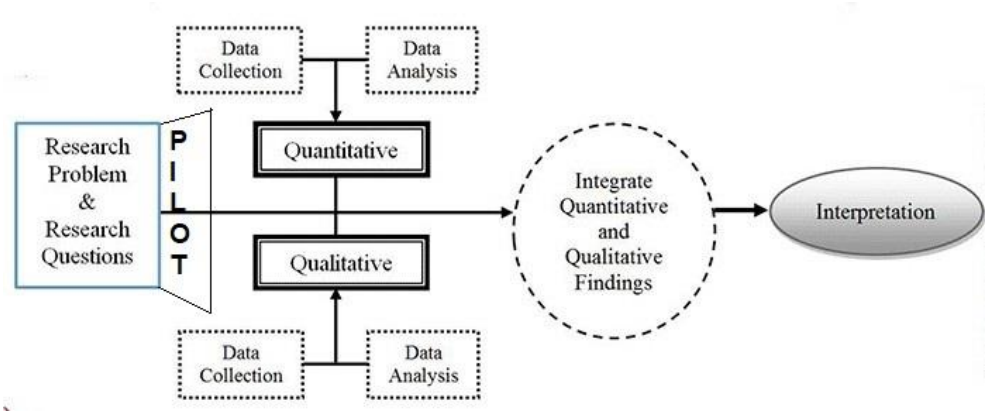


Figure 5: Research Design Model- Integration of Findings

The high-impact areas of GDPR on the business functioning of the SMEs are shown in Figure 6 below. These high-impact areas are based on the preliminary review of the literature on the topic.

Figure 6: High-Impact of GDPR Compliance

h) SMEs/Participants Selection for Research Survey

EU SMEs that are part of the EU digital economy have been identified as the target for the research. Participants working in these EU SMEs are employees who hold various management and non-management positions that are directly linked to GDPR compliance in their SMEs. PollFish has been used as the online survey platform to publish the survey online and also to ensure data protection law compliance of the survey. These SMEs are part of the 700 EU SMEs network participating in the SME-focused GDPR business research project.

An SME's Competitiveness Analysis Model has been created for this research. The model is based on the existing key research on the topic by Bordin et al. 2015. The model is also based on the strategic business modelling guidelines for SMEs participating in the technology supply chain Johnson et al. 2015 **Strategic Management Model**.(Raynard et al., 2015, p. 10) Figure 8 below is the model proposed for this research.

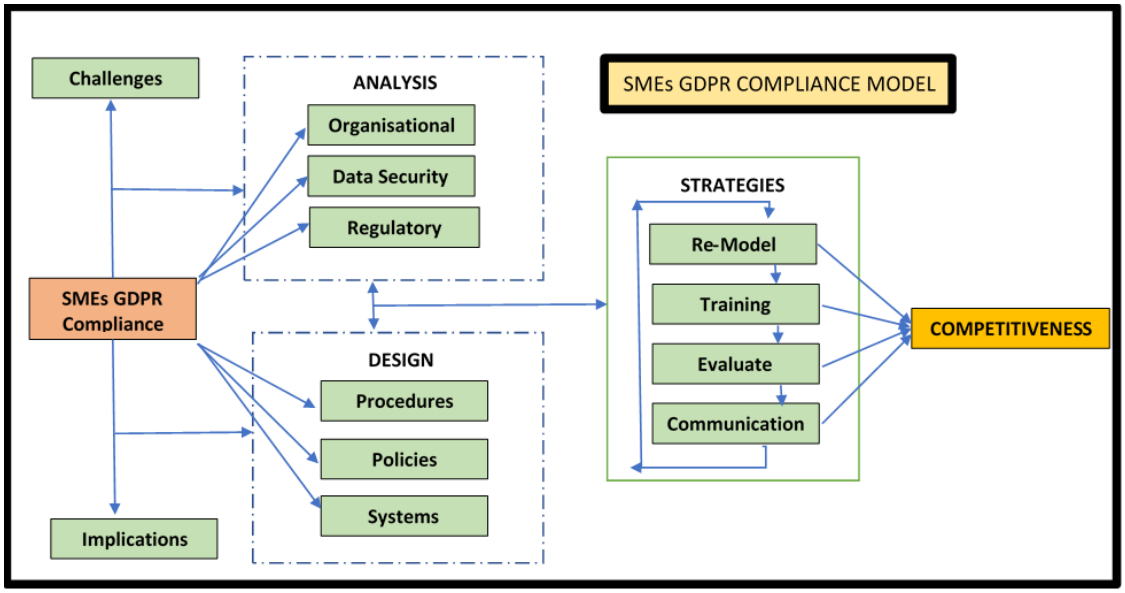


Figure 8: SME Competitiveness Model for GDPR Compliance for this research

i) Statistical Data Analysis

The use of Logistical Modelling techniques in business statistical data interpretations and inferences is a leading approach. Binary logit models allow researchers to use the collected data and infer if a certain variable, significantly impacts and affects the outcomes. We chose the binary logit model approach to study the GDPR impact on EU SMEs as it allows for a focused inference as a standard approach for testing the predictive value of GDPR on EU SMEs.

Logistical models including binary logistical models allow business researchers to process dependent data by assigning values of 0 or 1. In the case of our research, the modelling would help explain if the EU SMEs experienced a negative or positive impact post-May 2018, due to the implementation of GDPR.

Binary Logistic regression is also commonly used in business research for the prediction and classification of unique problems such as the imposition of mandatory regulations and sanctions. Lastly, the robustness of the data collected can be tested using the Binary Logistic regression models as they can identify data anomalies, such as false data.

The GDPR not only applies to and impacts EU SMEs, it also impacts EU SMEs' business across the EU borders. The transnational reach of GDPR on the EU SMEs has been catered to by using the Ordinary Least Squares (OLS) regression technique. OLS

regression technique for binary logit modelling is the best-known approach for variables that require global modelling using spatial regression analyses.

OLS regression has been chosen as an optimization strategy for a straight line or the closest possible data points for the linear regression equation formulated for this research. OLS is also considered the best optimization strategy within business research for binary regression models to find unbiased real value estimates for the beta.

j) Survey for the Statistical Analysis

The questions for the surveys and a brief on each question posed to the participants, followed the EU Regulation 2016/679 framework for conducting the research.

The framework defined in EU Regulation 2016/679 for conducting research has been successfully used in earlier research projects for assessing GDPR compliance and readiness globally. The framework is based on the GDPR data principles of legality, loyalty, transparency, specified objective, limitation of data to be collected, accuracy, limitation of storage time, integrity, confidentiality, and accountability. Figure 8 below shows the four key areas of GDPR that must be factored in when considering compliance for SMEs.

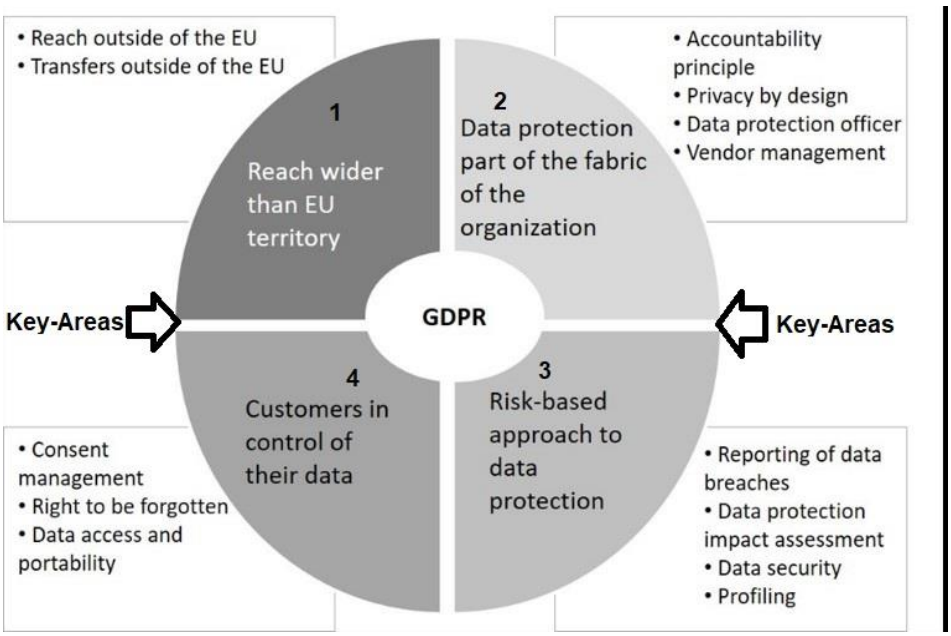


Figure 8: Four key areas of GDPR Compliance for SMEs

The questionnaire is focused on specific areas within the business operations of the selected SMEs, as elaborated in Figure 6 and Figure 7 above. The areas highlighted for mandatory compliance that impact the SME's ability to comply are shown in Figure 8 above. The sub-areas of business operations of the SMEs that the GDPR directly impacts are shown in Figure 9 below. The questions for surveys were factored in the scope of the responsibilities as per the business operations of the SMEs shown in Figure 9 below.

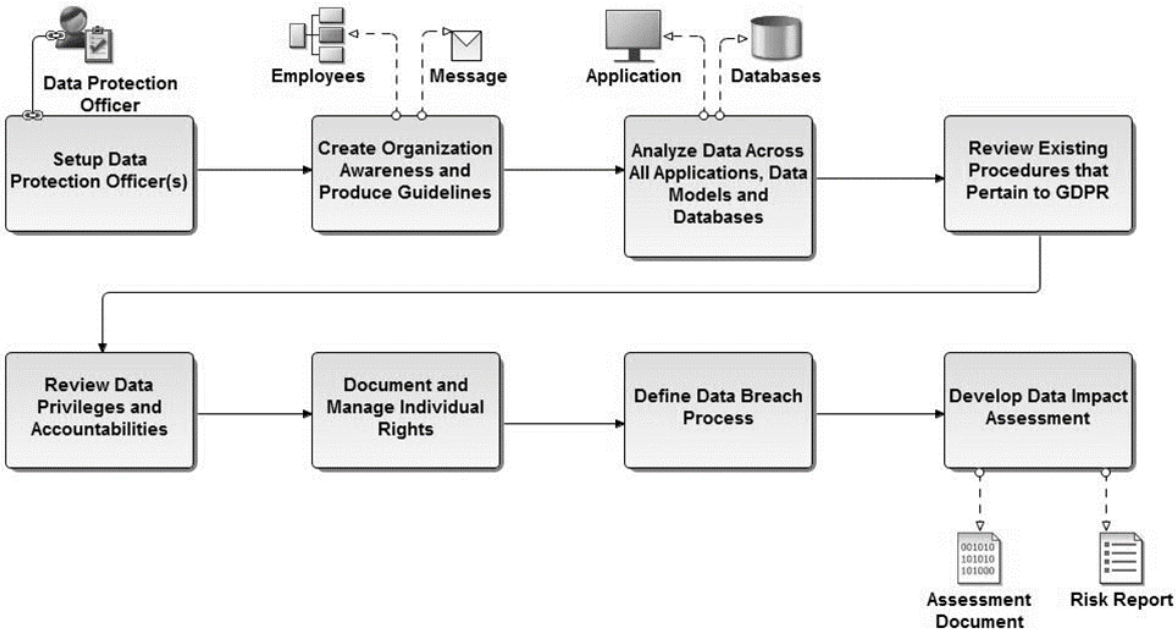


Figure 9: Scope of Business Responsibilities within SMEs for GDPR

The Pollfish publisher platform was used for the interviews/surveys. The online system helped economise on the financial/ human resources and time. (*Publisher's Terms of Use and Privacy Policy - Pollfish*, 2020.)

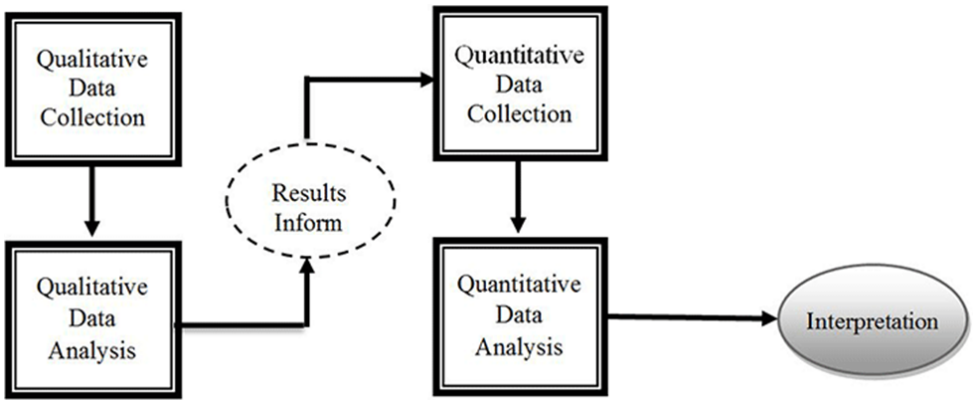


Figure 10: Sequence of Data Interpretation from the Research

k) Data Interpretation Sequence

The sequence of drawing interpretations from the data collected after the completion of the pilot is shown in figure-10 above. The data analysis from the secondary data sources and qualitative review of the literature also confirmed the findings and subsequent research conclusions. The quantitative data analysis followed the qualitative analysis.

The results from the qualitative analysis and the quantitative analysis were interpolated. The dotted '*Results Inform'* in the above Figure-10 reflects the interpolation step of the quantitative analysis with the initial qualitative data analysis. Ivankova et al. (2009) explain this as an 'exploratory' sequential mixed-method design. (Ivankova & Creswell, 2009, p. 136)

GDPR is a new area of research. This research will be amongst the first concrete efforts to explore the business impact of GDPR on EU SMEs. Exploratory research design using mixed methods is the preferred design for new areas of business research according to Creswell et al. (2017).

The qualitative literature review(n=x) was used, based on keyword search criteria through databases SCOPUS hosts and World of Science. The qualitative data about SMEs for developing the hypothesis and initial research questions was sourced from the EU SME DATA project (https://smedata.eu). SME data through the SME DATA project is focused on the EU SME's performance impacted by the GDPR.

The data from the EU Barometer Project database GESIS was used to cross-check the data from the SME DATA project. These databases have been selected because of their alignment with the EU GDPR framework chosen for the research.

2) LITERATURE REVIEW

a) Introduction

This research aims to study the impact of GDPR on EU SMEs vis-à-vis their competitive advantage. The research has a business scope, while the nature of GDPR is technological and it's grounded in EU law. The interdisciplinary nature of the research demands that the data and law aspects of GDPR must be considered while conducting the literature review for the business implications at the heart of this research.

The interdisciplinary nature of GDPR combined with the limited research emerging on the topic, places limitations on this research. Notwithstanding these limitations, this literature review endeavours to conduct a systematic literature review of the existing literature that has emerged since the enforcement of GDPR in May 2018.

The hypothesis of this thesis is grounded in the initial literature review that indicates a negative implication of GDPR on the EU SME's competitive advantage. This systematic interdisciplinary literature review of the existing literature seeks to test the hypothesis by putting forth the following questions:

- Research Question 1- Does the GDPR negatively impact the EU SMEs' competitiveness?
- Research Question 2- What is the level of GDPR compliance preparedness of EU SMEs?
- Research Question 3- Does the GDPR increase the cost of doing business for SMEs?
- Research Question 4- Has GDPR improved the privacy policies of EU SMEs?

The researcher has found considerable online materials in the shape of blogs and websites dedicated to helping and providing information for EU SMEs to prepare for GDPR compliance. Limited academic research focused on the business implications of GDPR has emerged since its enforcement in May 2018. The research on GDPR and its business impact on EU SMEs is even smaller.

One of the reasons observed from the preliminary review of the literature indicates barriers in collecting primary data from SMEs within the EU-27 that pertains to information that is specific to the data usage within the businesses of EU SMEs. This research aims to provide baseline data specific to the business implications of GDPR and focuses on the EU SMEs. The findings of this research will provide methodological foundations for future research through the correlation of interdisciplinary findings.

b) Search Methodology

The *preferred reporting items for systematic reviews and meta-analysis* (PRISMA) guidelines have been employed to conduct a systematic interdisciplinary literature review for this thesis. The search for literature from reputable journals, EU proceedings and various web sources was conducted between February 2021 and November 2023. Scopus and Web of Science databases were used for peer-reviewed journals and their ethical access.

The relevant research was carried out using the databases with parameters based on title, abstract and keywords relevant to the business nature of this research. The database searches utilized the Boolean operators ('And' / 'Or') for various combinations of GDPR impact on the EU SMEs.

The search keywords used for extracting the business-focused literature were:

["GDPR" OR "general data protection regulation] AND ["implications" AND "competitive advantage"] AND ["EU" OR "European Union" OR "EU SMES"]

c) Selection Criteria for Inclusion and Exclusion

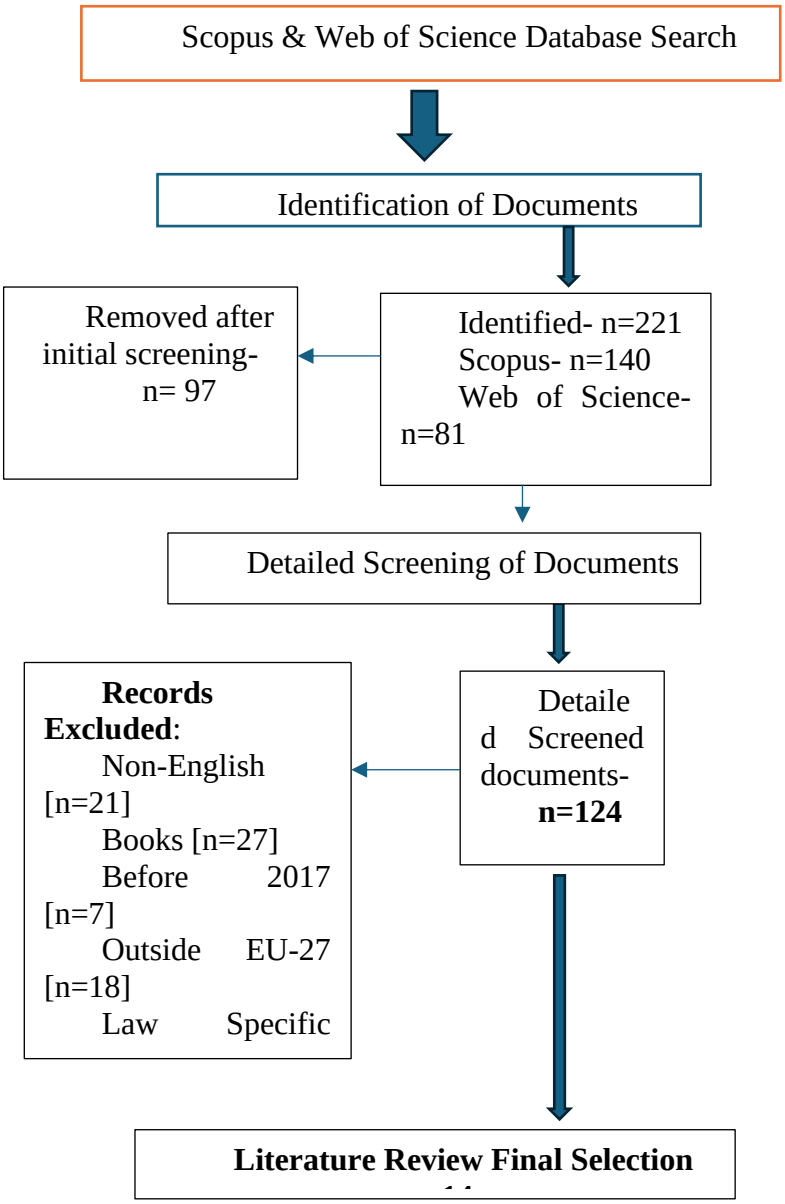
The search was focused, on further narrowing down the selection based on the type of literature document, year of publication and the scope of the research. The Scopus and Web of Science searches yielded 221 documents and after an initial screening of non-specific literature, 124 documents were selected for detailed screening.

A selection criteria model was developed to include or exclude documents. A model was developed to select potentially relevant business studies of GDPR. The model below explains the final selection of the literature used for the interdisciplinary literature review.

The books and periodical series were removed because of potential author bias and traditionally, books have a lower threshold of review compared to robust peer-reviewed journal articles. Non-English language-based research was excluded due to inadvertent translation errors or being country-specific. Any research that was not focused on EU SMEs was also removed from the records. A lot of research was found to be specific to EU law due to the nature of GDPR. Only specific interdisciplinary research related to EU SMEs grounded in GDPR impact on their business was retained for literature review.

Research and studies that were from non-EU countries and focused on EU SMEs but without any defined influences on their business due to GDPR were discarded. Finally, studies on the highly technical matters of data applications and sciences related to the EU SMEs and the regulatory compliance of GDPR were also discarded due to their lack of focus on the business aspects of GDPR's influence on EU SMEs.

The selected research and studies followed the criteria distilled from the research questions and the hypothesis of this thesis. The selected records align with the purpose and objectives of this research.



Model for Literature Selection

d) The Data Economy

The EU's data economy in 2015 was estimated at €285 billion or 1.94% of the total EU GDP. The year-to-year growth of the EU's data economy increased to 5.03% in 2017. This was the highest amongst all sectors of the EU's economy. The EU data economy is estimated to reach €739 billion by 2020 at the present growth rate. The EU data economy constitutes 4% of the total EU GDP, delivering 100% growth between 2015 and 2019. (EU Research, n.d.)

A global survey by Deloitte of Fortune 500 companies actively involved in Data business revealed that 57% of all companies surveyed discussed data security as an ongoing board discussion matter. 51% of the companies had cyber security of their stored data as an ongoing board discussion. 21% of the companies had an international data transfer as their top discussion point in the board meetings. (Strategic Research, n.d.)

Accenture undertook a 19-country survey of companies dealing with 'big data. The survey concluded that 2/3 of all SMEs in the 19 counties implemented at least one cycle of data-based business modelling to enhance their productivity. SME participation in global data markets has increased dramatically since 2015. SMEs' participation accounts for almost US$994 Billion in digital trade globally. (*Accenture-Cross-Border-the-Disruptive-Frontier.Pdf*, n.d.)

e) Transformation of Global Data Economies under GDPR

The data of a natural person is part of fundamental rights guaranteed under the EU Law. The intense debate surrounding the data rights being absolute or subject to intervention by the member states or the Union is ongoing. The EU considers data rights fundamental to its core principles that uphold human dignity. The critical transformation of the EU laws concerning the data of a natural person under the GDPR extends its scope internationally.

The three main articles of the GDPR considering its international scope and reach **(i)** the right to erasure under **Article 17** GDPR, exerting this right internationally under **Article 3 (ii)** the European Commission's sole ability to decide if 3rd countries dealing with EU Citizens data for storage and access have adequate data protection regimes under **Article 45** and **(iii)** EU's ability to impose hefty penalties on companies both local and international which are found to be in breach of GDPR under **Article 83**.

The international overreach and extraterritorial scope of GDPR make it necessary for businesses to avoid penalties. European Data Protection Board (EDPB) has 206,326 breaches recorded for GDPR in the first nine months of its enforcement. Billions of dollars in fines have been imposed on global businesses such as Google, Facebook, British Airways, Marriott Hotels etc.

f) Data Protection Beyond Business and Economics

The case law of the Court of Justice EU (CJEU) suggests that business and economic activities generated from the use of personal data are legal policy matters and not business policy matters. The CJEU views business activities using personal data as intrinsic to the fundamental right of data protection enshrined in Article 8 EU Charter of Rights (Article 8- CFREU). CJEU gives broad interpretations of personal data rights when a third party processes data for a business activity. Google v Spain is the seminal case for personal data rights in the EU. (*CURIA - List of Results*, n.d.)

g) International Privacy Law & GDPR

The right to be forgotten or erased under GDPR Article 17 has found favour with other countries such as Australia, Canada and Japan. The data rights debate in these

countries is triggered by CJEU's seminal case of Google v Spain. Legislations are being proposed in Argentina, Brazil and Mexico based on the Google v Spain ruling and GDPR. These legislations based on GDPR will have a far-reaching impact on SMEs and their ability to use personal data for business activities.

h) Data Transfer for Business & Economic Activities

Article 45 of GDPR aims to bring some certainty through the Adequacy of Protection decisions by the European Commission. This area of business law concerning data transfer is not without its pains. The interpretation under Article 45 GDPR will have a wide-ranging impact on the US$ 600 billion digital economies of the EU. The Commission hopes to sustain the US$ 600 billion data business through harmonization efforts. These efforts include Article 45 GDPR voluntary adoption by the third countries. The requirement is for data storage arrangements in 3rd countries under GDPR for business purposes.

i) GDPR Enforcement & Impact on Business

Article 83 GDPR imposes heft fines through its two-tiered system of financial penalties. Article 83(4) imposes a fine of €10 Million or 2% of the total annual revenue for the preceding year, whichever is higher for any breaches under the GDPR of €10 million or, in the case of an "undertaking," two per cent of total annual revenue for the preceding financial year. The higher fine under Article 83(5) concerns the violation of the basic principles of consent and cross-border infringements under Articles 5 & 6 GDPR. The fines are for €20 million or 4% of the total annual revenue for the preceding financial year, whichever is higher. Academic commentaries support these fines and make them akin to the fines for corporate crimes such as insider trade and money laundering. Companies such as Facebook, Google, Apple, and Amazon, with their colossal earnings, could potentially face fines between €5.0B and €7.0B.

The famous quote of Samuel Johnson aptly describes the fears of GDPR by the business community, '*Depend upon it, sir, when a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully'*.(Boswell, 1851)

A 2017 global survey conducted by TrendMicro indicated that nearly 67% of the global firms directly influenced by EU GDPR do not understand the business and legal implications of EU GDPR. The same survey indicated that 42% of the firms have no idea or are confused about the exact data protection requirements of GDPR that impact their business. (*Trend Micro Survey on GDPR,* n.d.)

j) GDPR- EU Efforts for a Single Digital Market

GDPR aims to prepare the European economies for Europe's Digital Single Market Strategy. The strategy is to harmonise the data protection regime within the EU. GDPR claims to serve the broader business and rights protection objectives of the EU. GDPR is indeed a law, but its scope is business. It gives rights to consumers within the digital space. These rights directly impact the business models of the companies within the data markets. EU has taken over the role of regulating the global data markets through GDPR. The Treaty of Lisbon clarified the *supranational* role of the EU in regulating EU-wide economic activities.

k) GDPR as an EU Protectionist Strategy

Research has emerged against the GDPR with compelling arguments. These arguments are based on the EU's unilateral decision to force the storing of EU data within the geographical boundaries of the EU. Data warehousing is now a multi-billion-dollar business. Data storage does not follow geographical boundaries. US companies dominate the global digital markets. Facebook, Google, Microsoft, Apple and Amazon control 60% of the global digital business.

The US-based technology giants control 83% of worldwide internet intermediation revenues. The EU-27 accounted for only 1.7% in 2018. 80% of EU-27 online search business is controlled by Google. Google and Facebook take 70% of all revenues from online advertising from EU-27. 72% of Cloud computing Services provided in EU-27 store their data in the US. United States terms GDPR as a regulatory wall built to harm the US businesses' competitiveness within the digital space.(Hofheinz & Mandel, 2014)

The GDPR has been termed as the EU's protectionist policy to shut out the best technology companies from the EU's data business. A study on behalf of the US Chamber of Commerce gives negative growth for the US technology companies' compliance with GDPR for the next few years. The cost for US companies to do business in the EU would be increased by 20%. It would resultantly reduce the EU GDP by 0.4% per year. The US trade representative offices term GDPR as *unproportionally injurious* to US companies and their economic interests.

A recent research study shows that the GDPR has the potential to reduce the volume of a data storage business in the US due to the strict data security requirements under the GDPR.(Hazen et al., 2014, p. 74) Before GDPR, the regulation asymmetry existed between the US and EU data protection regulations. This regulatory asymmetry is not the only reason for the stemmed growth of the EU technology companies.

l) SME Competitive Advantage

Businesses are not homogeneous and the companies that are running these businesses are also of varying types that are multi-dimensional in terms of their size, target demographics and services. The terms competitive advantage for companies differ in terms of the size of the company. Most of the existing literature defines competitive advantage for companies without any consideration of their size. Limited research has emerged focusing on competitive advantage for SMEs.

Michael E. Porter's work on competitive advantage for businesses is considered seminal (Porter, 1985). Porter's (1985) definition of competitive advantage targets corporate businesses in general and does not differentiate between large, medium and small enterprises. Porter states:

"*Competitive advantage stems from the many discrete activities a firm performs in designing, producing, marketing, delivering, and supporting its product. Each of these activities can contribute to a firm's relative cost position and create a basis for differentiation*(Porter, 1985, p. 61)."

Essentially Porter is referring to the competitive advantage in terms of differentiation that a firm creates by controlling its production costs and creating higher productivity for the firm and its clients.

Porter's Model of Firm's Competitive Advantage- Source (Amadeo, 2022)

m) Data Services, Innovation & Competitive Advantage

Data services have undoubtedly changed the business landscape of every form of service across the world. Information and Communication Technologies (ICT) has transformed how customers, services and businesses engage in transactions.

Gill Press collected global research on the impact of data on businesses in 2020 that was published by Forbes Publications (Press, 2020). The research collected by Press (2020) states that the global generation of data jumped 5000% in ten years between 2010 and 2020. Press (2020) also reports global business investment for direct digital transformation reaching $6.8 trillion by 2023.

Selling products and services in a Business-to-Business (B2B) and Business-to-Consumer (B2C) is a core activity of businesses regardless of their size. The future of sales has transformed from experience and intuitive to data-driven decision-making within the B2B and B2C sales environment. Gartner reports that 60% of companies of all sizes across the globe are expected to shift their business sales models to data-driven decision-making by 2025(Kelly, 2020).

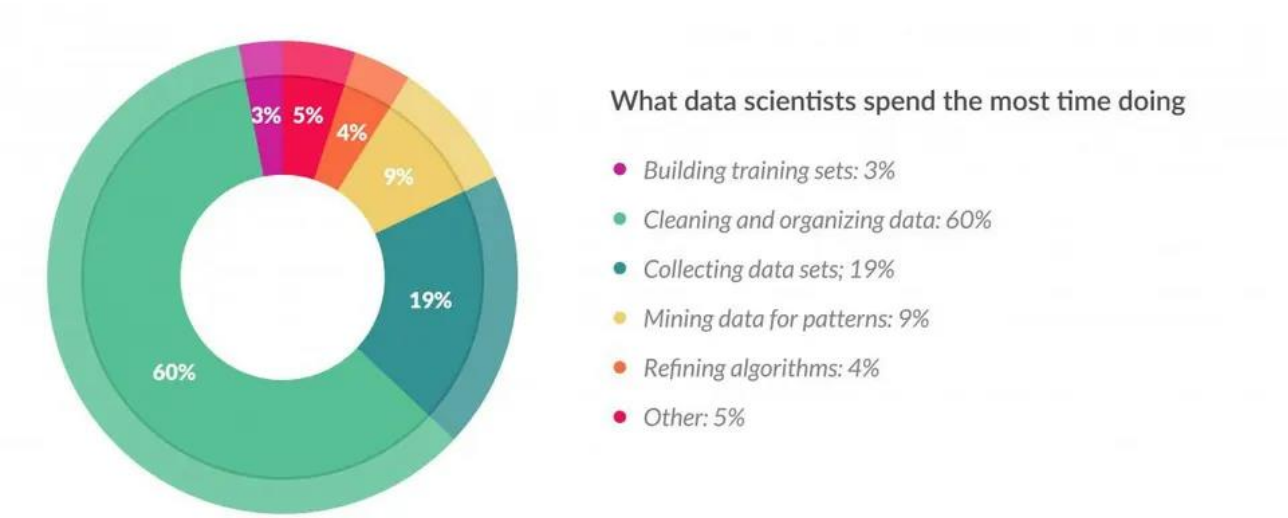
Hyperautomation within the corporate environment especially linked to the digital transformation of businesses poses serious challenges to data security and data protection for the business collecting, storing and processing data for their business activities. Data theft and other cyber security challenges have risen since the global

sharing of customer data within the core business activities. Global cybercrimes cost a whopping $8 trillion in 2023, compared to $3 trillion in 2015(S. Morgan, 2022). The $8 trillion cybercrime loss to global businesses due to data theft is third to the GDP of the US and China in 2022.

Hyperautomation and transforming to data-driven business modelling are not enough to deliver a competitive advantage to businesses. In the wake of data theft and related cyber crimes over the web, there is rising customer bias against the sharing of their data across the web. This is also true for businesses generating data and sharing it for B2B or B2C business activities.

Research indicates that robust data analytics, sharing data with targeted resources and usage of relevant data sources to achieve precise corporate goals is the key to obtaining competitive advantage using data in the contemporary digital economy(Goasduff, 2022). Gartner research predicts that businesses achieving digital trust in their data subjects are 50% more likely to generate higher revenue and participate in global digital ecosystems for competitive advantage compared to companies that fail to achieve data trust in their customer base(Goasduff, 2022).

Goasdull's (2022) findings about clear and precise usage of data by constantly refining the data that can provide competitive advantage through innovation to the businesses is confirmed by a survey by Crowdflower. Research indicates that 80% of the time spent by data scientists is on preparing data for precise analysis that can provide focused solutions to businesses for their challenges and drive higher productivity for competitive advantage.



Data Preparation for Competitive Advantage: Source (Press, 2016)

n) Data Challenges & SME's Competitive Advantage

Things are not all that rosy when it comes to consumer data and its ability to provide a competitive advantage to businesses. While larger businesses can employ resources for preparing, sorting and analysing data for competitive advantage, SMEs have limited resources and time to use data for their competitive advantage. As already mentioned earlier consumer trust in the ability of the business to protect their data is

one of the key elements to create competitive advantage for the business, research indicates that SMEs generally struggle with legacy data platforms that limit their ability to gain competitive advantage from available data.

Various studies have emerged that touch upon various challenges that SMEs face when leveraging data for competitive advantage. A recent study based on data collected from IBM, Forrester and Forbes Survey indicates the following four major obstacles for SMEs to achieve desired business outcomes from data for their competitive advantage(Gudeta, 2023):

- **Complex Architecture**: difficulty in having resources (in-house) to use various data language programs to fully understand the data parameters for the business
- **High Latency**: difficulty in having resources to make real-time decisions as the data becomes available and new data replaces the existing data
- **High Total Cost of Ownership**: operational costs of sourcing data from various platforms that are relevant to the business
- **Data Protection**: ability and platform to ensure customers' trust in protecting and securing their data

o) ICT as SMEs Competitive Advantage- EU Industry 4.0

SMEs are not in a favourable position compared to large corporations when it comes to leveraging ICTs and pursuing innovation as a competitive advantage. The role of innovation and adoption of cutting-edge ICTs as a competitive advantage for businesses is well documented. However, SMEs are limited in their ability to adopt ICTs and pursue innovative solutions for their growth. SMEs represent 99% of all companies registered within the EU. These EU SMEs employ over 100 million people across the EU and generate 50% of the EU's GDP. Having such a vital socio-economic impact, limited research has emerged on the topic of ICT and innovation as a competitive advantage for EU SMEs.

Digitization of EU SMEs has been recognised by EU policymakers. With the rising competition from Asia, especially China and the tight hold of US technology companies on the EU markets, the need for EU SMEs to adapt to the rapid technological changes within the business ecosystem is vital. The task is easier said than done. EU-27 is a collection of countries that are at extremes of socio-economic development. Economic powerhouses of Western Europe such as Germany, Norway, Finland etc. outperform countries like Albania and Bulgaria etc.

EU Industry 4.0 is the conceptual framework recognised by the EU parliament to define the digital opportunities presented to EU-27 due to the advancements in technology. The three principles defined by the EU for preparing its businesses particularly the SMEs to leverage technology as a competitive advantage are:

- A single digital market that is scalable
- Competitiveness and inclusion through leveraging commercial use of data
- Invest in innovation and speedy adoption of technology especially emerging Artificial Intelligence frontier

The three EU principles for achieving competitive advantage through the Industry 4.0 vision outlined above are further explained by compartmentalizing technology as transactional, operational and informational. While funding is being poured into digitizing the EU-27 single digital economy project, very little research has emerged if these interventions are resulting in any competitive advantage for EU SMEs.

p) GDPR and SME's Competitive Advantage

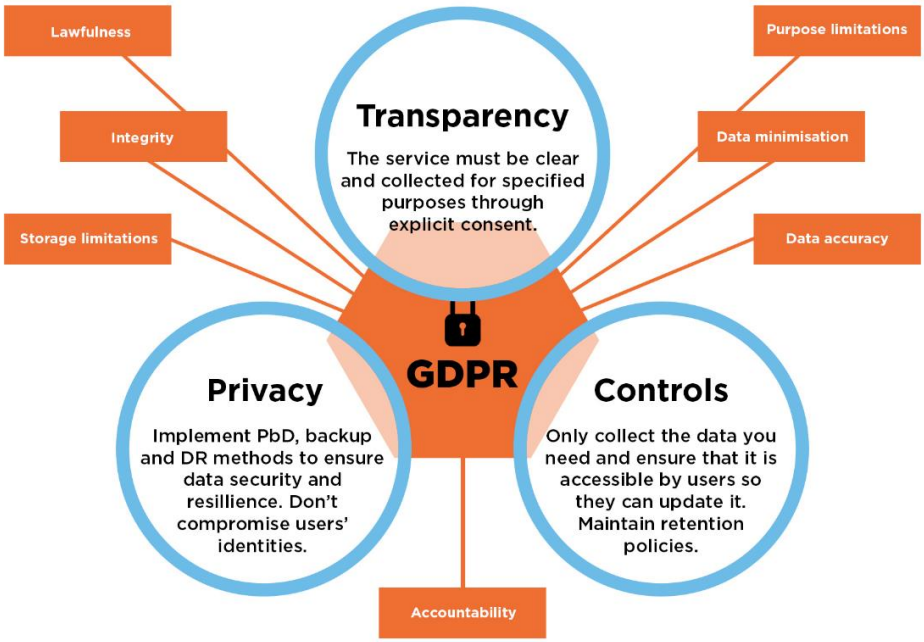
A search for GDPR and its competitive advantage for SMEs or lack thereof does not return any results on search engines like Google Scholar, EBSCO, JSTOR, and Directory of Open Access Journals. However, limited research has emerged on GDPR's impact on businesses in general with some research on its impact on SMEs. Research is also emerging on specific business sectors that have been directly impacted by the enforcement of GDPR since May 2018.

q) Conclusion

EU GDPR came into force on 25th May 2018. Research has started to emerge pointing to the unique set of findings that raise questions on multiple fronts about the business impact of GDPR. Those fronts are economic, legal and technological. EU faces competition from countries like the USA in the areas of advanced technologies. GDPR aims to check the dominance of US tech giants in the global data markets. Google, Facebook, Microsoft, Apple and Amazon are at the top of the global digital economy's food chain. SMEs are a crucial part of the upstream and downstream data business. SMEs act as the catalysts for technology innovation and adoption.

The EU SMEs play a crucial role in the current growth of the EU's digital economy at 7% per year. The EU SMEs also attract a large portion of the foreign direct investment (FDI) coming into the EU from the US and Asia. Existing research has largely examined specific implications of data regulation, such as advertising, product pricing, defaults in financial markets and the impact on medical services.

This research will help answer the crucial question(s) about the competitiveness of EU SMEs due to GDPR compliance. Any reduction in the competitiveness of the EU SMEs will also deprive the EU economy of billions of dollars. This research and other future research will help the EU SMEs find their way around the GDPR enforcement which remains an enigma to the business world. GDPR is the EU's answer to the evolving data privacy and protection needs of its residents, who are natural persons. It has defined parameters and principles that provide that protection.



Source: https://cloud.netlifyusercontent.com/

3) INTERDISCIPLINARY LITERATURE REVIEW

a) Why the Interdisciplinary Approach?

The reach of data within the various tiers of business is ubiquitous. SMEs are no exception. An interdisciplinary approach is being encouraged in social sciences especially business studies to explore critical challenges facing businesses today. Interdisciplinary approach in literature review for business studies in being encouraged to problem solve complex concepts such as amalgamation of statistically intense, legally embedded business challenges in this data-driven global businesses.

An interdisciplinary approach to literature review has been included as a separate component of this research due to the legal nature of GDPR posing business challenges to the EU SMEs in real-time. This interdisciplinary approach has helped to uncover and synthesise the complexity of GDPR's legal impact by translating it into expressive knowledge that can be applied to business impact scenarios. The interdisciplinary research model for literature review is an innovative approach that allows the integration of distinct knowledge fields such as business, law and technology for a given set of problems and offers insights that may not emerge if considered in isolation.

The interdisciplinary literature review has helped and supported this research in exposing the outliers of GDPR's legal and technological components that directly affect the business operations of EU SMEs.

b) Legal Business Foundation of EU

The genesis of the EU is intrinsically grounded in the European continent's business and economy. The EU's genesis can perhaps be best attributed to the signing of the '*Customs Convention'*[1] in September 1944. The devastations of World War II brought about the need to rebuild the shattered economies of the European continent. The purpose of the Customs Convention of 1944 was to remove trade barriers between the Benelux nations[2]. The Benelux countries are Belgium, the Netherlands, and Luxembourg.

The European Coal and Steel Community[3] ("**ECSC**") followed in April 1951. ECSC was originally only envisaged between France and West Germany, the final signatories were France, West Germany, Italy, and the Benelux countries. The treaty aimed to remove the control of steel and coal by the wartime industries and divert the

[1] 'The Netherlands–Belgium–Luxembourg Customs Convention': Source: https://www.cvce.eu/en/epublications/eisc/historical-events

[2] Belgium, Netherlands, and Luxembourg. 'Benelux' is from using first alphabets of signatory nations, [**B**e**N**e**L**ux]

[3] 'Schuman Plan 1951 was proposed by French economist Jean Monnet and tabled by the French Foreign Minister Robert Schuman

steel and coal resources to the rebuilding of Europe. ECSC's framework provided for the establishment of a '***High Authority***' comprising **'*Council of Ministers*'** representing the member states. It also provided for an '***Assembly***' and a '**Court of Justice'** to deal with all matters arising from the '**Acts**' of the Council of Ministers. This legally unique and independent organization was the creation of a truly '***internationally enforceable***' business and economic agreement between nations.

The agreement allowed for the transfer of sovereignty for the matters covered under the agreement from the member states to ECSC institutions. This is the legal foundation that led to the later creation of the European Economic Community ("EEC"), signed in a treaty by the same six signatory nationals of ECSC in 1958. The transfer of sovereignty concerning business and economic decisions from the state to a supranational body laid the foundation of modern supranational business laws within the corpus of International Business Law.

The signing of the Brussels Treaty in 1965 and the 'Single European Act' ("**SEA**") in 1986 paved the way for the 1993 Maastricht Treaty known as The Treaty on European Union ("**TEU**"). TEU laid down the broad European intergovernmental cooperation through the so-called '*Three Pillars*' established through the TEU.

- The **first pillar** was the unification of all previous bodies such as the EEC, ECSC etc.
- The **second pillar** speaks to intergovernmental cooperation for security and foreign affairs.
- The **third pillar** concerns justice and home affairs.

In addition to the defined 'three pillars' of TEU, the TEU also proposed the **European Central Bank** and the European Currency '**Euro**'. It also proposed a social chapter that would enhance Europe's 'social' identity.

The UK had been one of the main architects of the TEU but negotiated an '***Opt-Out***' for both the proposals under the TEU in 1993. While this is a factual reality, the point has never been raised in the arguments that followed the UK's decision to exit the EU in 2020.

The **'Treaty of Lisbon'** signed in December 2007 and enforced in December 2009, retained the TEU and renamed the **EC Treaty** as the 'Treaty on the Functioning of the European Union' ("**TFEU**"). Both **TEU** and **TFEU** are the basis of the primary sources of the EU Law.

TFEU also proposed the European Charter of Fundamental Rights ("**CFREU**"). CFREU Article 8(1-3) guarantees the protection of a natural person's data under the title of Freedoms. Personal data protection of the natural person is not an absolute right under the CFREU. The EU member states can interfere with this right under certain exceptions that include national security etc. The development of EU Data Protection laws through TEU and TFEU led to the framing of GDPR as the latest body of natural persons' data protection rights.

c) EU's Four- Freedoms & Business

The Council of Europe, Strasbourg laws concern the principles that uphold democracy, protection of fundamental rights and the rule of law. The EU laws from Brussels ensure broader and much deeper cooperation between the EU-27 member states for '**socioeconomic freedoms**' as the **principle aims** of the 27-member state union. The cornerstone of the EU is to guarantee the so-called four freedoms. The freedoms are:

- The free movement of *people*
- The free movement of g*oods*
- The free movement of *services*
- The free movement of *capital*

These freedoms are covered under Article 26(2)[4] TFEU. Both the Council of Europe and the EU share the same *fundamental values* that guarantee fundamental rights, democracy, and the rule of law.[5] GDPR is considered to uphold the principles of the four freedoms under Article 26(2) TFEU, CFREU and ECHR to protect the privacy of natural person data as well as allow businesses to leverage the benefits of personal data within the global digital economy advancements. These stated aims are under review in this thesis as GDPR is a legal instrument that has a business scope.

d) EU Law is Foremost a Business Law

In the paragraph ante, it has been argued with evidence that the genesis of the EU is for the economic prosperity of the EU-27 thus business activities lead the legal and policy formulations at the highest levels of governance. If this argument holds, it can be inferred that the business and economic realities deeply influence EU Law and by extension laws such as GDPR.

The two distinct and independent law-making bodies that prescribe various laws that govern the continent of Europe and EU-27 are the Council of Europe ("**COE**"), Strasbourg France and the European Union ("**EU**") Brussels. Both of these bodies have been explained in the section above. However, to clarify once again, COE, headquartered in Strasbourg, France, is not a part of the governmental or hierarchical structure of the EU-27 Brussels. COE is an independent intergovernmental body that proposes laws for human rights, democracy and the rule of law. It has no links or functional conflicts with the EU-27 or its law-making. All laws formulated by COE are adjudicated by its independent Court (ECtHR) in Strasbourg, France. COE and EU-27 owe their genesis moments to the end of the Second World War.

[4] Article 26(2) TFEU: "*The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties."*

[5] https://www.coe.int/en/web/portal/european-union

e) Council of Europe (COE)- Foundation of EU Business

The idea of a unified European economic community 'is linked to the Truman Doctrine[6]. The Truman Doctrine, the so-called '**Truman Declaration**' was made to the US Senate by US President H.S. Truman in March 1947. It called for immediate aid to Greece and Turkey to prevent both countries from falling under the influence of the Soviet Union at the end of World War II. The doctrine evolved from Great Britain's economic inability to offer assistance to the countries that were crucial to secure the Mediterranean's trade and economic gateway to Europe.

The US Senate agreed to the Truman Declaration to assist Greece and Turkey in their post-war rebuilding efforts and securing the Mediterranean waterways for business and economic activities critical to Europe and North America. President Truman announced a US$ 4 Billion aid package to Greece and Turkey. The aid helped to secure the Mediterranean Sea routes from any potential Soviet interventions. Regardless of the political reasons for the massive aid by the US to Greece and Turkey in 1947, the trade and business implications of the action resonate within the trillion-dollar trade movements through the Mediterranean to this day.

The British Prime Minister Winston Churchill in his September 1946 speech at Zurich University, floated the idea of the '*United States of Europe*' based on the Truman Declaration. UK became a critical ally of the US in protecting the combined economic and business interests of Europe and North America in the emerging new economic world order of post-World War II. The collapse of the British Empire at the end of World War II saw Great Britain aligning itself with the US-Europe socioeconomic agendas globally. Churchill chaired The Hauge meeting of the '*Congress of Europe'* that laid the foundation for the Council of Europe (COE) and European Court of Human Rights (ECtHR) in Strasbourg, France. The UK's supportive role resulted in the signing of the '*Statute of the Council of Europe*'[7] on 5th May 1949. The COE Statute came into force on August 3, 1949.

> *"The Council of Europe's most famous legislation is the European Convention of Human Rights ("ECHR"). ECHR was adopted by its 10 original members[8] on the 4th of November 1950. The signatory states to the ECHR are called 'High Contracting Parties'. The 27-member states of EU-27 along with other nations, comprise the 47-member states that are the High Contracting Parties to ECHR. The ECHR is enforced and adjudicated by the European Court of Human Rights ("ECtHR"), Strasbourg. While ECHR protects fundamental human rights, there is no distinct and defined right for the protection of a natural person's personal data protection. However, recently, the ECtHR determined and interpreted the data protection right, emerging under EU Law and more specifically GDPR as,*

[6] McCullough, David (1992). Truman. New York: Simon & Schuster.

[7] https://rm.coe.int/1680306052.

[8] 10 original signatory states to ECHR are: Kingdom of Belgium, the Kingdom of Denmark, the French Republic, the Irish Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Kingdom of Norway, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland

> *"The mere storing of data relating to the private life of individual amounts to an interference within the meaning of Article 8 of the European Convention on Human Rights."*[9]

The ECHR also does not provide for absolute protection of any data protection rights of the natural persons. The states reserve the right to interfere with the data protection rights on public safety and national security. The exceptions to allow a High Contracting Party of ECHR to interfere with the personal data rights under Article 8 ECHR are not based on any business considerations, unlike GDPR. All legislations of the Council of Europe are called '*Conventions*'.

It must be noted COE was the first law-making body within Europe to come out with a data protection convention in the face of emerging information and communication technologies in 1981. The Council of Europe's Convention 108 is the first European internationally enforceable and legal instrument on data protection that is part of its body of law. COE Data Protection Convention 108, however, is not a binding law that can override the national laws of the High Contracting parties that are signatories to it. Nor does the COE Convention 108 provide any protection to natural persons' data from any violations from business usage.

There are no COE Conventions for business or economic activities between the High Contracting Parties. Thus, a body of laws under the Council of Europe remains distinct from EU law within the scope of any business activities or any related business laws such as GDPR. The enforceability of ECHR extends beyond Europe due to the membership of non-EU countries such as Turkey etc.

f) EU Data Protection Laws & their Business Scope

The European Union ("EU") is a distinct and unique legislative body within the global community of law-making bodies that aims to provide freedom of trade and investment across a supranational union of 27 sovereign states. EU has been described as a unique socio-economic experiment by social scholars across the globe. In that, it gave rise to a body of law that is based on the economic needs of the European continent post-second World War. EU law has supremacy over the national laws of its 27 member states. GDPR is part of the EU law that has supremacy over the 27-member national laws concerning natural persons' personal data protection, especially its use by businesses.

The EU's first supranational data protection law came as a Data Protection Directive in 1995. Article 16 TFEU affirms the distinct data protection right under Article 8 of the EU Charter for Fundamental Rights (CFREU). GDPR enforced since May 2018, is according to the EU, an answer to protect personal data due to the rapid advancements in information and communication technologies. The fundamental difference between an EU Directive and EU Regulations is that EU directives require the member states to enact legislation within their national laws that conform to the EU Directive. In contrast, EU Regulations do not require the member states to enact the EU

[9] https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

Regulations. The EU Regulations supersede the national legislation once enacted and are enforceable throughout the 27-member union.

g) EU Resident versus EU Citizen in GDPR.

GDPR is considered by far the most rigid natural persons data protection law anywhere in the world. The stiff penalties associated with GDPR non-compliance and its broadly enacted language make it a compliance and implementation challenge for EU SMEs. At the heart of EU data protection, law-making is the protection of a natural person's data within the scope of its use in the 21st-century explosion of personal data usage in the global economy, which is predominantly digital. It is beyond the scope of this research to explain and identify the reasons for GDPR's wider coverage of the natural person's data to any resident of the EU-27 and not just EU Citizens within the EU-27. It must, however, be explained briefly how the 'European identity' of EU residents becomes a critical consideration that operates to provide protections under GDPR.

Recital 14 of the GDPR explanatory notes, Recital 14 states that "the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, concerning the processing of their data."(Vollmer, 2021)

SMEs would need resources to understand the legal complexities of GDPR. It practically means for an SME offering any internet-based service that any person, regardless of their origins, nationality or citizenship, is afforded data protection if they access any internet-based service while being within the territorial boundaries of EU-27. It also means that any EU SME or any international company using the personal data of a person or offering the service to any user within EU-27 would have to be GDPR compliant.

h) Business Opportunity Vs. Data Protection

In her April 2019 article on web personalisation and data privacy, Susan Moore, a web technology and business expert highlighted the conjoined concepts of personalization and privacy. (*How To Balance Personalization With Data Privacy*, n.d.) Moore successfully argued the point of personalised web experience of users by combining identity data with behavioural data. This is true for technology giants that can use the data subject's data, combine it with the user's web service behaviour and generate content and services to provide a customized web experience to the data subject. While, in theory, this is a win-win situation for the web service providers and data subjects, it comes with its risks of personal data theft and web service providers breaching their data privacy obligations to the data subjects.

GDPR proposes to protect the 'web identity' of the data subjects by ensuring that the businesses accessing, storing, and monetizing the collected identity personal data of the natural person ensure the individual's data protection rights.

Under GDPR, data protection remains robust regardless of any national laws within the EU member states that may or may not afford the same protection as legislated in their national laws. Before the enforcement of GDPR, there were examples of web service providers 'shopping' for jurisdictions within the EU, where the data

protection rights of the natural person were not fully protected against any unlawful breaches by the service providers.

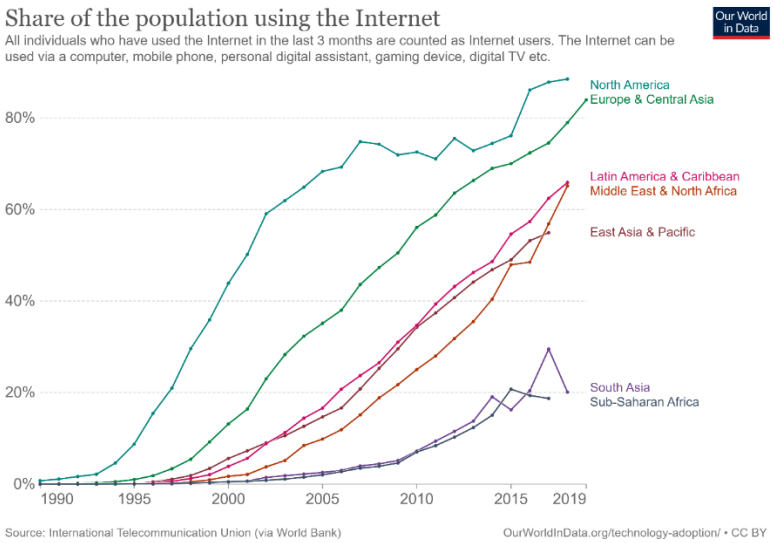
There is an elaborate body of case law of the Court of Justice of EU (CJEU), Luxembourg that pertains to breaches of data protection rights of the EU residents/citizens by businesses within the EU as well as internationally. The detailed discussion of such cases is beyond the scope of this paper. As regards CJEU's position on balancing the needs of business and the privacy rights of the data subjects, CJEU has emphasised. We would ensure the free movement of data for business purposes based on the EU Four Freedoms doctrine of EU law. The Court has also recognised that the EU resident data versus EU citizen data 'limitation' speaks to the principle of non-discrimination on any grounds as laid down in the EU Charter of Rights. Article 21(1) TFEU makes it evident that the right conferred by the freedom of movement for trade and investment is '*subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect'*. This means that GDPR is well placed to protect the rights of the EU residents as well as balance the business needs of the EU and international businesses looking to explore the data services arising from the customer data of EU residents.

i) Digital Value of Personalized Content

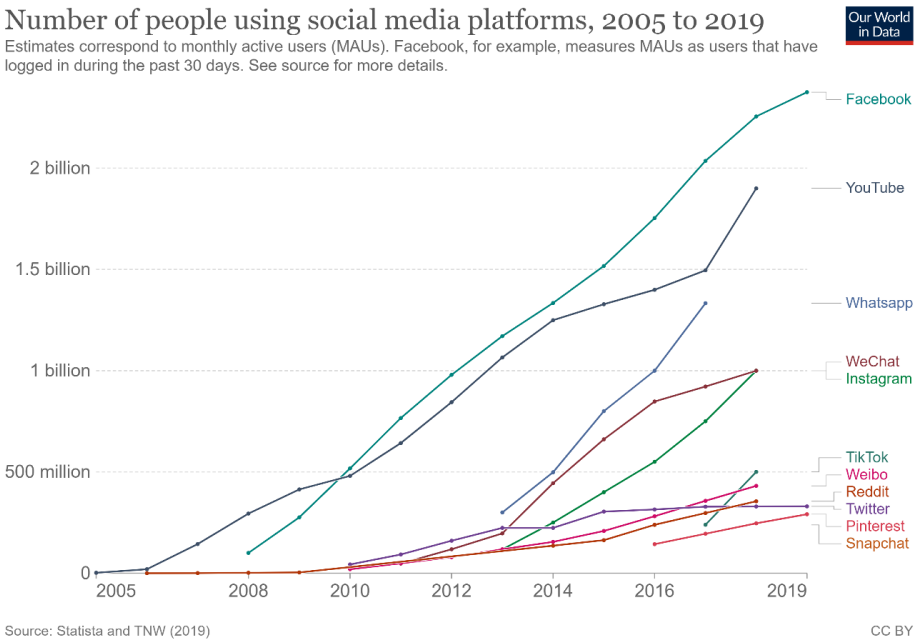
The use of the word '**identity**' within the context of natural persons' data specifically within the language of GDPR refers to the potential misuse of personal identity breaches in the wake of the digital revolution.

The technological advancements in ICTs have revolutionised the use of personal data and the personal identity of natural persons within the context of global socio-economic activities. The average internet use on social media alone went up from 45 minutes in 2012 to 3.7 hours in 2019. (*Social Media Captures Over 30% of Online Time*, 2017) There are over 4.9 billion internet users in the world today, which comprises two-thirds of the world's population.

The development of supercomputers, advancement in artificial intelligence (AI) based platforms etc. fully rely on the natural persons' data and, by extension, their identity, which fuels the global technology businesses. The data chart below shows the global internet penetration between 1990 and 2019.



Internet penetration comes at a cost as the innovations rely on increased personal data generation to fuel automation within the digital economy. Social media platforms are the best example of monetizable behaviour of personal data usage, which heavily relies on the identity aspects of the data subject. Social media platforms like Facebook, Twitter, Instagram TikTok etc., use the personal identity markers of the data subject to generate billions of dollars in personalised advertising. However, the dispossession of data subjects' identities creates challenges such as identity theft and unauthorised usage of the data subjects' personal information throughout the web. The chart below shows the social media penetration over the period 2005 to 2019.



j) Protecting Personal Identifiable Data & GDPR

GDPR Article 4(1) clarifies the importance of 'identity' within the scope of personally identifiable data of the natural person. The wording is essential as we have demonstrated that identity monetisation is the business of the modern digital economy. GDPR Article 4(1) reads:

> "personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"("Art. 4 GDPR – Definitions," n.d.)

The linkages between personal data leading to the identification of natural persons and GDPR's compliance requirements to protect the identity of the natural person while accessing web services stems from the case law of CJEU. The case law of CJEU suggests that '*identity*' remains the core defining word when it comes to any data that pertains to a natural person and for data protection.

In the seminal joint cases of **Volker und Markus Schecke GbR**(*Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 2010) concerning the protection of a natural person's identity concerning the processing of personal data, the CJEU held: (Para 52-54)

> 'The right to respect for private life concerning the processing of personal data, recognised by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, concerns any information relating to an identified or identifiable individual. Legal persons can thus claim the protection of Articles 7 and 8 of the Charter only in so far as the official title of the legal person identifies one or more natural persons. That is the case where the official title of a partnership directly identifies natural persons who are its partners.'

The case referred to above indicates that data protection concerns the identity of a legal person conferred through the EU Charter Rights under the definition of a legal person who is 'officially' entitled to be identified as a natural person. The word 'officially' emphasizes the business construct for the meaning attached to the identity of the person. In simple words, CJEU weighed in on the pervasive use of identity for any monetised value and the attached protection afforded to the identity of the natural person within the EU Charter Rights.

The CJEU in the same case laid down the guidelines when the data rights could be interfered with in various situations: (Para 52,65)

> "Article 52(1) of the Charter of Fundamental Rights of the European Union accepts that limitations may be imposed on the exercise of rights such as those outlined in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms, and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. The limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated concerning Article 8 of the European Convention on Human Rights."

The limitations on the right of data protection are limited by 'lawful' tolerance concerning the rights. The lawful right to interfere flows from the rights of the State under the EU Law or for any lawful business activities that are protected under the Four Freedoms of EU Law. GDPR has pointed to the protection of natural persons' data rights within the 'identity' context and for the usage of such identity data in line with the Four Freedoms of EU Law.

Edward Snowden's revelations about the covert global data collection under the US PRISM program exposed personal identity data leakages from Big-Data companies such as Google, Microsoft, IBM and Facebook etc. to the government agencies without the consent of data subjects. It included access, storage and retention of personal data of EU residents/citizens by government agencies. Such unauthorised data collection of the natural person is covered in GDPR Article 48. It reads:

> "No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State."("Art. 48 GDPR – Transfers or Disclosures Not Authorised by Union Law," n.d.)

The wording of Article 48 precludes any entity, including any judicial or government entity outside the EU from disclosing any personal data of EU residents. This clause requires any business to seek legal authorisation from EU Courts to share the personal data of any EU resident regardless of the geographical location of the commercial entity. Any violation of this GDPR article carries hefty fines. The wording of GDPR Article 48 comes from the case law of CJEU.

The mass personal data collection and storage of EU residents for identification was challenged in the pre-GDPR CJEU seminal case of Digital Rights Ireland. (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 2014) The CJEU first declared EU Directive 2006/24/EC, which was an EU Directive authorising EU residents' data collected by the US agencies invalid. Secondly, the CJEU held that any EU Directives violate the Article 8 Charter Rights of EU residents' personal data protection. The Court also laid carefully selected guidelines for any interference with the Article 8 EU Charter data protection rights.

The foremost criteria set by CJEU for any usage/ interference with data protection rights required a 'valid legal basis. CJEU also declared the collected data must be 'retained within the EU' and within 'strict limits' of the specified retention period. CJEU elaborated that a natural person's data is linked to their 'personally identifiable information'. Such identity is linked to an individual's 'resurfacing' in multiple events in a community. CJEU was referring to the web usage of the data person and their access to various web content. CJEU deemed the data protection of any natural person while accessing web services that could form the basis of unauthorised use of their 'identity' specific to the data generated. The Court held: (Para 32)

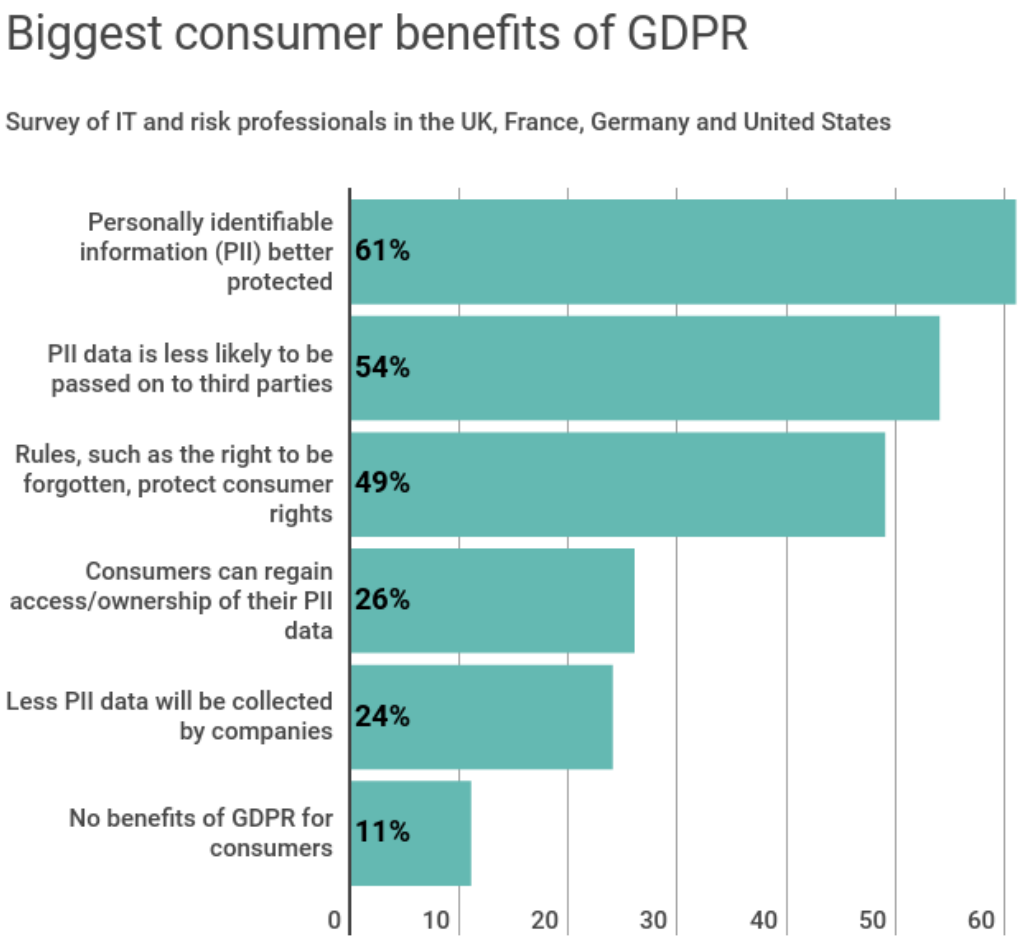
> ‘This is defined as a subset of communications data that identifies the sender or recipient of a communication; the time or duration of a communication; the type, method, pattern, or fact of communication; the system from, to, or through which a communication is transmitted; or the location of any such system’.

The 2014 CJEU’s cases of Watson and Schrems(*CJEU - Joined Cases C 203/15 and C 698/15 - Tele2/Watson*, n.d.) also played a deciding role in the framing of GDPR’s powerful wording to protect the data of EU residents. The CJEU combined both cases as cases related to the indiscriminate retention of EU residents’ data and the violation of EU Charter rights for data protection under Article 8 of the Charter.

In Watson, the Court held that the retention of a natural person’s data provided the exact location of the data subject and also would provide ‘precise conclusions’ for the data subject’s ‘private lives that include everyday habits.’ The CJEUs' reference to the important issue of protecting the ‘identity’ of the data subject with relation to their ‘private lives and everyday habits’ refers to any monetisation of such information by any web content service provider without the data subjects’ consent.

The CJEU raised the question of ‘identity’, ‘everyday habits’ and ‘private life’ within the context of the personal data of a natural person. Any cursory review of the monetised personal data-based advertising taking place on the internet would confirm personalised web advertising to be based on just those three factors as highlighted by the CJEU. It seems GDPR Article 48 referring to the identity protection being intrinsic to the personal data of the natural person provides such protection by imposing the consent limitation on the web service providers.

Research has emerged post-May 2018 implementation of GDPR that suggests a global shift in the personal data protection awareness of natural persons accessing web services that use their ‘identity’ through the collection of their data. The chart below explains some of the benefits outlined by experts.



Source:https://www.raconteur.net/legal/data-protection/gdpr-europe-lead-data-protection/

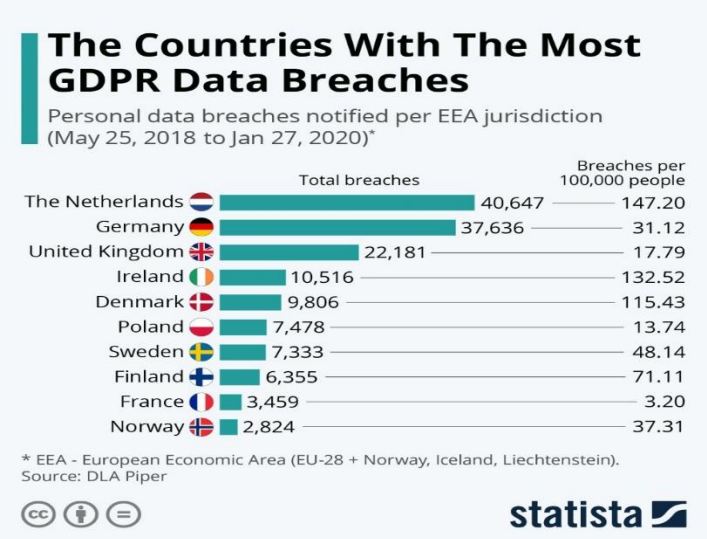
The GDPR came on the heels of the CJEU's decision in the above-mentioned seminal cases of natural person's data and their identity while using internet services etc.

The European Data Protection Supervisor (EDPS) is the EU's independent data protection authority. (*About | European Data Protection Supervisor*, n.d.) EDPS guides business and legal communities for the EU's data protection and privacy laws. EDPS has added 'trust' as an essential condition for the evolution of ICTs based on the EU laws protecting the data rights of its citizens/residents. Essentially, EU lawmakers advocate an ethical framework for developing ICT services that could satisfy the data protection rights conferred by Article 8 of the EU Charter. These ethical and legal reasons form the basis for web services and businesses to ensure compliance with GDPR.

GDPR Article 48 is a powerful clause that prevents EU residents' data from being retained, stored, accessed or disclosed to any entity without the data subject's consent. Article 48 operates against any non-EU country and its legal system's ability to access the EU resident's data or store it without their consent. Article 48 of GDPR also precludes any agreements between EU-27 member states and any non-EU country to share or transfer such data.

The UK (while it was still part of the EU) opted out of this clause since the US and the UK and Canada, Australis, and New Zealand exchange their citizens' data under the Five-Eye arrangement. The UK took the opt-out option of Article 48 GDPR under Protocol No. 21 of TFEU which allowed the UK and Ireland to opt-out of any EU laws that the UK and Ireland do not want to adopt in the areas of Freedom, Justice and Security.

Data has emerged which confirms UK citizens' aversion to any collection of their data without their consent since the enforcement of Article 48 GDPR. The chart below captures the data subjects reporting a violation of their data protection rights under GDPR since May 2018. It must be noted that the UK is in the top 3 countries with the highest number of GDPR breaches of EU Charter Article 8 rights under GDPR Article 48.



4) SURVEY DESIGN & QUESTIONS

a) GDPR Survey: Impact on EU SMEs & Competitiveness

The research was designed to study the impact of GDPR and the resulting business competitiveness on the EU SMEs within its data economy. The EU's data economy relies on its SMEs and their ability to remain competitive within the global data economy. The GDPR survey questionnaire for this thesis research has been designed to build upon earlier quantifiable business research studies conducted within the EU measuring the impact of the GDPR on the EU economies.

b) Survey Questionnaire Outline

The survey was designed with the main objective to answer the question of GDPR's impact on SMEs within the EU Data Chain. The survey targeted EU professionals working in EU SMEs who are either directly or indirectly involved in the implementation of the GDPR within their companies. The selection of SMEs was done with the help of the available data currently held with the EU's SME DATA[10] project. The survey aimed to answer sector-specific questions regarding the impact of the GDPR. The participants were asked to answer the questions through self-assessment and awareness of compliance with the GDPR. SMEs and various professionals within SMEs who participated in the survey are referred to as "participants" or "respondents" interchangeably throughout this thesis.

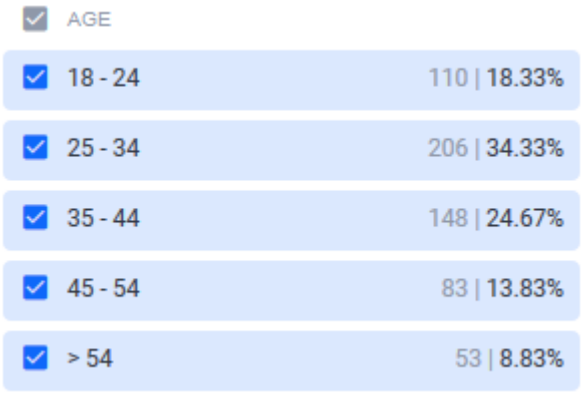
c) Survey Response Assessment Methodology

The participant's response assessment methodology for the specialized questionnaire fulfils the purpose of gathering information and understanding in terms of (1) To what extent are the participants informed and aware of the GDPR requirements as they impact their organisations and (2) How the specific areas of the GDPR impact the competitiveness of their companies. The methodology aimed to guide the participants in the accuracy of their responses and achieve high-quality data. The survey questionnaire was sent to a target group of 1500 using Pollfish. 600 participants were screened through a qualifying question that limited the participants working specifically with GDPR in an EU SME. The participants' demographics are shown below.

[10] https://smedata.eu/

Countries of Survey Participants*

***** The survey was completed in April 2020, thus within the scope of the UK remaining in the EU's common market and party to EU GDPR till Dec 31, 2020. GDPR still applies to the UK's SME sector handling EU citizen data.



Age of Survey Participants

Number of Employees in Survey Participant's SME

Roles of the Survey Participants in their SME

d) Survey Questionnaire Objective

The core objective of the survey was to identify, gather, and assess the business impact and SMEs' competitiveness due to the application of the GDPR. The questions framed for the survey specifically targeted the following areas to meet the survey objective:

- GDPR preparedness within the SME
- GDPR business impact due to its implementation on the EU SMEs
- SME investments to implement GDPR
- The positive or negative impact of GDPR on the SME
- Long-term impact of GDPR on the SME's business activities
- GDPR provides a competitive advantage to EU SMEs due to its implementation
- GDPR provides any added data protection due to its implementation
- GDPR is an ideal response to improve SMEs' business prospects

e) Survey Conduct

The survey was conducted in electronic format anonymously and confidentially using Pollfish. GDPR compliance was ensured throughout the data collection process to exclude prejudice or improper use of survey data. The researcher used technical, and regulatory steps to guarantee the complete anonymity of the respondents. The questionnaire was designed to ensure that responding to the survey questionnaire to the shortlisted respondents would take no longer than 30 minutes. The qualified participants were notified and directed to the website of Pollfish where the survey questionnaire was hosted. The participants were selected based on their existing knowledge and skills, including their role within the SME regarding the implementation of GDPR. The SMEs under the European Commission are defined in the EU recommendation 2003/361. It states

> "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro."

The quality of survey participation followed a bi-level approach. Firstly, only fully completed survey forms were considered for the data collection. Secondly, the introductory control question about the participant's ownership/employment within the EU SME disqualified other participants as an objective criterion. Each response to the questionnaire was weighted equally. The invited participants' completion of the survey was voluntary. The participants also had the choice to withdraw from the survey at any time. GDPR rules regarding such research surveys demand that all responses should be anonymous. None of the responses can be connected to any identifying information about the participants. All responses were/are to be kept confidential. The responses are strictly to be used for this research only as statistical materials.

f) Ensuring Integrity of Data

The survey questionnaire was delivered electronically using the state-of-the-art next-generation 'Organic Sampling' through the Random Device Engagement (RDE) approach. Respondents were invited through double-opt-in to avoid river sampling. Pollfish applied their proprietary AI algorithm to check the participants selected for the survey. The algorithm. The algorithms detect:

- Paid participation and professional survey participants
- Fraudulent bots and suspicious activity at question-level
- Questions being answered too quickly or nonsensical answers

g) Survey Questionnaire Structure

The survey questionnaire was structured to answer qualitative and quantitative typologies. The qualitative inquiry meets the need to understand GDPR and its business application within the scope of EU SMEs in the data economy. The quantitative inquiry targeted specific information related to the business impact of GDPR compliance and the competitiveness of EU SMEs due to its implementation. The survey questions comprised closed and semi-structured questions. The questions were directed towards the participants to focus on their SMEs' implementation, business impact, and competitiveness. The questionnaire complies with GDPR rules for such surveys. Each question carried an explanatory paragraph that guided the participants in the choices available for their answers. Participants were provided with an email address to seek clarifications if the question and its provided explanation needed further clarity.

h) The Questionnaire

The questionnaire consisted of ten questions. The participants were asked to make a single selection to avoid any open-ended answers. The answers had detailed explanations to allow the participants to make their choices with ease and clarity. The questions are listed below:

Screening Questions:

SQ-1. Are you an owner or work with an SME in Europe/EU-27/UK?

Choices: A1- Yes, A2- No

Notes: If the answer to this question is A1, you may proceed and complete the survey. If the answer is A2, please quit the survey.


SQ1. Are you an owner or work with an SME in Europe/EU-27/UK?

#	Answers	Answers (%)	Count
A1	Yes	100.00%	600
A2	No	0.00%	0

TOTAL UNIQUE RESPONDENTS 600/1508

This question reduced the total number of participants from 1506 to 600 participants directly/indirectly working within the EU SMEs.

Participant SME is within EU-27:

Q1. What is the type of business that defines your SME? (Single Selection)

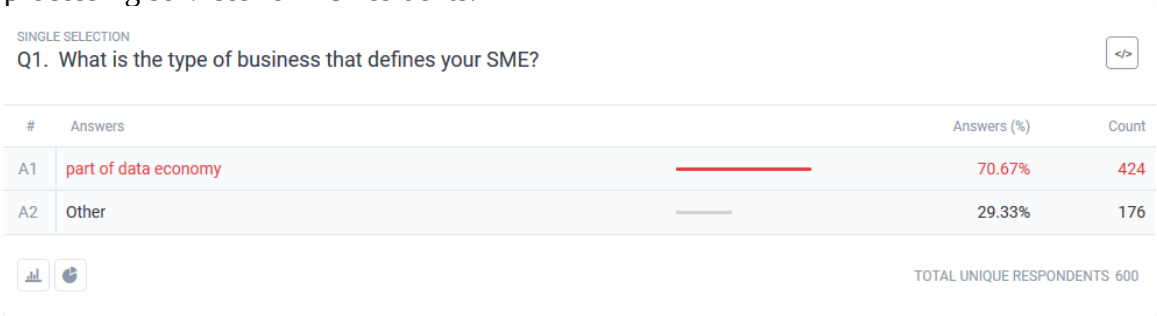
A1- Part of Data Economy

A2- Other

Notes:

A1- Part of the data economy means that your SME is a direct participant in the web-based business or services that utilise EU residents' data, which may **directly** involve accessing, storing, and processing such data using in-house or outsourced data housing and processing services.

A2- 'Other' means that your SME is producing goods and services that rely on web services but do not directly offer web-based services. Your SME is in the category of 'Other' if it may **indirectly** use the services of a company or individuals accessing, storing, or processing EU residents' data but has no in-house or outsourced data processing services for EU residents.


SINGLE SELECTION

Q1. What is the type of business that defines your SME?

#	Answers	Answers (%)	Count
A1	part of data economy	70.67%	424
A2	Other	29.33%	176

TOTAL UNIQUE RESPONDENTS 600

GDPR Preparedness:

Q2. How would you describe the GDPR preparedness of your SME? (Single Selection)

A1- Prepared

A2- Somewhat prepared

A3- Not Prepared

Notes:

A1- Preparation of your SME for GDPR means that your SME has mechanisms (written policies and systems) in place for handling the following mandatory areas of GDPR compliance:

- personal data
- data subject rights
- accuracy and retention
- transparency requirements
- other data controller obligations

- data security
- data breaches
- International data transfers

A2- If your SME is still in the process of preparing the mechanism as listed above in A1 and has covered 5 or more items out of 8 items listed in A1.

A3- If your SME is still in the process of preparing and has covered 4 or fewer items listed in A1 above.

SINGLE SELECTION

Q2. How would you describe the GDPR preparedness of your SME?

#	Answers	Answers (%)	Count
A1	Prepared	45.33%	272
A2	Some what prepared	49.17%	295
A3	Not Prepared	5.50%	33

TOTAL UNIQUE RESPONDENTS 600

GDPR Compliance Challenges for the SME:

Q3- Has your SME faced any legal challenges due to non-compliance with GDPR since May 2018?

A1- Some Challenges

A2- No Challenges

A3- DO not know

Notes:

A1- Some challenges mean that either your SME has (1) Not engaged any legal professionals to assist in preparing and implementing GDPR compliance within your SME or (2) the GDPR compliance preparations are not moving due to any existing legal challenges facing your SMEs business

A2- If your SME has (1) successfully implemented GDPR compliance or (2) a legal team is assisting your firm's GDPR compliance preparations without any known impediments to the process

A3- If your SME has not shared any legal challenges with the staff or has not proceeded to audit its legal compliance with the GDPR preparedness/ implementation.

SINGLE SELECTION

Q3. Has your SME faced any legal challanges due to non compliance of GDPR since May 2018?

#	Answers	Answers (%)	Count
A1	Some challanges	49.17%	295
A2	No challanges	41.50%	249
A3	Do not know	9.33%	56

TOTAL UNIQUE RESPONDENTS 600

Financial Impact of GDPR on the SME:

Q4- Has the business volume of your SME been impacted by the GDPR compliance?

A1- Some Financial Impact

A2- Great Financial Impact
A3- No Financial Impact
A4- Don't know

Notes:

A1- GDPR Preparedness and compliance cost diverted the SME from its core business and resulted in the reduction of its business volume between **10 or less or up to 20%** compared to the year before GDPR preparedness and compliance started for the SME

A2- GDPR preparedness and compliance costs diverted the SME from its core business including diverting its reserve investments for growth. The resultant reduction in the business volume of the SME was **more than 25% and up to 40% or more**.

A3- The SME was already in compliance with previous EU data protection laws and/or the cost of GDPR preparations and compliance neither reduced the business nor increased for more than 5% of its comparable volume a year before GDPR compliance.

A4- SME does not quantify such business volumes or no such information is made available to the staff.


SINGLE SELECTION
Q4. Has the business volume of your SME been impacted by the GDPR complaince?

#	Answers	Answers (%)	Count
A1	Some financial impact	38.17%	229
A2	Great financial impact	29.50%	177
A3	No financial impact	25.33%	152
A4	Dont know	7.00%	42

TOTAL UNIQUE RESPONDENTS 600

GDPR Direct Impact on SMEs Cost of Business:

Q5-Has your SME invested in GDPR preparedness and compliance?

A1-Some investment
A2-Lot of investment
A3-No investment
A4-Don't know

Notes:

A1- SME made investments that were already part of its ongoing GDPR preparedness plans and no extra funding had to be taken out of the business investments or the additional investments for GDPR preparedness did not exceed above 10% of the already anticipated/available budget.

A2- SME made additional investments through 100% borrowing/loans or SME had to supplement its existing budgeted investment for GDPR preparedness that exceeded 60% or more of the budget amount or SME had to divert 100% of its reserve investment funds to ensure GDPR preparedness.

A3- All investment required for SME's GDPR preparedness came in the shape of a national/regional/third-party grant/program that did not impose any financial burden on the SME for its GDPR preparedness.

A4- No such information is kept by the SME or SME staff is not provided with this financial information.

SINGLE SELECTION
Q5. Has your SME invested in GDPR preparedness and compliance?

#	Answers	Answers (%)	Count
A1	Some investment	49.33%	296
A2	Lot of investment	30.83%	185
A3	No investment	12.33%	74
A4	Dont know	7.50%	45

TOTAL UNIQUE RESPONDENTS 600

Direct Impact of GDPR on the SME:

Q6- In your opinion, the GDPR has positively or negatively impacted your SME's business?

A1- Negative Impact

A2- Positive Impact

A3- No Impact

Notes:

A1- The GDPR's negative impact on your SME business is (1) if the SME relied on international business within the data value chain and the upstream business reduced your business volume due to GDPR compliance matters (2) customer trust levels in your company's GDPR compliance efforts reduced the business (3) business is struggling to meet the cost of compliance (4) GDPR compliance had diverted the limited human resource to compliance readiness and reduced business productivity (5) any cost or customer-related adverse impact due to GDPR compliance are harming the SMEs business.

A2- GDPR compliance has improved the customer's confidence and resultantly improved the SMEs business (2) GDPR compliance and readiness have brought new business (3) better ICT systems/ upgrades in software and hardware due to GDPR preparedness are also benefiting the business efficiency (4) staff motivation and confidence has improved with the improvements and upgrades due to GDPR preparedness.

A3- Such data is not maintained by the SME/ Staff does not have any such information/No evidence is seen of any negative or positive impact

SINGLE SELECTION
Q6. In your opinion, the GDPR has positively or negatively impacted your SME's business?

#	Answers	Answers (%)	Count
A1	Negative impact	23.17%	139
A2	Positive impact	53.33%	320
A3	No impact	23.50%	141

TOTAL UNIQUE RESPONDENTS 600

GDPR Impact on Data Privacy of Customers within the SME:

Q7- Has the GDPR changed the privacy policies of your SME?

A1- No change to privacy policies

A2- Some changes to privacy policies

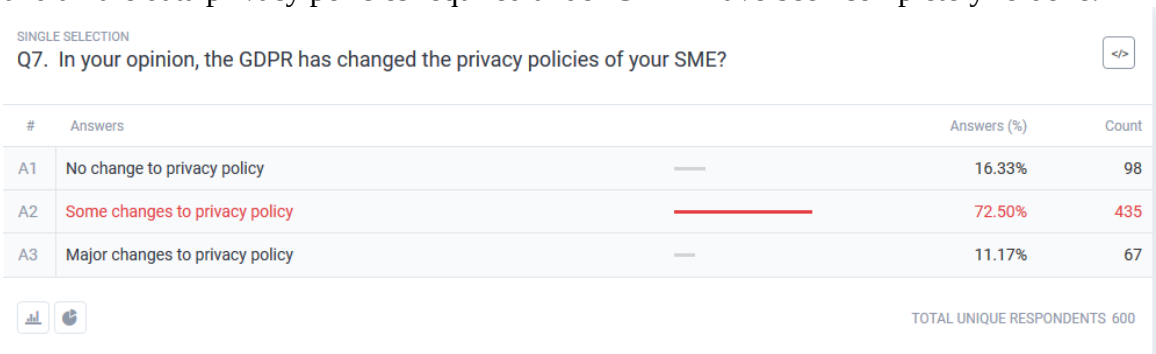
A3- Major changes to privacy policies

Notes:

A1- SME has been keeping up with previous data protection laws of the EU and has been working with much more robust privacy policies that came out to exceed the requirements laid out in GDPR.

A2-SME has been working with the previous data protection policies of the EU and after auditing GDPR requirements, the existing policies are now in compliance with GDPR.

A3- SME did not have any existing data privacy policies/limited privacy policies and all the data privacy policies required under GDPR have been completely re-done.



SINGLE SELECTION

Q7. In your opinion, the GDPR has changed the privacy policies of your SME?

#	Answers	Answers (%)	Count
A1	No change to privacy policy	16.33%	98
A2	Some changes to privacy policy	72.50%	435
A3	Major changes to privacy policy	11.17%	67

TOTAL UNIQUE RESPONDENTS 600

(Reverse Impact-Coding Question to detect false data)

Q8- Do you think that GDPR is the ideal response for data protection, and it will help improve your SMEs business prospects?

A1- Not ideal but will improve the business

A2- Ideal and will improve the business

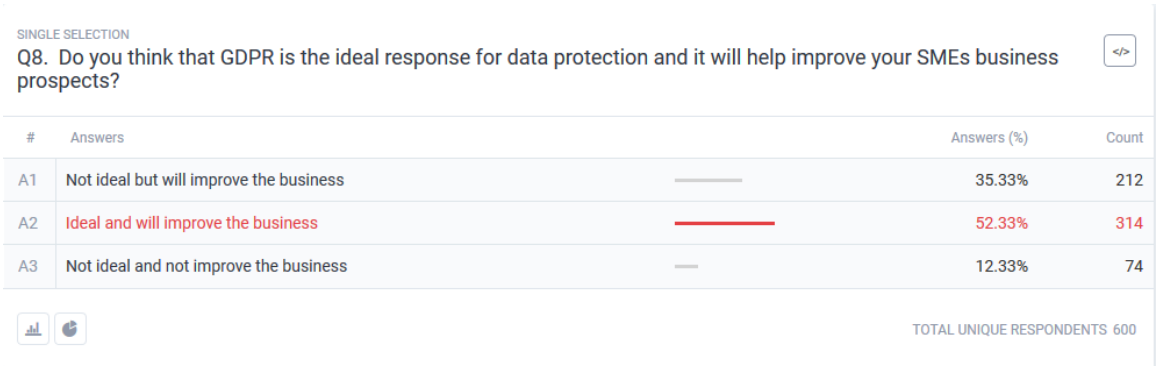
A3- Not ideal and will not improve the business

Notes:

A1- GDPR is vague and complicated and its compliance cost is not suited to the SMEs, however, customer confidence will improve the business in the long run.

A2- GDPR is best suited to protect the customers' data and its compliance costs notwithstanding, it will be a win-win for the data subjects as well as the SME.

A3- GDPR is not suitable for SMEs due to its vague language, and high costs of compliance that are difficult for SMEs to absorb. The anticipated operating costs of the SME will rise with the GDPR ongoing compliance costs and will not be beneficial to the SME business.



SINGLE SELECTION

Q8. Do you think that GDPR is the ideal response for data protection and it will help improve your SMEs business prospects?

#	Answers	Answers (%)	Count
A1	Not ideal but will improve the business	35.33%	212
A2	Ideal and will improve the business	52.33%	314
A3	Not ideal and not improve the business	12.33%	74

TOTAL UNIQUE RESPONDENTS 600

Competitive Advantage to SME- GDPR:

Q9- Do you think that GDPR impacts the competitive advantage of EU SMEs?

A1- No advantage

A2- Some Advantage

A3- Great Advantage

Notes:

A1- GDPR favours tech giants like Google, Facebook, and Microsoft to take the investment capacity to comply and even fight the steep fines for GDPR compliance. Limited financial investment and the detrimental impact of GDPR fines do not offer any advantage to EU SMEs. GDPR is focused more on the data protection rights of the data subjects and does not balance the innovation needs of emerging technologies like AI and Blockchain etc. EU SMEs will be limited to any investments available within the EU only due to restrictions imposed by GDPR for data localisation within the EU.

A2- GDPR compliance costs and steep fines are negative for EU SMEs. US tech giants will be able to navigate the challenges imposed on their businesses due to their investment capacities. However, any limits on US tech giants are likely to improve the business opportunities for EU SMEs as the potential for growth through partnerships and synergy development within the EU will benefit in the long run.

A3-GDPR can harmonise data protection policies across EU-28. It will impose steep fines on any violations of GDPR and improve consumer confidence in their data protection by EU SMEs. Continued compliance with GDPR will improve the data protection systems within the EU and result in improved innovation and business opportunities.

SINGLE SELECTION

Q9. Do you think that GDPR impacts the compatitive advantage of EU SMEs?

#	Answers	Answers (%)	Count
A1	No advantage	21.33%	128
A2	Some advantage	69.33%	416
A3	Great advantage	9.33%	56

TOTAL UNIQUE RESPONDENTS 600

Impact of GDPR on SMEs:

Q10- GDPR will have a long-term impact on the SME's business?

A1- Negative Impact

A2- Positive Impact

A3- Some Impact

A4- No impact

Notes:

A1- GDPR is an overly restrictive data protection law that does not favour the EU SMEs/EU Data Economy due to its high costs of implementation and restrictions imposed on aggregated data products. GDPR does not consider advanced and emerging technologies like AI and Blockchain including personal identity-based customized web products. The venture capital markets of North America/Asia for technology innovation are going to ignore EU SMEs due to restrictive GDPR compliance and data localisation requirements.

A2- GDPR is going to improve the EU's internal data innovation market through data protection law harmonisation. It will improve the flow of venture capital to EU SMEs for technology innovation due to their GDPR compliance edge.

A3- GDPR may improve the EU SMEs' ability to innovate in the long run if the consumers continue to demand higher standards of their personal data protection from tech giants external to EU-27.

A4- The global data economy is much larger and more resilient to any drastic changes to EU legislation for data protection demands. It is unlikely that GDPR will effectively rope in international tech giants for their non-compliance with GDPR concerning EU residents' data.

SINGLE SELECTION

Q10. GDPR will have a long term impact on the SME's business?

#	Answers	Answers (%)	Count
A1	Negative impact	6.17%	37
A2	Positive impact	48.83%	293
A3	Some impact	37.00%	222
A4	No impact	8.00%	48

TOTAL UNIQUE RESPONDENTS 600

5) RESEARCH METHODOLOGY FOR DATA ANALYSIS

a) Research Methodology- Binary Logistical Models (Logit Models)

The use of Logistical Modelling techniques in business statistical data interpretations and inferences is a leading approach. Binary logit models allow researchers to use the collected data and infer if a certain variable, significantly impacts and affects the outcomes. We chose the binary logit model approach to study the GDPR impact on EU SMEs as it allows for a focused inference as a standard approach for testing the predictive value of GDPR on EU SMEs.

Logistical models including binary logistical models allow business researchers to process dependent data by assigning values of 0 or 1. In the case of our research, the modelling would help explain if the EU SMEs experienced a negative or positive impact post-May 2018, due to the implementation of GDPR.

Binary Logistic regression is also commonly used in business research for the prediction and classification of unique problems such as the imposition of mandatory regulations and sanctions. Lastly, the robustness of the data collected can be tested using the Binary Logistic regression models as they can identify data anomalies, such as false data.

The GDPR not only applies to and impacts EU SMEs, it also impacts EU SMEs' business across the EU borders. The transnational reach of GDPR on the EU SMEs has been catered to by using the Ordinary Least Squares (OLS) regression technique. OLS regression technique for binary logit modelling is the best-known approach for variables that require global modelling using spatial regression analyses.

OLS regression has been chosen as an optimization strategy for a straight line or the closest possible data points for the linear regression equation formulated for this research. OLS is also considered the best optimization strategy within business research for binary regression models to find unbiased real value estimates for the beta.

b) Data & Logit Estimation Empirical Strategy using Binary Logit Model

This research uses binary logistic regressions (otherwise known as logit) to estimate the effect of explanatory variables on a binary choice outcome.

Survey responses are grouped to allow for a binary result. For example, for Question 1, the choice is identifying as in the data economy (1) or not being in the data economy (0). Logit allows us to calculate the probability that a respondent chooses 1 rather than 0.

Logit assumes that the joint density of errors is independent and identically distributed *(i.i.d.)* type I extreme value (Gumbel) with a variance equal to *π 2/6,* which allows for a simple closed-form expression for choice probabilities.

Modelling as a binary logit choice probability requires the form:

$$P_{n1} = \frac{e^{V_{n1}}}{e^{V_{n1}} + e^{V_{n2}}} = \frac{1}{1 + e^{-(V_{n1} - V_{n2})}}$$

Pn1 = e Vn1 e /Vn1 + e Vn2 = 1 /1 + e−(Vn1−Vn2)

Here *Vni* is the utility of choice *i* for person *n*, which is determined based on observed attributes from the survey data. Combined with our unobserved utility (*our logit errors*), this represents the true utility of each choice.

Writing both probabilities as an odds ratio gives:

$$\frac{P_{n1}}{P_{n2}} = e^{V_{n1} - V_{n2}}$$

(Pn1/ Pn2 = e Vn1−Vn2)

Taking the log odds ratio of choice 1:

$$ln(\frac{P_{n1}}{1 - P_{n1}}) = V_{n1} - V_{n2} = \beta'(x_{n1} - x_{n2}) = \beta' x_n$$

(ln(Pn1 /1 − Pn1) = Vn1 − Vn2 = β ′(xn1 − xn2) = β ′xn)

Where xn = (xn1, xn2) contains data about both choices.

This provides a linear form, allowing us to use OLS to estimate these probabilities. In other words, the β's are estimated by using the difference between the observations for respondents choosing 1 and the observations for respondents choosing 0.

Coefficients should be interpreted as log-odds, meaning that if a coefficient value is 0.5, then that explanatory variable has the effect of increasing the probability of choice 1 by e 0 .5 = 1.6847 times.

If our variable was discrete, this would be a unit increase in probability. If the variable is a dummy variable, it's a one-time effect.

To ensure the robustness of our data analysis, we are only showing results with robust standard errors. Coefficients in our data analysis should be interpreted as log odds, meaning thereby that, *e^(beta)* readings allow us to observe how many times, the effect of GDPR increased or decreased when the survey participants chose 1.

The binary logit regressions have been applied to nine of the survey questions by excluding Question 8. Question 8 was a reverse coding question rephrased to check for response bias within the survey. The response bias check through question 8 would not allow it to fit into the needed structure for our binary logit regression model.

c) Log Odd Ratios & Independent Variables of the Data

The research calculated the log-odds ratios for the survey participants' choices between 0 and 1 as a dependent variable. In other words, we estimated the *probability* that the respondent chose to answer 1 instead of 0.

The independent variables selected to calculate log-odd rations are the ones that showed any or some significance for one or more one or more survey questions. The independent variables that are used as regressors in each question are defined as follows:

- D is a dummy for treatment (=1 if within the EU).
- Gender is a dummy for women (=1 if female).
- PoC is a dummy for non-white (=1 if any other response than white).
- Age is a continuous variable of the respondents' age.
- Low is a dummy for low-income (=1 if in a low-income tier).
- High is a dummy for high-income (=1 if in a high-income tier).
- High school is a dummy for low education (=1 if middle or high school is the highest obtained).
- Technical college and postgraduate are also dummies.
- High Tech is a dummy for a career description likely to be impacted by GDPR. High-tech is roughly half of the data samples which includes high-tech services and all data-reliant industries within the EU.
- Mgmt is a dummy for management positions (=1 if product manager, middle manager, or CTO)
- Owner is a dummy for owners/partners (=1 if owner-partner).

The omitted categories were university education, middle income, non-managerial staff, etc. and are treated as the reference groups in this context.

d) Data Analysis

Base Line Model:

$$Y\_i=\alpha+\delta D\_i+X\_i\,\gamma+ Z\_i\,\tau+ \mu\_i$$

The aim here is to test the question outcomes Y_i as a function of the treatment effect δ (where D=1 if the respondent is in an EU-27/ GDPR compliant country) and other covariates that do not impact the treatment status. These include respondent demographic information X_i such as gender, race, and income, or industry / firm-level information Z_i such as the number of employees or equipment details etc.

Additionally, we matched respondents in the treatment and control groups to see if it's possible to obtain treatment effects outside of a regression.

e) Basic Descriptive Statistics

Respondents:

- 600 total respondents
- Respondents located in the UK (53.17%) counted as the control group.

Demographics:

- Respondents who identify as female (47%)
- Respondents who identify as non-white (27.06%).
- The average age of respondents is ~40. The median is 38. The youngest is 22, oldest is 69.
- The average number of children is less than 1 (0.7798).
- Respondents are single (34%), married (34%), or partnered (25%).
- Respondents' highest educational achievements were high school (17%), technical college (23%), university (39%), and graduate school (13%).
- The average number of languages spoken is 1.693. The median is 1.
- Incomes are distributed as lowest (15%), low (18%), low middle (32%), high middle (17%), high (9.5%), higher (4.5%), and highest (1%).
- Industry / Firm-Level Characteristics
- Respondent roles vary from technical staff (12%) and other non-management (21%) roles to product managers (4%) and middle managers (36.5%) to owners/partners (22%) and CTOs (4.5%).
- The number of employees varies from six to ten (19%), eleven to twenty-five (26%), fifty-one to one hundred (32%), to one hundred to two hundred fifty (23%).

Fama-French 10-Industry classification:

- Durables (4%)
- Nondurables (1%)
- Manufacturing (5.5%)
- High Tech (18%)
- Telecommunications (1.5%)
- Shops/Retail (7%)
- Healthcare (6.5%)
- Utilities (1%)
- Other (55%)

Technology Platforms:

- The manufacture of firms ICT equipment is American (12%), Korean (6%), Taiwanese (0.5%), Chinese (5.5%), Japanese (0.1%), or undeclared (75%).
- The systems used for data storage are Android (25%), iOS (31%), and web interfaces (44%).

i) Statistical Data Analysis Results

Question 1: What is the type of business that defines your SME?

Answer: Data Economy = 1 (70%), Other = 0 (30%)

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q1_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)        1.67371    0.44838   3.733 0.000189 ***
D                  0.05443    0.21170   0.257 0.797085
Gender            -0.15004    0.20003  -0.750 0.453210
PoC                0.13023    0.23148   0.563 0.573708
Age               -0.03347    0.00871  -3.843 0.000121 ***
low               -0.51554    0.22699  -2.271 0.023134 *
high               0.02587    0.30291   0.085 0.931944
high_school        0.35541    0.25520   1.393 0.163728
technical_college  0.30928    0.26052   1.187 0.235173
postgraduate       0.53892    0.33199   1.623 0.104524
High_Tech          0.01860    0.19815   0.094 0.925199
mgmt               0.77346    0.22942   3.371 0.000748 ***
owner              0.76925    0.27826   2.764 0.005702 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 662.57  on 543  degrees of freedom
Residual deviance: 622.83  on 531  degrees of freedom
  (56 observations deleted due to missingness)
AIC: 648.83

Number of Fisher Scoring iterations: 4
```

Question 2: How would you describe the GDPR preparedness of your SME?

Answer: Prepared / somewhat prepared = 1 (95%), Not prepared = 0 (5%)

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q2_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)        5.308308   0.931007   5.702 1.19e-08 ***
D                 -0.249687   0.407570  -0.613   0.5401
Gender             0.164324   0.402529   0.408   0.6831
PoC               -0.653920   0.421518  -1.551   0.1208
Age               -0.047610   0.015616  -3.049   0.0023 **
low               -0.712635   0.425747  -1.674   0.0942 .
high               0.302046   0.685242   0.441   0.6594
high_school       -0.172686   0.477089  -0.362   0.7174
technical_college  0.020153   0.494851   0.041   0.9675
postgraduate       1.552856   1.065404   1.458   0.1450
High_Tech         -0.203011   0.392993  -0.517   0.6055
mgmt              -0.009658   0.450822  -0.021   0.9829
owner              0.298995   0.571859   0.523   0.6011
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 237.83  on 543  degrees of freedom
Residual deviance: 217.17  on 531  degrees of freedom
  (56 observations deleted due to missingness)
AIC: 243.17

Number of Fisher Scoring iterations: 7
```

Question 3: Has your SME faced any legal challenges due to non-compliance of GDPR since May 2018?

Answer: Some challenge = 1 (55%), No challenge = 0 (45%)

"Do not know" responses are dropped, leaving 544 responses.

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q3_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       -0.215458   0.445068  -0.484 0.628314
D                  0.754726   0.207895   3.630 0.000283 ***
Gender             0.096830   0.196913   0.492 0.622905
PoC                0.469910   0.224181   2.096 0.036071 *
Age               -0.027702   0.008939  -3.099 0.001942 **
low                0.172358   0.228593   0.754 0.450853
high               0.529610   0.287986   1.839 0.065913 .
high_school        0.518897   0.252234   2.057 0.039667 *
technical_college  0.280408   0.258622   1.084 0.278260
postgraduate       0.721649   0.315755   2.285 0.022285 *
High_Tech         -0.016949   0.195379  -0.087 0.930869
mgmt               0.824148   0.234977   3.507 0.000453 ***
owner              0.760720   0.278517   2.731 0.006308 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 686.80  on 496  degrees of freedom
Residual deviance: 625.71  on 484  degrees of freedom
  (47 observations deleted due to missingness)
AIC: 651.71

Number of Fisher Scoring iterations: 4
```

Statistical Analysis for Hypothesis: Question 3 shows a **highly significant effect of treatment being 0.75**. The interpretation is that being in the EU increased the probability of facing legal challenges related to GDPR compliance by 0.75 percentage points.

Question 4: Has the business volume of your SME been impacted by the GDPR compliance?

Answer: Some or great impact = 1 (73%), No impact = 0 (27%)

"Do not know" responses are dropped, leaving 558 responses.

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q4_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       0.921138   0.477988   1.927 0.053966 .
D                 0.882920   0.241044   3.663 0.000249 ***
Gender            0.045012   0.216063   0.208 0.834971
PoC               0.269632   0.261871   1.030 0.303180
Age              -0.018208   0.009421  -1.933 0.053273 .
low               0.508085   0.258502   1.965 0.049357 *
high              0.224605   0.313466   0.717 0.473668
high_school       0.097158   0.276682   0.351 0.725472
technical_college -0.202441   0.275943  -0.734 0.463172
postgraduate      0.496901   0.378188   1.314 0.188880
High_Tech        -0.415704   0.217733  -1.909 0.056232 .
mgmt              0.817676   0.257851   3.171 0.001519 **
owner             0.300339   0.297482   1.010 0.312685
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 586.20  on 507  degrees of freedom
Residual deviance: 537.49  on 495  degrees of freedom
  (50 observations deleted due to missingness)
AIC: 563.49

Number of Fisher Scoring iterations: 4
```

Statistical Analysis for Hypothesis: Question 4 shows a **highly significant effect of treatment of 0.88**. The interpretation is that SMEs being in the EU increased the probability of facing business impact related to GDPR compliance by 0.88 percentage points.

Question 5: Has your SME invested in GDPR preparedness and compliance?

Answer: A lot of investment =1, Some investment = 0

"Do not know" are dropped, so are "no investment" answers, leaving 481 responses.

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q5_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       -0.079285   0.482780  -0.164  0.86955
D                  0.378745   0.214452   1.766  0.07738 .
Gender             0.226582   0.206430   1.098  0.27237
PoC                0.226856   0.229691   0.988  0.32332
Age               -0.026329   0.009691  -2.717  0.00659 **
low                0.150466   0.239475   0.628  0.52980
high               0.084002   0.291102   0.289  0.77291
high_school        0.242824   0.265003   0.916  0.35951
technical_college -0.105418   0.280089  -0.376  0.70664
postgraduate       0.218856   0.308286   0.710  0.47776
High_Tech          0.023406   0.206422   0.113  0.90972
mgmt               0.189139   0.250458   0.755  0.45015
owner              0.176481   0.291256   0.606  0.54456
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 579.34  on 436  degrees of freedom
Residual deviance: 558.73  on 424  degrees of freedom
  (44 observations deleted due to missingness)
AIC: 584.73

Number of Fisher Scoring iterations: 4
```

Statistical analysis for hypothesis: Question 5 shows a **low significant effect of treatment of 0.37**. The interpretation is that the probability of EU SMEs investing in GDPR compliance is low by 0.37 percentage points.

Question 6: In your opinion, the GDPR has positively or negatively impacted your SME's business?

Answer: Negative impact = 1 (30%), Positive impact = 0 (70%)

"No impact" answers are dropped, leaving 459 responses.

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q6_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       -0.211396   0.516550  -0.409   0.6824
D                 -0.480746   0.234724  -2.048   0.0405 *
Gender            -0.581705   0.229536  -2.534   0.0113 *
PoC               -0.075874   0.253663  -0.299   0.7649
Age                0.017708   0.009852   1.797   0.0723 .
low               -0.392522   0.263398  -1.490   0.1362
high               0.022935   0.318884   0.072   0.9427
high_school        0.028480   0.291000   0.098   0.9220
technical_college -0.534329   0.310968  -1.718   0.0857 .
postgraduate       0.162787   0.341089   0.477   0.6332
High_Tech         -0.477376   0.225508  -2.117   0.0343 *
mgmt              -0.564975   0.271005  -2.085   0.0371 *
owner             -0.356179   0.315124  -1.130   0.2584
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 511.91  on 415  degrees of freedom
Residual deviance: 486.18  on 403  degrees of freedom
  (43 observations deleted due to missingness)
AIC: 512.18

Number of Fisher Scoring iterations: 4
```

Statistical analysis for the hypothesis: the negative values across the variable provide inconclusive results to provide negative or positive probable impact on EU SMEs.

Question 7: In your opinion, the GDPR has changed the privacy policies of your SME?

Answer: Some / major changes = 1 (83%), No changes = 0 (17%)

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q7_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       0.994647   0.547932   1.815  0.06948 .
D                 0.329322   0.259921   1.267  0.20515
Gender            0.318651   0.248473   1.282  0.19969
PoC              -0.343476   0.274018  -1.253  0.21003
Age               0.008311   0.010860   0.765  0.44409
low              -0.194305   0.269796  -0.720  0.47141
high              0.682480   0.474818   1.437  0.15062
high_school      -0.790138   0.329865  -2.395  0.01660 *
technical_college -0.942493   0.326284  -2.889  0.00387 **
postgraduate     -0.323376   0.444468  -0.728  0.46688
High_Tech         0.556616   0.250803   2.219  0.02646 *
mgmt              0.413202   0.268572   1.539  0.12392
owner             1.338845   0.419199   3.194  0.00140 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 484.81  on 543  degrees of freedom
Residual deviance: 439.40  on 531  degrees of freedom
  (56 observations deleted due to missingness)
AIC: 465.4

Number of Fisher Scoring iterations: 5
```

Statistical Analysis for the Hypothesis: Question 7 shows a **low significant effect of treatment of 0.32**. The interpretation is that the probability of EU SME privacy policies changing due to GDPR compliance is 0.32 percentage points.

Question 9: Do you think that GDPR impacts the competitive advantage of EU SMEs?

Answer: Great / some advantage = 1 (78%), No advantage = 0 (22%)

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q9_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)       1.114151   0.478934   2.326  0.02000 *
D                 0.560871   0.243821   2.300  0.02143 *
Gender            0.398771   0.223882   1.781  0.07489 .
PoC               0.499203   0.275835   1.810  0.07033 .
Age              -0.028954   0.009513  -3.044  0.00234 **
low               0.393738   0.267161   1.474  0.14054
high              0.072800   0.318311   0.229  0.81910
high_school       0.558634   0.289760   1.928  0.05386 .
technical_college 0.405415   0.286137   1.417  0.15652
postgraduate      0.456468   0.361513   1.263  0.20671
High_Tech         0.316071   0.220186   1.435  0.15115
mgmt              0.280416   0.252889   1.109  0.26750
owner             0.724962   0.334229   2.169  0.03008 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 568.99  on 543  degrees of freedom
Residual deviance: 529.51  on 531  degrees of freedom
  (56 observations deleted due to missingness)
AIC: 555.51

Number of Fisher Scoring iterations: 4
```

Key Statistical Analysis of the Hypothesis: Question 9 shows a medium **effect of treatment of 0.56**. The interpretation is that the probability of GDPR providing a competitive advantage to EU SMEs is 0.56 percentage points. However, within the EU SME High Tech sector the probability drops to 0.31 percentage points.

Question 10: GDPR will have a long-term impact on the SME's business?

Answer: Some / positive / negative impact = 1 (92%), No impact = 0 (8%)

```
Call:
glm(formula = response ~ D + Gender + PoC + Age + low + high +
    high_school + technical_college + postgraduate + High_Tech +
    mgmt + owner, family = "binomial", data = q10_data)

Coefficients:
                  Estimate Std. Error z value Pr(>|z|)
(Intercept)        2.39965    0.69015   3.477 0.000507 ***
D                  0.40358    0.35573   1.135 0.256581
Gender             0.02774    0.32030   0.087 0.930985
PoC               -0.12718    0.37984  -0.335 0.737761
Age               -0.02721    0.01359  -2.002 0.045295 *
low                0.65701    0.39156   1.678 0.093363 .
high               0.62919    0.52246   1.204 0.228480
high_school        0.21017    0.40094   0.524 0.600138
technical_college  0.32981    0.41440   0.796 0.426113
postgraduate       0.63713    0.58017   1.098 0.272133
High_Tech          0.06952    0.31897   0.218 0.827480
mgmt               0.79349    0.36557   2.171 0.029967 *
owner              0.64433    0.45470   1.417 0.156470
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 315.26  on 543  degrees of freedom
Residual deviance: 299.25  on 531  degrees of freedom
  (56 observations deleted due to missingness)
AIC: 325.25

Number of Fisher Scoring iterations: 5
```

Statistical analysis for the hypothesis: Question 10 shows a **low significant effect of treatment of 0.40**. The interpretation is that the probability of long-term impact on EU SMEs related to GDPR compliance is 0.40 percentage points.

i) Summary of Statistical Analysis

Description of Choices and Variables: The same explanatory variables are used to estimate Questions 1-7, 9, and 10. Answers to Question 8 were omitted due to it being a reverse coding question to eliminate false data. Binary choices are set up for each question as:

Question 1: 1 = Data Economy, 0 = Other
Question 2: 1 = Prepared, 0 = Not Prepared
Question 3: 1 = Yes, 0 = No
Question 4: 1 = Yes, 0 = No
Question 5: 1 = Yes a lot, 0 = Yes a little
Question 6: 1 = Negative impact, 0 = Positive impact
Question 7: 1 = Yes, 0 = No
Question 9: 1 = Yes, 0 = No
Question 10: 1 = Yes, 0 = No

Statistical Significance for the Hypothesis: The variables used to run logit regressions are the purposes of our hypothesis are as follows:

- **Treatment (D):** Our treatment variable is a dummy, D, which indicates that a respondent is from an SME within the EU-27, implying enforcement of GDPR compliance. Otherwise, a respondent is outside of the EU. Interpret coefficients on D as representing the impact of GDPR compliance on respondent choice probabilities.

  Significance: This is highly significant and positive for Questions 3 and 4, while positive and less significant for Questions 6 and 9.

- **Gender:** There is a dummy for gender which indicates when a respondent is female. The reference group is then all male respondents and we can interpret the coefficient on gender as representing the impact of being a female on a respondent's choice probabilities.

  Significance: This is of low significance and negative for Question 6, indicating a reduced probability of saying there was a negative impact from GDPR for women working in EU SMEs. By probability, it discards the possibility of any gender bias when it comes to the impact of GDPR on EU SMEs.

- **Ethnic Minorities (POC)**: This is a dummy variable that indicates ethnic minorities amongst the respondents. The reference group is then Caucasian respondents. Interpreting this variable is interesting as it allows further research into the topic from the perspective of the application of GDPR compliance penalties within the EU SMEs based on ethnicity.

Significance: This is of low significance but positive for Question 3, meaning that there is an increased probability of facing legal challenges by ethnic minorities within the EU SMEs for GDPR non-compliance. It has no impact on the other questions.

- **Age**: Age is a variable calculated by taking the difference between their birth year and the year of response, which should approximate their exact age. We have interpreted the impact as the increased probability based on a 1-year increase in the age of the respondent.

  Significance: This is significant for varying degrees when it comes to GDPR impact within the EU SMEs for Questions 4, 6 and 7. The probability is negative for Questions 1, 2, 3, 5, 9, and 10. Interpretation of age as an independent variable for its impact depends on the question and binary choice in question, but this seems to be a truly significant factor for almost every question.

- **Income:** Respondents had to indicate their level of income, so all low, middle, and high responses were grouped. Dummies are only regressed for low and high-income individuals, leaving middle-income as the reference group.

  Significance: Low income was weakly significant and negative for Question 1, but otherwise was insignificant for all the other questions. High income seems to have had no GDPR impact. A significant analysis is that the data shows lower-income respondents are less likely to be part of the data economy / EU SMEs within the data business due to cost barriers, etc.

- **Education**: Respondents had to indicate their highest level of schooling, so these responses were grouped (middle school and high school were combined) and used as dummy variables. Bachelor degrees were omitted as the reference group.

  Significance: High school education is of low significance and positive for Question 3, while both high school and technical college were of low significance and negative for Question 7. Postgraduate education seems to have no impact.

- **Industry**: We grouped the industry responses into two groupings: one related to the data economy (high technology) and those that were not. The dummy used is for high-technology firms.

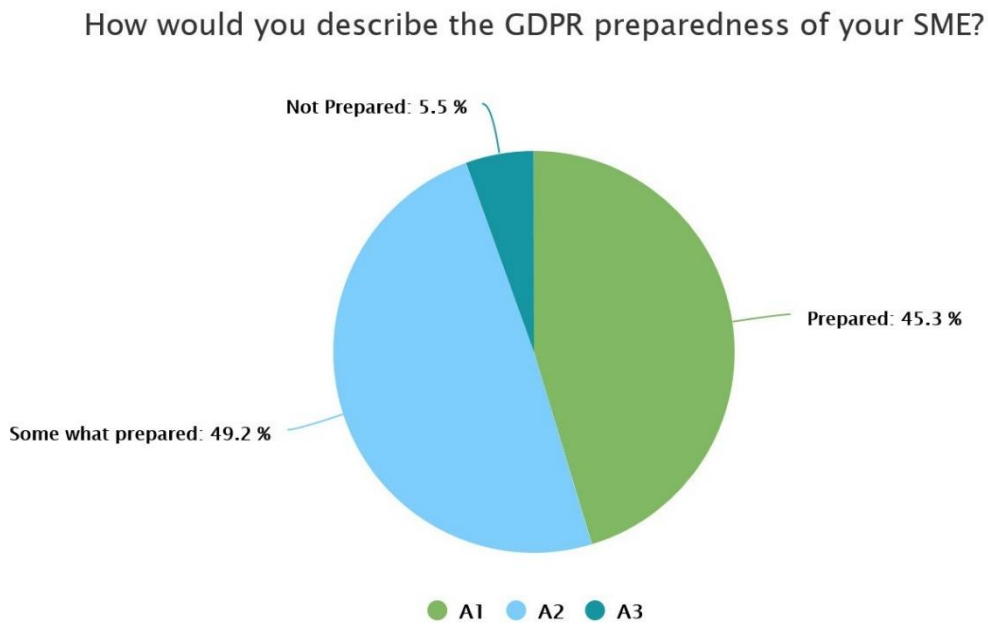
  Significance: High technology was of low significance and negative for question 6. It was also of low significance and positive for Question 7.

- **Occupation/Ownership**: Respondents were also asked to indicate their role in the EU SME being surveyed. These were grouped into non-management, management, and owner categories and used as dummy variables. Non-management staff were omitted as the reference group.

  Significance: Management and owners were both strongly significant and positive for Questions 1 and 3. This is also true for management with Question 4, but not for owners. Management is of low significance and negative for Question 6, and low significance and positive for Question 10. Ownership is of strong significance and positive for Question 7, and low significance and positive for Question 9.

6) THESIS HYPOTHESIS WITH LIT REVIEW

a) Finding 1- SME Preparedness of GDPR



EU SMEs' preparedness for GDPR since May 25, 2018, has been a topic of great discussion within the wider business community of the EU. Implementation of GDPR for SMEs is not an optional matter within the EU. It is mandatory compliance. Any infringement of GDPR can result in huge fines. Also, compared to the previous EU legislation for data protection that had reached within the EU, GDPR has a global reach.

The question of EU SME preparedness speaks directly to the question of business competitiveness and subsequently business survival. EU SMEs are now subjected to a much tighter regime of data protection compared to SMEs in other parts of the world that may potentially deal with EU data. The survey result found that 49.2% of participants declared partial GDPR preparedness of their SMEs and 45.3% declared full preparedness.

Data collected by various research organisations within the EU have done surveys to check compliance with GDPR within the EU SMEs but have not paid much attention to the foremost reason behind the compliance i.e., SMEs preparedness to meet the compliance standards.

Data and Marketing Association (DMA), UK surveyed in November 2019 about the SMEs' awareness and compliance with GDPR. (*DMA Survey Highlights Gaps in SME GDPR Knowledge and Compliance | News*, n.d.) The DMA survey included 293 respondents compared to our survey which had 319 respondents. DMA survey showed that 68% of the respondents claimed that they had good to moderate awareness of GDPR. Our survey shows that out of the 319 respondents from the UK, 159 (46.9%) stated that their SMEs were prepared for GDPR in 2020.

Baker McKenzie surveyed GDPR preparedness (named as 'run-mode' in their survey in late 2019. (*Gdpr_survey.Pdf*, n.d.) McKenzie (2020) found that 47% of the respondents considered the preparedness of their SMEs in line with the GDPR requirements.

McKenzie's data and findings are consistent with the data found through our survey. Martin Brodin(Brodin, 2019a) did a literature review of GDPR readiness and compliance literature in April 2019. Brodin indicates a baseline of 30% of SMEs considered their readiness for GDPR in December 2018. Using Brodin's 2018 findings and McKenzie's 2019 findings, the GDPR preparedness findings of this survey are consistent.

b) Finding-2 GDPR Implementation Challenges for SMEs

The survey found 49.2 respondents stating some challenges to implementing GDPR within their SMEs. Upon clarification from the respondents, the respondents stated that their SMEs managed their GDPR challenges internally and felt secure in their process of GDPR compliance.

The bigger problem posed by GDPR for SMEs is that the regulation applies if the data controller/processor and the data subject are based. The regulation also applies if the data controller/processor is outside the EU, but the data subject is an EU resident.

Note the difference between EU residents and EU citizens. GDPR as a single set of rules applies to all EU member states and any business organisations within the EU. GDPR Article 7-Consent of the data subject, Article 35 -Data Protection Impact Assessment, and Article 32- Data breaches are some of the biggest challenges faced by SMEs processing EU resident data. Any violation or non-compliance with the specified articles can result in huge fines that can result in catastrophic financial losses for any SME.

The use of machine-learning-based algorithms commonly referred to as AI or *artificial intelligence* relies on using personal data sets to create economic benefits for web-based services. The benefits are in terms of matching a data subject's profile with products and services being advertised on the web, as an example. Data bots are being

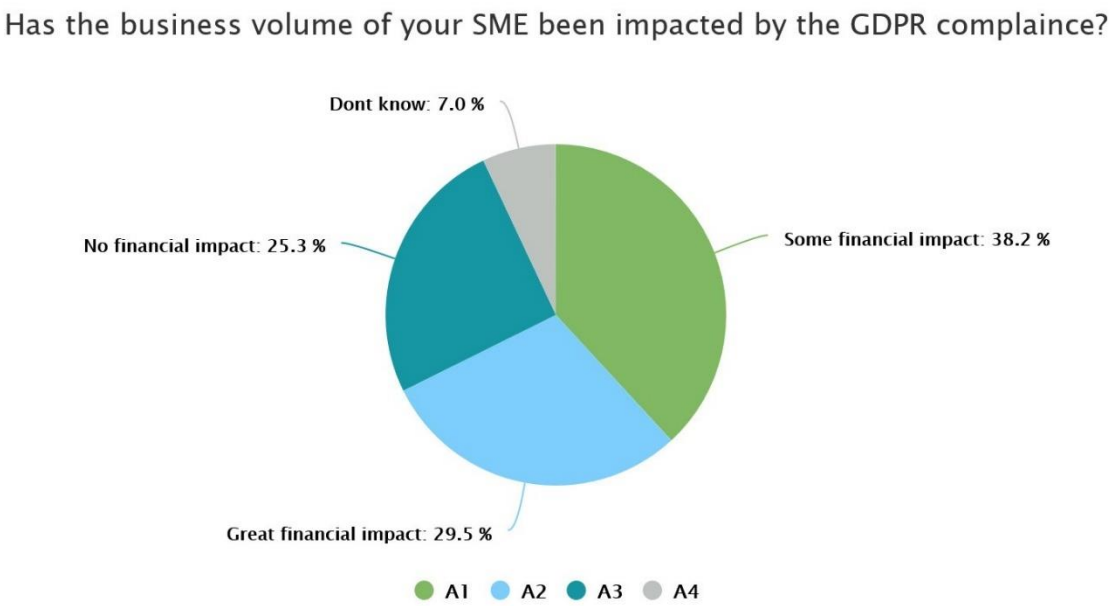
increasingly used by web service providers to provide 24/7 customer chat for various services. These data bots collect the user data and match it with service agents in various jurisdictions for better response.

These advanced AI algorithms are now part of web services globally. Companies that Amazon. Facebook (Meta), IBM Twitter etc. access, store and process billions of personal data sets in microseconds across the globe. It is impossible to keep track of specific EU resident data crisscrossing networks that may or may not comply with GDPR. EU SMEs within such complex data chains are still subjected to any breaches of GDPR if any data subject raises concerns under the legally restrictive clauses Articles 7, 32 and 35.

The response from survey respondents specifically touches upon these legal challenges faced by EU SMEs with the enforcement of GDPR. On the converse side, 41.5% of respondents reported no challenges in the survey. Upon clarification with the respondents, the reason stated for no challenges was consultation with lawyers/legal experts to manage GDPR compliance.

A German software company ECOMPLY surveyed 100 software companies (SMEs) worldwide. All companies selected for their survey either operated in the EU or stored/processed EU resident data. Their survey indicated that 42% of respondents consulted lawyers to advise on GDPR compliance. 50% of respondents did not seek any external help and managed the compliance internally. (*GDPR Readiness Survey for Software and SMEs | ECOMPLY.Io*, n.d.) The data from ECOMPLY confirms the findings of our survey and provides corresponding data results.

c) Finding 3- Business Impact due to GDPR Compliance on SMEs



The fundamental question of increased regulatory compliance for SMEs and its impact on their business bottom line is always complex. Regulations usually entail investment for their compliance and are thought to benefit the business growth in the

long term. The supra-national and international reach of GDPR along with a single set of rules governing the storage and processing of individual data is new territory.

Limited research has emerged on the true impact of GDPR compliance on SMEs in general and EU SMEs in particular. While a lot of literature is available on general information about GDPR etc. both pre and post-May 2018, zero search results returned any word pairing "GDPR benefits for SMEs" or "GDPR Benefits for EU SMEs" anywhere during the forward and backward searches.

The proportionality principle guiding lawmakers to enact business regulations demands any cost related to new regulation compliance must be commensurate with the intended benefits. For SMEs, it directly translates into their ability to survive and generate business specifically related to the new regulations. Since compliance with GDPR is mandatory, EU SMEs have been actively taking measures to ensure compliance and avoid any hefty fines related to non-compliance.

This survey finding specifically related to business benefit or dis-benefit was framed specifically to address the absent data presently existing in the literature. The findings of this particular survey question may potentially spur further research on the topic. Our survey respondents indicate that 29.5% of respondents found GDPR to have a great financial impact on their business. Upon clarification, the group indicated that the impact has been in terms of the added financial burden for compliance, increasing their cost of business and reducing their business volume.

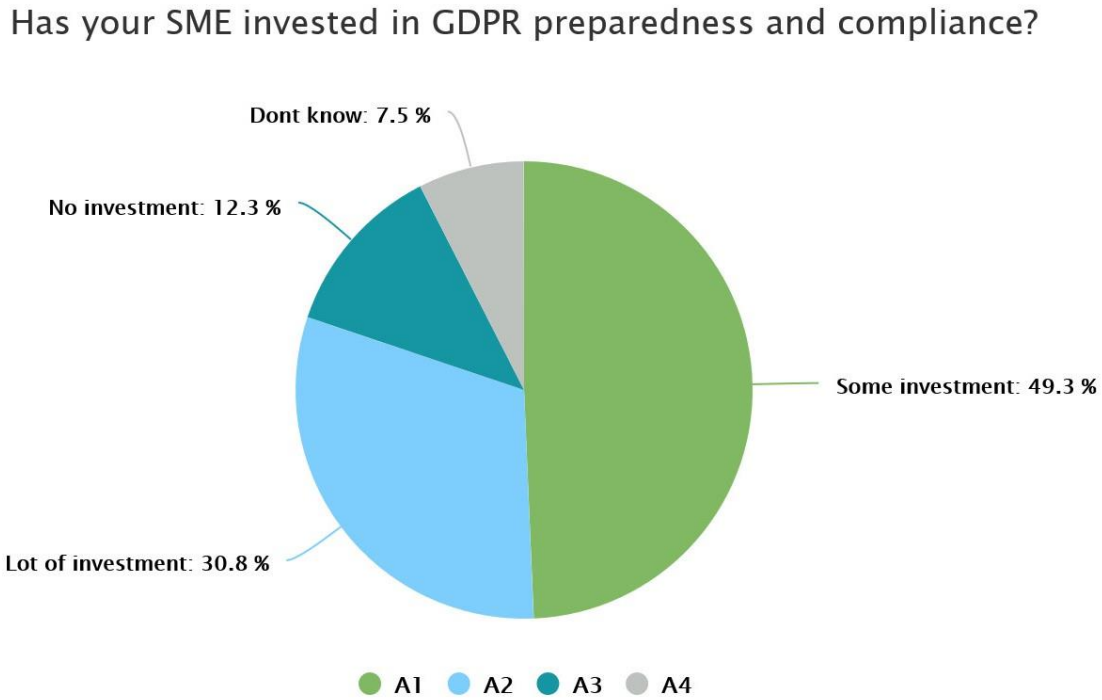
In a study published by University College London(Buckley et al., 2021) in October 2021, the benefit element of GDPR's impact on SMEs has been discussed. In the conclusion section on page 13, the authors draw the same conclusion that has been surmised above in the discussion, related to the benefit to the business vis-à-vis GDPR.

The authors conclude,

> "GDPR is a regulation that is designed to safeguard EU citizens' data privacy. The benefits to the consumer and the regulator and the downsides to business are relatively predictable. What we are interested in however is whether there are any benefits of GDPR to business and how they might affect the different parts of an organisation. To our knowledge, nobody has looked at this from the perspective of business since GDPR came into effect in May 2018."(Buckley et al., 2021, p. 13)

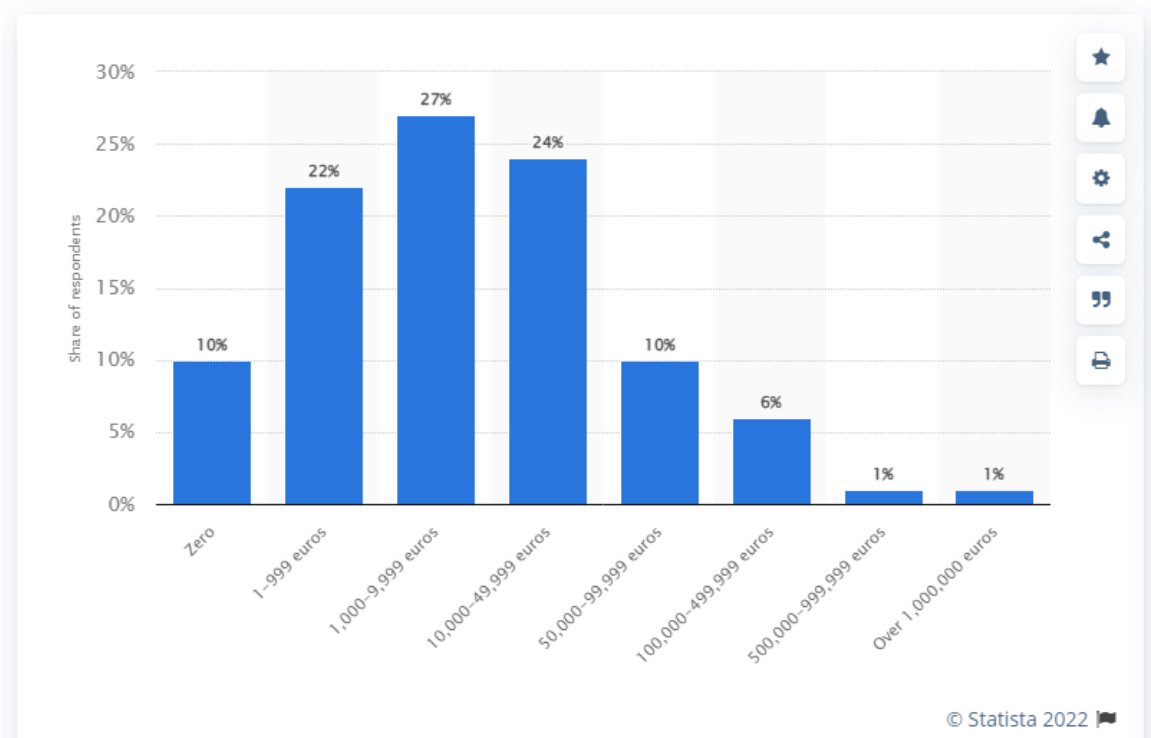
GDPR applies the same set of rules for large multinational data corporations such as Amazon, Google etc. to SMEs. This does not level the playing field in any way for SMEs with limited budgets and resource constraints. It remains to be seen how the future business modelling of SMEs will emerge when better-quantified data emerges after a few years.

d) Finding 4- SME Investment in GDPR Compliance



GDPR preparedness and compliance costs for EU SMEs are still an unsettled question due to the dynamic nature of GDPR compliance that requires continued investment. The preparedness costs are linked to;(1) improving data storage (2) staff training (3) auditing existing data security compliance with GDPR etc. The compliance costs related to setting up systems to seek consumer consent at every event pre-processing, having systems in place for notification to inform the data subject in case of breach etc.

Cursory references exist in the literature to offer any quantifiable data that alludes to the EU SMEs' spending/cost for GDPP preparedness and compliance. The most sensible reason could be that GDPR is still in its infancy and such data would emerge as the regulation compliance matures over time. Researcher Joseph Johnson published his findings on Statista in November 2020. (*EU*, n.d.) The graph below represents his findings that are grouped in terms of the Euro spending percentile.



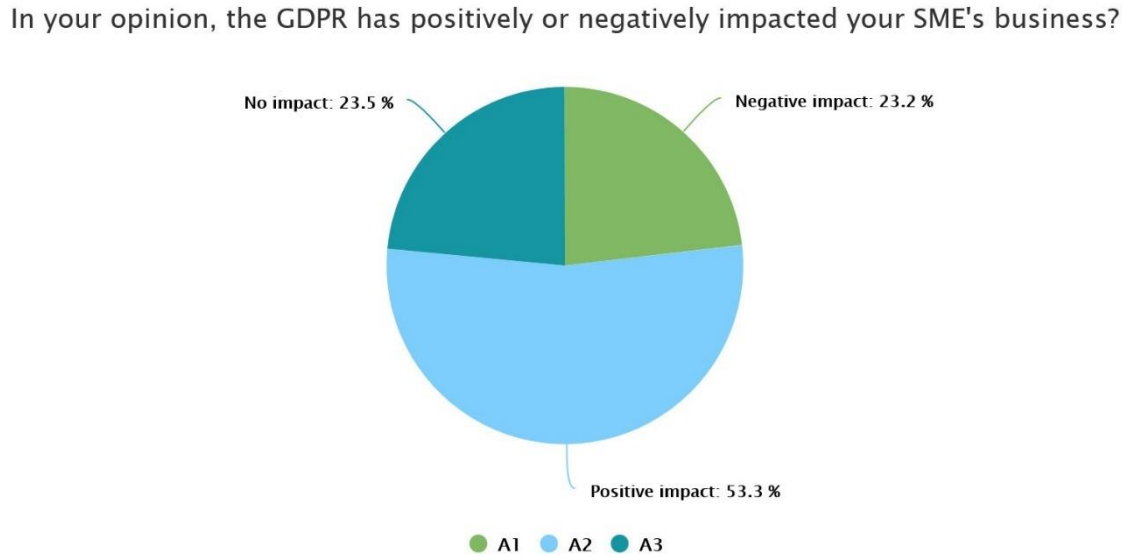
Research organisation Egress published an independent poll(*Egress-Research-Report-Gdpr-Compliance. Pdf*, n.d.) in late 2019. The poll surveyed 250 individuals at the decision-making level in companies impacted by GDPR in the UK. Only 34% (n=85) of the target group of 250 represented SMEs. The findings of the Egress poll correspond with the findings of our survey.

According to Egress,

> "28% of the GDPR decision-makers surveyed said that their biggest area of investment had been in implementing new processes around the handling of sensitive data. This figure rose to 30% in mid-size companies and 32% in large enterprises."

The 30% figure of investment in a large investment in SMEs in Egress supports the 30.8% figure expressed by the respondents in our survey. Our respondents also confirmed in the follow-up queries that the lion's share of investment went to implement new systems for handling sensitive information of data subjects. The questions remain about the maintenance costs of compliance with GDPR over time.

e) Finding 5- GDPR Impact on EU SMEs



This finding is one of the key questions being asked in this thesis. The business impact of GDPR on EU SMEs. While there is a marginal difference between the results of 'no-impact' (23.5%) and 'negative impact' (23.2%), 53.3% of respondents answered that GDPR had a positive impact on EU SMEs. As has been explained earlier, GDPR is in its infancy and literature limitations as regards data are obvious. Business research conducted post-May 2018 enforcement of GDPR provides limited data about the business impact of GDPR on SMEs/EU SMEs.

European Digital SME Alliance(*ABOUT US - European DIGITAL SME Alliance*, n.d.) has an impressive membership of over 45,000 SMEs directly impacted by GDPR as one of the core digital economy stakeholders. The organisations came about with the efforts of 30 national and regional European countries.

In one of their response papers titled, "Europe's Digital Decade:2030" released on March 9, 2021, Digital governance such as GDPR is one of the four key targets. (*Digital_Decade_Targets_2030_DIGITAL_SME_Consultation_Response.Pdf*, n.d.)

The paper also highlights the fact that SMEs form 99% of European businesses and employ two-thirds of total employment in Europe. One of the key findings of the organisations' research states, "Data is a prerequisite for many innovative digital technologies. At the moment, about 90% of Europe's data is stored and processed outside of Europe".(*Digital_Decade_Targets_2030_DIGITAL_SME_Consultation_Response.Pdf*, n.d., p. 3)

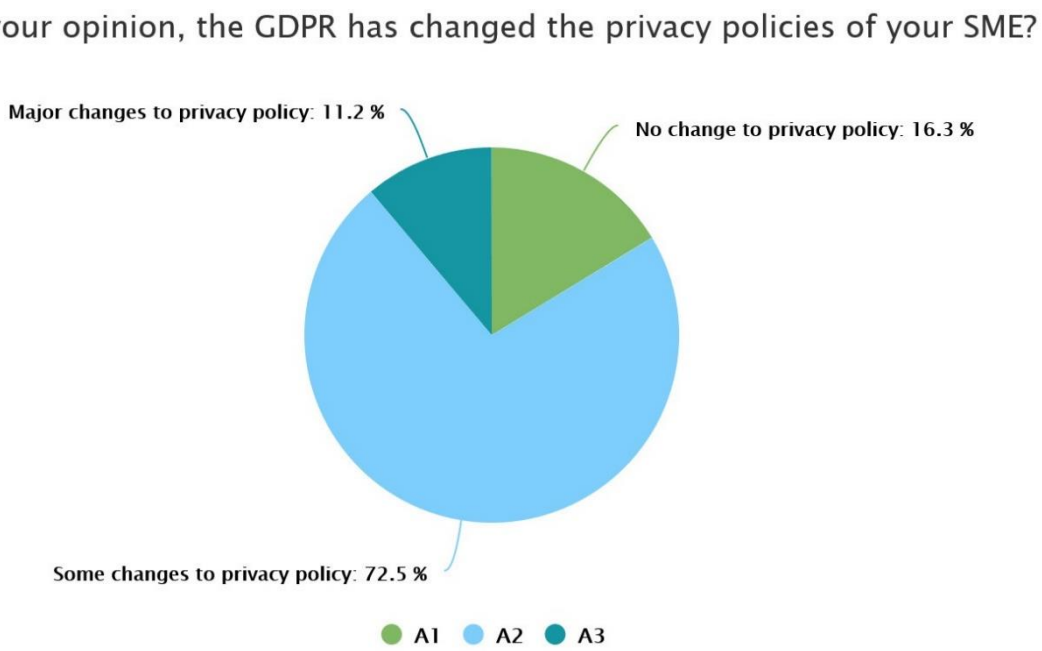
GDPR has allowed regulation of EU residents' data outside EU borders and restrained large global corporations operating outside the EU to comply with EU data protection laws. Kati Suominen in her 2017 research details that of the total US global digital services, 45% are destined for the EU and 46% of the EU's global digital services end up in the USA. (Suominen, 2017)

The concept of data localization ties in with the cost of data protection. While GDPR does not aim to localize the data of EU residents for transnational data trade, it does restrict the movement of EU residents' data under its regime.

European Commission in its proposed framework to promote EU Digital trade in 2017(*EC COM 2017*, n.d.) estimates Euro 415 billion growth in the EU digital economy through a regulatory harmonization of EU's digital markets. GDPR is considered a key component of that projection.

However, it must be noted that research available thus far does not fully reveal the direct or indirect impact of GDPR. Teixeira et al. in their 2019 literature review-based research highlight GDPR benefits to SMEs in terms of better data protection, cost reduction, improved reputation and better management of any potential data breaches.(Teixeira et al., 2019)

f) Finding 6- GDPR Impact on SME's Privacy Policies



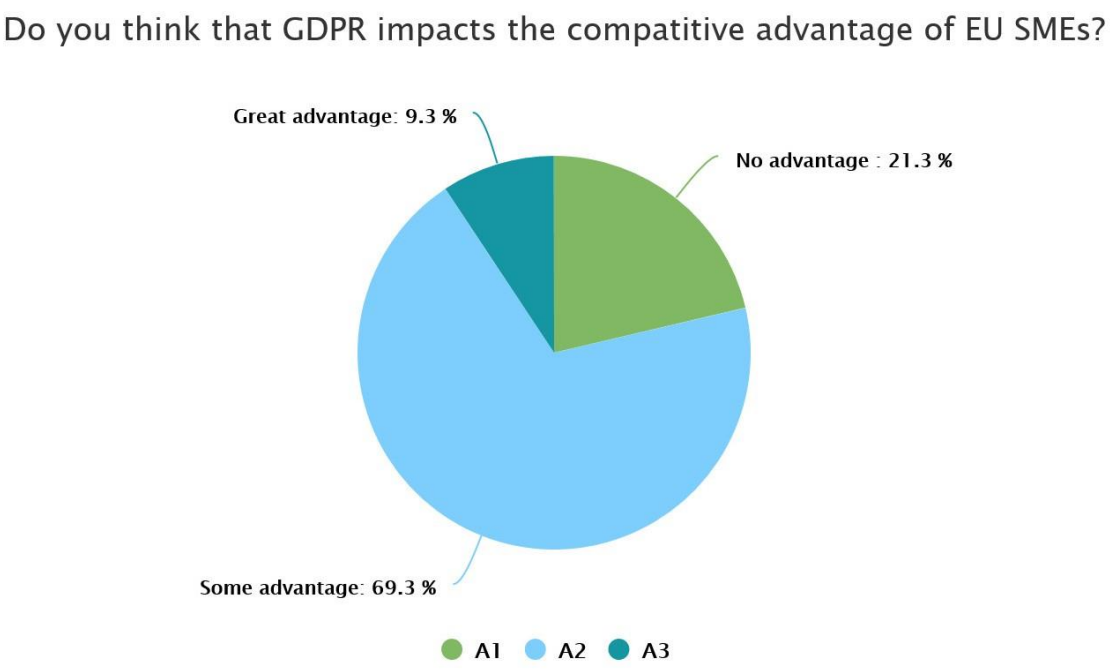
The EU has been working on improving the privacy of its residents since the 1980s. The European Charter of Human Rights (distinct from the European Convention on Human Rights) has a separate article that speaks to data privacy within the EU. GDPR aimed to strengthen and improve personal data protection on a much higher scale. Our survey indicates 72.5% of respondents confirming changes to the data privacy policies within their SMEs triggered by GDPR compliance.

Critics of GDPR consistently refer to the Euro 20 million or 4% of the gross worldwide revenue as the major motivation for this change. While the fear of hefty fines may be a major contributing factor in improving data privacy policies by SMEs, there are other factors also at play. The user's awareness of their data monetization by internet-based service companies, personal data breaches on the internet due to insufficient data protection mechanisms by the data processors and misuse of personal data without the consent of the data subject are some of the other motivations for improving data privacy policies. The data subjects are fully aware of the economic power of their data as well as their rights if there are any data breaches or violations of their privacy rights.

EU's privacy legislation before GDPR such as the 1995 Data Protection Directive (95/46/EC) and 2002 Directive (2002/58/EC) indicate the EU's awareness of the data privacy rights flowing from the European Charter. GDPR simply aimed to further strengthen the privacy rights of EU residents' data as a unified approach that could harmonize data protection throughout the EU. A comprehensive empirical analysis of 6,759 websites from the EU-28 was carried out by Thomas Linden et al. in 2020.(Linden et al., 2020) The study aimed to analyse the impact of GDPR on websites within the EU-28 with a minor analysis of global trends in privacy policies due to GDPR. They concluded that,

> "The results of our tests and analyses suggest that the GDPR has been a catalyst for a major overhaul of the privacy policies inside and outside the EU. This overhaul of the policies, manifesting in extensive textual changes, especially for the EU-based websites, does not necessarily come at a benefit to the users. Policies have become considerably longer (a fifth longer in the Global set and a third longer in the EU set). Our presentation analysis, however, identified a positive trend in user experience, specifically for the EU policies; such a trend was not found for Global policies."(Linden et al., 2020, p. 63)

g) Finding 7- GDPRs Competitive Advantage to EU SMEs



The question of GDPR aiming to provide any competitive advantage to EU SMEs is critical to answering the impact of GDPR on EU SMEs. The respondents to the survey were asked to answer this question with an explanation that the competitive advantage in this question strictly pertains to the business competitiveness within the scope of the digital economy vis-à-vis their competitors globally. The majority of respondents agreed that GDPR increased the competitiveness of the EU SMEs within the global digital economy that relies on EU residents' data within or outside the EU. This view is not shared by researchers from outside the EU who consider GDPR as a restrictive regulation that prevents the free flow of personal data sharing between transnational business entities for monetization.(Gal & Aviv, 2020, p. 351)

Presently there is no quantifiable study of GDPRs' impact on EU SMEs or SMEs in general. The positive impact of GDPR on SMEs was conveyed to the participants of our survey in terms of increase in data security measures, customer confidence in the SMEs' ability to safely store their data, better training of staff in understanding the GDPR as a data security regulation etc. The negative impact was explained as the reduction in business volume, higher costs of GDPR compliance and any fines imposed on the SME due to non-compliance etc.

Jasmontaitė-Zaniewicz et al. argued (Jasmontaitė-Zaniewicz et al., 2021) in their book that provides a simple guideline for SMEs to implement GDPR that the competitive advantage for EU SMEs is linked with the successful implementation and compliance with the regulation. The book came out as part of the "STAR II (Support small and medium enterprises on the Data Protection Reform II) research project, co-funded by the European Union within the scope of the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017), under Grant Agreement No. 814775."[11]

The theme of the argument forwarded by Jasmontaitė-Zaniewicz et al. also suggests that EU SMEs' compliance with the GDPR in itself fosters competitive advantage. The scholars translate the competitive advantage in terms of consumer trust in the SMEs' ability to protect their data and resultantly provide new business opportunities for the SMEs. The key to unleashing this competitive advantage is linked to a sound understanding of the GDPR implementation requirements.

[11] ("Star II Project," n.d.)

7) CHALLENGING THE HYPOTHESIS

a) Background

This chapter is critical to the thesis and its research. Our research findings point to the negative impact of GDPR on EU SMEs. However, the defend the hypothesis emerging from the thesis research, it is fundamental and critical to explore evidence that may defeat the findings and at least examine the counter-evidence. The United States is the biggest player in the global data market and also the global economy. The US and the EU are the largest trade partners within the data economy. These findings have been supported in this thesis in the earlier chapters.

The global economy has been slowing down for the past two years according to the World Bank. (Mason & Shetty, 2019) Mason & Shetty (2019) prepared the report commissioned by the World Bank under its project titled, Global Economic Prospects (GEP). The report provides empirically calibrated predictions about the trends of the global economy going beyond 2019. The report could not see the COVID-19 pandemic coming; however, it did base its empirical findings on global economic data. The January 2019 World Bank report highlights the financial stresses confronting the global economy. Emerging markets and developing economies (EMDEs) are recognised as the main drivers of the global economy in the report.

According to Mason & Shetty (2019), the developed economies of G-7 decelerated to 2.3% by the end of 2018, predicted to slow further to 1.5% in 2019. The EDMEs of Asia are expected to maintain their growth at 6% due to China maintaining a growth rate of 6.2%. The global economic growth, in turn, would see a downturn from 3% in 2018 to 2.8% in the 2019-20 period. Mason and Shetty (2019) attribute the increasing national trade and business protectionist policies as the biggest contributor to the global economic slowdown. (Mason & Shetty, 2019, p. 6) Within the preview of this background, this chapter of the thesis explores GDPR, its impact on the digital economy, and EU SMEs from the perspective of the EU's largest data trade partner the US.

b) GDPR & SMEs- The American Perspective

Matthew Heiman is a distinguished American legal scholar who specialises in cyber laws. Heiman is the Director of Planning at the National Security Institute at George Mason University's Antonin Scalia Law School. He is the Chairman of the Cyber & Privacy Working Group of the Regulatory Transparency Project. Heiman wrote a scathing criticism of GDPR in his 2019 paper titled, "The GDPR and the Consequences of Big Regulation."(Heiman, 2019) Heiman is not the lone voice from across the Atlantic criticising GDPR for its overreach and potentially detrimental impact on the growth of the ICTs including the ability of the American/EU SMEs to cope with the GDPR compliance.

Heiman strongly objects to the international reach or the 'extraterritorial' reach of GDPR.(Heiman, 2019, p. 949) Heiman's strongest criticism of GDPR is the imposed cost of compliance with GDPR on the SMEs. Heiman does not discriminate between the US and EU SMEs, rather, he argues that GDPR favours large data corporations like

Google, Facebook etc. due to their financial ability to absorb the high costs of GDPR compliance.

Highlighting the adverse impact of GDPR compliance on SMEs, Heiman argues,

> "Like many regulations, the GDPR's complexity and burdens will be most easily borne by the largest actors in the marketplace such as Google, Facebook, and Amazon. These organizations have the resources, lawyers, and compliance experts necessary to ensure compliance. Smaller organizations will struggle to meet the GDPR's requirements. A recent survey showed that a company will spend $1 million to acquire the technology necessary to comply.26 This is peanuts for a large organization, but it is a huge burden for small companies doing business in the EU. For those that cannot afford compliance, they will have to accept the risk of being caught or choose not to serve those in the EU."(Heiman, 2019, p. 950)

Roslyn Layton, while testifying before the United States Senate Judiciary Committee formed to examine GDPR in March 2019, highlighted "10-Problems of GDPR".(Layton, n.d.) The US Senate Judiciary Committee decided to title the final report the "10 Problems of GDPR".

Layton highlighted GDPRs ten problems:

> "1. The GDPR strengthens the largest players.
> 2. **The GDPR weakens small- and medium-sized firms.**
> 3. **The GDPR is cost-prohibitive for many firms.**
> 4. The GDPR silences free speech and expression.
> 5. The GDPR threatens innovation and research.
> 6. The GDPR increases cybersecurity risk.
> 7. The GDPR and the CCPA create risks for identity theft and online fraud.
> 8. The GDPR has not created greater trust online.
> 9. The GDPR and the CCPA use the pretence of customer control to increase the power of government.
> 10. The GDPR and the CCPA fail to meaningfully incorporate the role of privacy-enhancing innovation and consumer education in data protection."(Layton, n.d., p. 2)

The second and third problems highlighted in Layton's expert testimony before the US Senate concerning GDPR resonates with Heiman's assertions about the adverse competitive impact on SMEs and the steep compliance costs of GDPR on the SMEs compared to the mega-corporations like Google, Facebook etc.

In his final analysis, Heiman observes the potential 'protectionist' nature of GDPR. Heiman asserts, "Some have not unreasonably suggested that the GDPR is less about upholding cherished European ideals of privacy than it is a protectionist economic tool."(Heiman, 2019, p. 953) Heiman refers to the 'protectionist' nature of GDPR within the context of the EU promoting cloud services within the EU against the perceived supremacy of US companies as global leaders in the data economy.

Layton does not directly call GDPR a 'protectionist' regulation. Rather, Layton sees GDPR as Brussels's attempt to legitimize the EU Project in the face of rising

nationalism and EU scepticism within the EU leading to the BREXIT in 2020. (Layton, n.d., p. 9)

c) GDPR Compliance & EU SMEs

It is important to examine literature that either supports or questions the assertions of Heiman and Layton as regards (1) GDPR favouring mega-corporations like Google and Facebook etc. while imposing a financial burden on the SMEs and (2) GDPR is the EU's attempt to protect EU-27s digital competitiveness through protectionist policies and defeat EU scepticism rather than about privacy protection of EU residents' personal data usage.

European Digital SME Alliance ("**SME Alliance**")(*ABOUT US - European DIGITAL SME Alliance*, n.d.) published a position paper offering a two-year post-GDPR enforcement impact on EU SMEs in June 2020. (*Position-Paper-GDPR-Review-2020.Pdf*, n.d.) The SME Alliance is an important body as it specifically represents European/EU SMEs in the digital sector. While various surveys conducted by various research and business organisations are important to gather reliable data on the impact of GDPR on EU SMEs, it is important to pay particular attention to the collective voice of the European/EU SMEs when it comes to the applied impact of GDPR on their business.

SME Alliance terms GDPR as by far the 'most ambitious' data protection legislation globally with the potential to impact global data protection law-making. This statement resonates with the findings of this research throughout the thesis. The alliance acknowledges the aim of GDPR to empower the data subjects in terms of their data and to harmonise data protection across the 'European legal space'. However, the alliance does not agree with the 'one-size-fits-all' approach of GDPR and its failure to modify the behaviour of big tech companies concerning 'exploitation of personal data as their business model".(*Position-Paper-GDPR-Review-2020.Pdf*, n.d., p. 1)

The SME alliance shows concern about the ambiguities within GDPR that especially hinder the ability of SMEs to innovate while complying with GDPR within the EU and internationally. The SME alliance proposed three areas of emphasis for EU lawmakers concerning GDPRs' ability to support EU SMEs:

"1.) Increasing legal certainty for SMEs and working towards incentives for privacy-based innovation.
2.) Application of the GDPR must be uniform across Europe and needs strong European-minded DPAs and European oversight.
3.) Making sure the GDPR does not hinder innovation."(*Position-Paper-GDPR-Review-2020.Pdf*, n.d., p. 1)

d) EU SMEs' Experience of GDPR

The EU funded business research titled, STAR II (**S**uppor**t** Mall **A**nd Medium Enterprise on the Data Protection **R**eform) under the European Commission's Directorate for Justice and Consumers. The purpose of the project was to support the 22 million EU SMEs in resolving the peculiar implementation challenges of GDPR. ("Star II Project," n.d.) The project published a report at the end of the first year post-GDPR implementation in July 2019. (Barnard-Wills et al., 2019)

The STAR II report provides some insight into the various aspects of legal, technical and financial challenges faced by the EU SMEs in the implementation and compliance with GDPR. The STAR II project did not seek any data on the business competitiveness of the EU SMEs in terms of their mandatory compliance requirements with the GDPR.

Chapter 7, section 7.2(Barnard-Wills et al., 2019, p. 3) of the STAR II report highlighted the following challenges faced by EU SMEs in implementing GDPR:

- "It is difficult to understand exactly what changes are required to be made to the privacy policies/systems/business to comply with GDPR.

- No clarity or guideline on how to develop and no description of what procedures are to be adopted to implement the changes.

- Difficulty in sourcing appropriate funding and support in staff training on GDPR compliance."(Barnard-Wills et al., 2019, p. 34)

The three challenges described in the EU-funded STAR-II report also echo the findings of this thesis as well as the criticism of GDPR by the two leading papers from the US mentioned earlier in this chapter. The EU Data SMEs Alliance also highlighted these challenges in their position paper discussed earlier in this chapter. The report also touched upon the concerns of the EU SME Alliance and stated the following concerns:

- "Concern that EC stakeholder groups on data protection tend to be dominated by representatives of a larger industry, to the exclusion of SME representatives.

- Concern about the consistency of implementation of the GDPR across the Member States."(Barnard-Wills et al., 2019, p. 35)

8) GDPR, COVID-19 & EU SMEs

a) Background

The first case of nCov-2019 was reported in Wuhan China on 21 December 2019. At the time of the writing of this paper, over 412 million cases have been reported worldwide with 5.2 million fatalities and over a billion doses of Covid-19 vaccines administered. (*WHO Coronavirus (COVID-19) Dashboard*, n.d.) That means roughly 5% of the world's population got infected with Covid-19 and of the 5% infected 1.21% of those infected died from the virus. The coronavirus pandemic resulted in global vaccine-mandated restrictions imposed through emergency measures by the governments. These measures have resulted in major disruptions in the global economy including severe supply chain challenges for consumer products and services. The world is now transitioning to relaxation of some of the restrictions after entering the third year of this pandemic.

The social, political, and economic order of the world as we knew it before nCov-2019 has changed dramatically. The most pressing need of the hour for any government became the protection of their population from the existing and potential threats of the virus. Governments all over the world have tried to respond to this unprecedented situation using varying degrees of emergency legal powers that would allow them to curb civil liberties to impose restrictions on free movement. These restrictions came on the heels of various guidelines by medical experts to limit the spread of the virus amongst the population.

The use of legislated emergency powers by the governments of constitutional democracies allowed for bypassing the legislative and judicial oversights for the use of any resulting orders or measures. Some of the measures included lockdowns, curfews, shutting down of businesses and in most cases cancellation of surgeries that were not considered more urgent than managing the virus. (Zhong et al., 2020)

Zhong et al. (2020) and other scholars have argued that the use of emergency powers by the executive branch of the government is necessary, yet they may have serious consequences for the global economy especially the SMEs in the present and future. One of the key challenges for EU SMEs has been to comply with GDPR while responding to the drastic transition of EU economies to digitised socio-economic space during the pandemic. Online services have taken over the traditional access of services by almost the entire global population. This chapter explores the impact of COVID-19 and GDPR compliance challenges for the EU SMEs during this time.

b) SMEs Challenges & Covid-19

Covid-19 has severely hit SMEs globally. G-20 and G-7 countries have recognised the need to quantify the economic and business damage to their SME sector with varying degrees of relief measures that include financial assistance for short and medium terms. The uncertainty imposed by COVID-19 restriction mandates suggests that any SMEs failing to recover from the COVID-19 imposed restrictions are likely to fold for good. McKinsey Group conducted Covid-19 impact research on 2200 SMEs in five EU countries in August 2020 (before the final exit of the UK in December 2020).

(*COVID-19 and European Small Businesses | McKinsey*, n.d.) McKinsey's research is by far the most comprehensive and authoritative research on the topic of COVID-19's impact on EU SMEs within the major EU economies.

McKinsey's research findings conclude that:(Dimson et al., 2020)

- 70% (1540 out of 2200) stated the severe financial impact of Covid-19 with a major revenue decline.
- 20% (440 out of 2200) stated default on their loan liabilities and laying off of their employees.
- 28% (616 out of 2200) stated that all growth projects had been cancelled due to the Covid-19 impact.
- 50% (1100 out of 2200) stated that they will not survive for another 12 months (by the end of the year 2022).

It is a grim and distressing picture for the 22 million EU SMEs that employ over 90% of the EU's workforce. It must also be noted that 2200 EU SMEs surveyed by McKinsey also received a varying degree of financial assistance from their respective governments including tax incentives. The domino effect of 20% of EU SMEs folding for good would also mean 20% of the EU SME workforce (aggregate) would be unemployed and place a further economic burden on the economy for benefits etc.

c) Covid-19, Scientific Data & GDPR

One of the biggest tools being advocated by governments all over the world to track the spread of COVID-19 is through personal phone data collection of natural persons. This mode of collecting data for scientific research involves ICT companies, SMEs providing various elements of the web service, scientific community sharing and analysing the data and the various government agencies accessing and processing the data. This huge chain of organisations accessing, storing, and processing natural person's sensitive medical and personal data was never envisaged by the lawgivers of GDPR. SMEs are an integral part of this data collection, storage, processing, and access. While GDPR allows protection to government agencies for breaches of GDPR compliance, SMEs are still expected to fully comply with the GDPR during this process.

In a chapter titled Covid-19 pandemic and GDPR(Hallinan et al., 2022, pp. 157–186), Dr Ludovica Pasari, an Italian scholar has explored the unique challenges of data protection for mass scientific data collected during the Covid-19 pandemic. Pasari argues that GDPR Article 89 provides for the 'determination' of scientific research for public deliberations to facilitate political decisions such as COVID-19 restriction mandates etc.(Hallinan et al., 2022, p. 157) The research points to the challenges faced by the scientific community to reconcile the data protection and privacy rights of the data subject and the larger public interest to protect the public during this pandemic. The research concludes that public safety outweighs any concerns for data privacy.

The EDPS (European Data Protection Supervisor) has also highlighted the unique challenges of data protection and privacy in the wake of COVID-19. EDPS recognised the public concerns and ensuing political debate on COVID-19 contact tracing apps and data localisation restrictions imposed through GDPR (Article 45 for localisation and

Article 49 for derogation allowed by the data subject), particularly on the businesses involved in the contact tracing apps within and outside EU.

In response to the French Senate's question on the implication of GDPR on the COVID-19 contact tracing app, the EDPS responded as follows:

"As contact tracing applications are currently being considered in the individual Member States, their deployment is primarily governed by the General Data Protection Regulation (GDPR) and the ePrivacy Directive and its implementing national legislation…… Though GDPR exists in the form of Regulation which is therefore directly applicable, binding and effective in all Member States it has to be complemented by national law (e.g., procedures)"(*EDPS Answers to French Senate*, n.d.)

The response from EDPS regarding GDPR compliance in the wake of COVID-19 tracing apps is a major legal deviation from the basic definitional difference between an EU Regulation (GDPR) and an EU Directive (ePrivacy). EU Regulations such as GDPR supersede any EU-27-member state national legislation on the subject and do not require any national legislation for its enactment. EU Regulations are directly transported into the EU-27 member states statutory law without any changes to its text or enforcement.

d) Covid-19- Game Changer for Tech Giants

We have highlighted the negative impact of Covid-19 on EU SMEs during the pandemic. The results highlighted that 70% of the EU SMEs are in detrimental financial loss during the ongoing pandemic in its third year. 50% of EU SMEs may not survive 2022 if the Covid-19 restrictions continue to hamper their business.

On the other end of the spectrum, some of the biggest business beneficiaries of the digitised global data services and initiatives such as remote productivity (work-from-home orders etc.) during COVID-19 are global tech giants like Google, Amazon, Microsoft, Apple etc. Other large technology service providers like CISCO, IBM Cloud services, and hardware companies like HP, IBM Lenovo etc. also gained tremendously. While the stock markets tumbled all over the world due to COVID-19 restrictions, wiping out trillions of dollars in stock losses, tech giants like Google, Amazon, Microsoft, and Apple made huge gains in their stock prices. (*International Funds Focused on Tech Giants Excel; Should You Invest in Global MFs?*, n.d.)

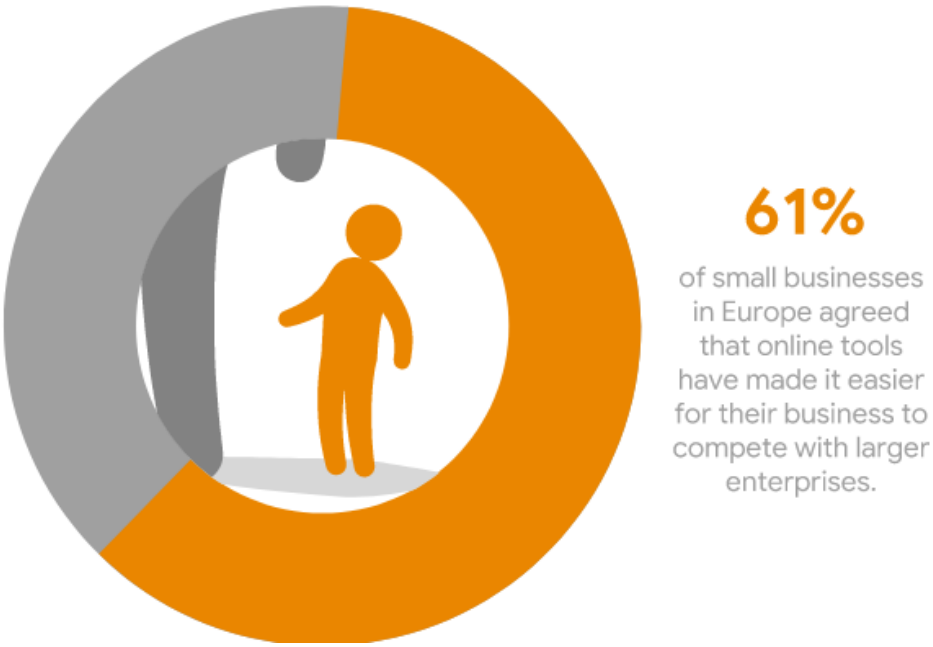
The tech giants are heavily invested through international equity funds (MFs/ETFs). The funds delivered 36.4% returns over the past year and gains of around 13.8 per cent in 2020. It is the second-best performer among international funds in the one-year timeframe during the last 20 years. (*International Funds Focused on Tech Giants Excel; Should You Invest in Global MFs?*, n.d.)

Google and Apple have been technology adversaries since the time of their inception. In an unprecedented move, Google and Apple came together to develop a joint application (App) that would be a decentralised nCov-2019 tracing tool (App). The App would allow users to track those potentially infected with nCov-2019. The announcement was made by both companies in April 2020. Apple's proprietary

software (IOS) and Google's universal Android platform are the two leading operating systems for global mobile phone and computing users. The combined effort-App would allow Apple and Android users to use the same App across multiple hardware and software platforms and have access to over 3.5 billion technology app users around the world. (*Apple and Google Partner on COVID-19 Contact Tracing Technology*, n.d.)

Both Google and Apple are amongst the largest repositories of global personal data. Governments around the world rely on their data for various purposes that include matters of public safety and security. Google has a 90% market share of the global search engine market and processes 63,000 search requests per second. The global search engine market value of Google is USD 739 trillion. Google's parent company Alphabet owns over 200 tech companies that allow the Google platform to service its 2 billion clients globally. (Aleksandra, 2018)

Such a massive repository of personal data collection and recording of search data history allows Google to profile, predict the behaviour and create customized content for its over 3 billion users globally utilising its advanced Artificial Intelligence (AI) algorithms. Google carries out its economic impact on various regions and businesses. According to Google, its impact on EU SMEs is quantified in terms of their ability to compete with larger businesses. (*Europe – Google Impact Report*, n.d.)



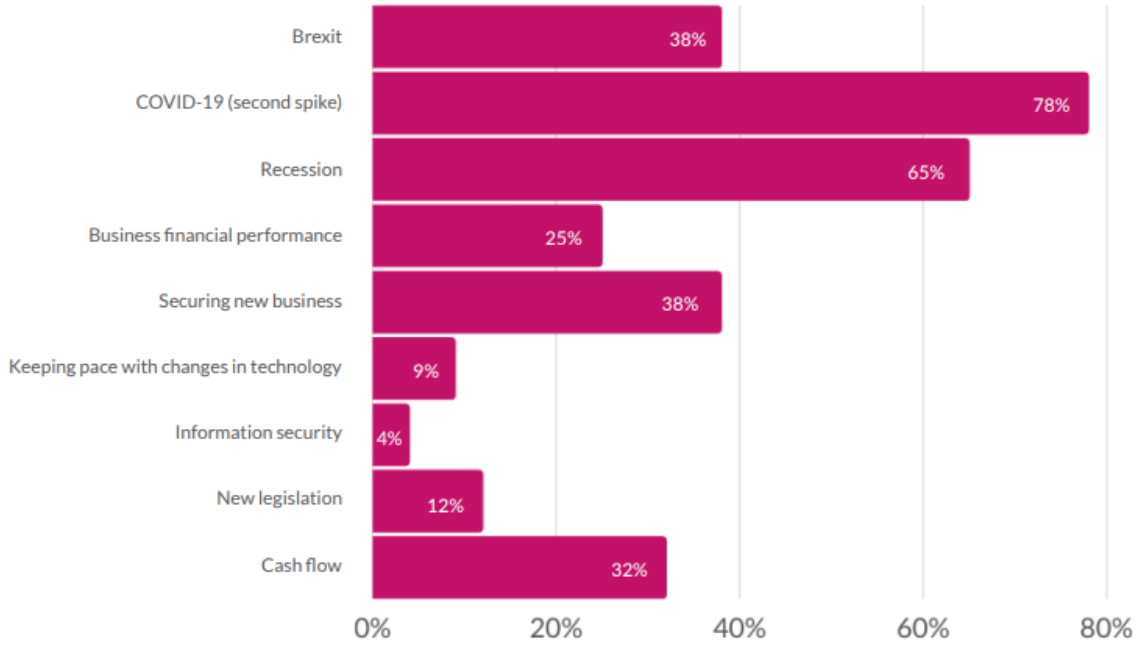
Source: https://googleimpactreport.publicfirst.co.uk/europe/

e) EU SMEs & COVID-19

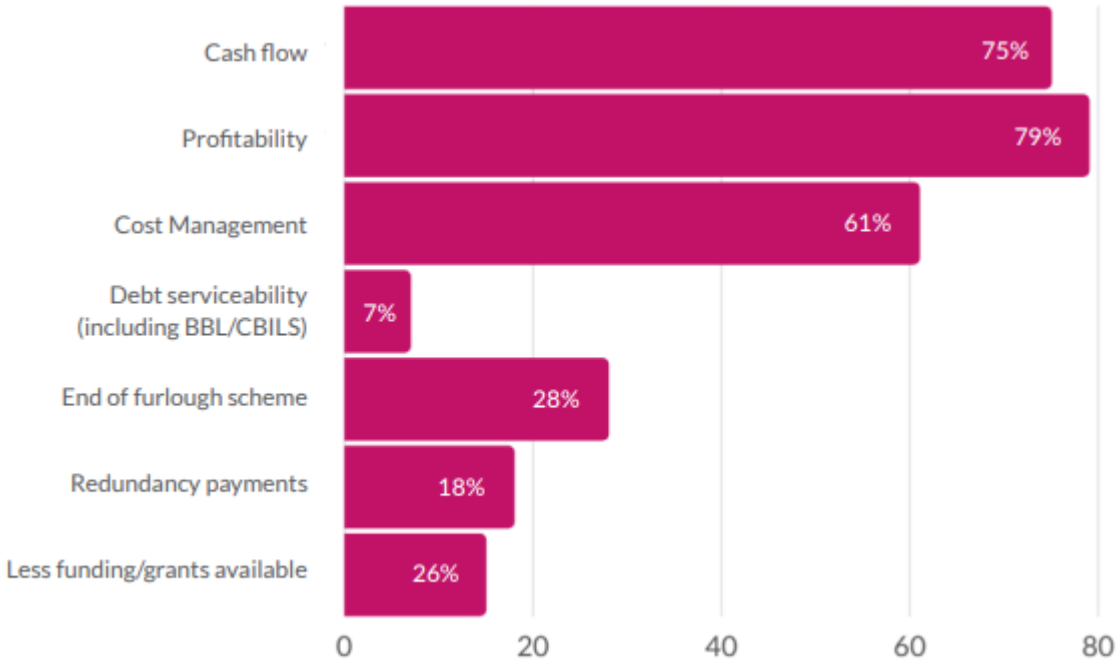
The discussion above highlighted the impact of COVID-19 on the EU SMEs, notwithstanding the limitations imposed by the compliance with GDPR. Covid-19 has highlighted the winners and losers in the digitized economy during Covid-19. While 22 million EU SMEs form the backbone of its economy, GDPR created further challenges for those EU SMEs during Covid-19. The explosion in the use of ICTs during COVID-19, such as enhanced reliance on daily functions of life like working from home, online

grocery shopping, access to medical services, food services etc. did not bring any advantages for the EU SMEs. Rather 50% of the 22 million SMEs risk closing their doors permanently if the COVID-19 restrictions persist in the third year as well.

A UK-based research institution www.hrsolutions-uk.com conducted a survey in October 2020 with SME leaders across the EU in partnership with Deloitte. (*HRSolutions-SME-Challenges-Post-Covid19-Results.Pdf*, n.d.) The purpose of the survey was to examine EU SME challenges, including the challenges of GDPR post-Covid-19. In response to the key question of the 3-biggest challenges facing EU SMEs post-COVID-19, GDPR came up among the top challenges under the heading of new legislation.



The profitability question also confirmed the findings of McKinsey quoted earlier, which showed 70% of the EU SMEs saw their profits dwindle during Covid-19 against 78% stated in the HRSolutions-Deloitte survey. The findings confirm that Covid-19 has stunted the growth of EU SMEs during Covid-19.



The findings by the HR Solution-Deloitte survey and McKinsey survey suggest that the 22 million EU SMEs face existential challenges during Covid-19. Compliance with GDPR remains a major challenge for EU SMEs due to a variety of reasons that include ambiguity in the language of the legislation, cost of compliance and inability of the EU to provide sufficient budgetary support for GDPR compliance to EU SMEs etc.

Big Data corporations like Google, Microsoft, Amazon, Facebook etc. have not only expanded their market share during COVID-19, but their stock performance and profits are the best seen during COVID-19 and compared with the figures of the last 10 years or so. The EU's GDPR compliance failures and resulting penalties on the tech giants seem to unfazed them due to their deep financial pockets and ability to prolong judicial proceedings without any cause for financial costs.

9) GDPR & EU SME BUSINESS CHALLENGES

a) Introduction

The European Union (EU) General Data Protection Regulation (GDPR) came into force in May 2018. The scope of GDPR is regulating the data protection of EU residents as a homogenous body of EU law. However, it targets and regulates EU business entities in particular and any business accessing EU resident personal data globally in general. Thus, the scope of GDPR is legal yet the application of the law is business in nature.

EU law is supranational, meaning that it has supremacy over the domestic law of the 27-member bloc. The EU Court of Justice (CJEU) Luxembourg established the truism of the supremacy of EU Law over the member states in the seminal case of Costa v ENEL. The GDPR not only has supranational reach, but its scope defines international reach within the reading of Article 8 Data Protection Rights afforded to all EU citizens under the European Charter of Fundamental Rights (CFREU).

GDPR aims to harmonize the data protection regulations for businesses that collect, store, access and process the personal data of EU residents. GDPR does not provide any such protection to an incorporated legal person, a corporation. The enforcement of GDPR is mandatory for all businesses in the EU without exception. GDPR relies on heavy fines as a deterrent to ensure compliance. We will be examining the transformative nature of the GDPR in light of our findings in the previous chapter. The analysis is based on literature that has emerged after May 2018 to ensure that the discussion provides a contextual view of post-enforcement.

b) GDPR- Business Limitations

The business world has specific rules of operation. These rules are deeply entrenched and flow from the corpus of municipal and international laws. The transformation of the global economy due to the explosive intercourse of technology with any and every sphere of life poses unique challenges for those making laws for the socio-economic spheres of human societies. Personal data has become the most valuable commodity within the global economy. With the advancements in AI technology, blockchain and integration of social media in the global data economy, personal data presents infinite uses and dimensions for businesses.

The '*Purpose Limitation*' is recognized as the guiding principle for formulating most of the existing international business law for data protection. In simple words, the businesses collecting, storing, and accessing a person's data must be for legitimate and specific purposes guided by the laws on data protection.

The European Union ("EU") is the result of the socio-political and socio-economic transformation of the European continent post-Second World War. The 'European Identity' is woven into the fabric that forms the basis of the EU and its socio-economic interests guiding the EU laws such as GDPR.

The General Data Protection Law[12] ("GDPR") of the EU came into force on 25th May 2018. Our research findings in the previous chapter have led to the conclusion that GDPR is transformative for not only the EU data economy/economy but also for the global data economy that relies on EU data. The research findings also point to the conclusion that GDPR will not only transform the business landscape of the EU but will have a profound impact internationally. 99% of the EU businesses are SMEs, a fact that we have already established in our discussion above.

Globalization gained momentum during the 1980s and it slowly started to dissipate in the late 1990s. The last two decades of the global economy are made up of regional and national business and economic activities that play out on the global business stage. President Donald Trump's rhetoric of '*America First'*.

The United States and the EU are the largest data economy, partners. Both the US and the EU have been trying to reconcile various legal challenges to facilitate the data business between the two. In 2016, the EU and the US reached an agreement to share the personal data of EU residents for commercial purposes.[13] The travel industry between the US and the EU is one of the main revenues generating businesses that utilize the personal data of EU residents as well as provide business opportunities to EU SMEs downstream. Post 9/11, the US Transportation Security Agency ("TSA") requires pre-boarding personal data of all travellers from the EU including the rest of the world for security purposes. The data is collected under the US Homeland Security Act[14].

The EU Data Security Supervisors[15] have raised concerns about the secure storage of EU resident data required by the TSA. The Court of Justice of the European Union ("CJEU"), Luxembourg[16] following the European Court of Human Rights ("ECtHR"), Strasbourg have started critically examining 'Big data'[17] potential

[12] Regulation (EU) 2016/679 on data protection. Source: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[13] 'The European Commission and the U.S. Department of Commerce reached on 2 February 2016 a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (IP/16/216). This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses.' Source: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

[14] US Home Land Security Act 2002. Source: https://www.dhs.gov/homeland-security-act-2002

[15] "As of 25 May 2018, the Article 29 Working Party will be replaced by the European Data Protection Board (EDPB). The EDPB has the status of an EU body with legal personality and is provided with an independent secretariat.". Source: https://edpb.europa.eu/

[16] Case Law Data Protection CJEU. Source: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf

[17] Case Law Data Protection ECtHR. Source: https://www.coe.int/en/web/data-protection/echr-case-law

violations of EU residents' data by technology giants such as Google[18] and Microsoft[19] since the implementation of the GDPR. Millions of Euros have been imposed fines on these tech giants due to GDPR violations since May 2018.

Jan Philipp Albrecht is an EU lawmaker and vice-chair of the civil liberties, home affairs and justice committee of the EU Parliament. In 2016, Albrecht wrote a paper titled, "How GDPR will change the world".(Albrecht, 2016) According to Albrecht, "From 24 May 2018, the fragmented digital market of today and the lack of enforcement in the field of data protection provisions will end."(Albrecht, 2016, p. 287) Albrecht, who is also an international law expert further explained the global implications of GDPR on the global data economy. His main argument rests on the fact that global businesses will now be working with a single set of data privacy laws for the EU, rather than 28 different laws governing data business (the article was written before the UK's exit from the EU-28). Albrecht has a strong argument in the sense that businesses globally seek certainty for rules that can potentially result in hefty financial losses or even loss of business. GDPR has brought legal certainty and coherence to the complex world of data collection, processing, access and storage.

c) GDPR – Personal Data Rights & Business Interests

Dr Isabelle Landreau is a Parisian legal scholar who has extensive experience in technology and intellectual property rights. Dr Landreau's 2019 paper titled. In "**The Legal Basis for a Data Economy Based on Trust**"(Landreau, 2019) she argues that while GDPR has the twofold objective of reaffirming the fundamental principle of free movement of data (within the EU), data portability must not be confused with the transfer. In simple words, portability refers to the retention of data by the operator for processing purposes at all times.(Landreau, 2019, p. 63) Dr Landreau highlights a unique point by stating in the case of GDPR, "In front of each (data) *right* conferred on natural persons, there is an *obligation* for the (business) organisations (using the personal data)."(Landreau, 2019, p. 61) Dr Landreau proposes that within the personal data economy (PDE), the data subjects may be financial beneficiaries of any potential monetization of their data. According to Dr Landreau, GDPR presents a unique opportunity to create a data economy in which the natural data subjects can, "sell, rent, transfer or even pledge" the monetized value of their data.(Landreau, 2019, p. 75)

The Big-Four or GAFA (Google, Apple, Facebook, Amazon) model of monetizing a natural person's data as a business model is categorized by Dr Landreau as, "the 'sleeping' provider of data with enormous potential."(Landreau, 2019, p. 75) GDPR has certainly raised the bar for natural person's data rights privacy rights and created limitations and boundaries about its usage by businesses and other entities within the EU and the global data economy.

Personal data privacy under GDPR concerns the intrinsic core concept of protecting the 'personal *identity*' of the data subject. In short, 'personal *identity*'

[18] Google v Spain (Right to be Forgotten). Decided 13 May 2014. Case No. number C-131/1. Held:' that an Internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties, upholding a right of erasure'.

[19] Source: https://blogs.bing.com/search/august-2016/bing-to-use-location-for-rtbf

protection is the underlying *aim* behind the concept of '*personal*' data protection under GDPR amongst other matters. The argument for 'personal *identity*' privacy is contingent on Michel Foucault's revolutionary ideas about the non-fixated notion of identity that concerns a *legal* person. Identity in Foucault's view is '*contingent, provisional, achieved not given'*[20].

In literature, not only is personal '*identity*' a difficult concept to be formally defined, but even the '*individual*' is a complex definition to reconcile. In the milieu of defining personal '*identity*' and '*individual*' as a person, the resultant argument is further complicated by the diachronic[21] nature of an individual's identity within the *community*. The *diachronic* identity means that the individual's identity is *established* through continuously '*emerging*' or '*reappearing*' in various events within the community. Thus, diachronic identification is not concerned with establishing '*separate identities*' between individuals in society, rather it concerns the same individual's identity concerning different events. This argument is based on the correlation between '*identity and person'* linked to *events* that take place within a community.

The significant factor considered by GDPR in the case of identity is the '*object*' to identify the natural *person*. Identity, therefore, can be a difficult concept in the absence of its *object*, the person. Also, the person's identity may be recognized through the surrounding community or community events as a frame of reference for the person's identity. What has emerged from our discussion is the establishment of a theoretical framework for how significant the 'identity' is once it is linked to the events within a community. The person's identity, therefore, remains critical to identify that person as long as the community exists.

The idea of '*identity management'* is by corollary intrinsically linked with the concepts of '*community management'*. The management of this '*contingent*' and '*achieved identity*' gives rise to questioning the purpose of '*identity management'*. It seems that the '*management*' of identity is a label and not the purpose. We assert this as the use of the word '*management*' in the context of '*personal identity'* or '*personal data'* lends it a meaning for '*securing*' the identity. One can argue that identity management is, therefore, an advertisement to create the notion of 'security' for the 'data subjects. The actual 'security' of the data would be an altogether different mechanism that has been labelled as a '*system*' for identity management. So, we are not sure what exactly is the settled meaning of personal identity and personal data. It is for this reason that socioeconomic studies refer to the legal domain for these definitions through Statutes and Case Law.

The GDPR Article 4(1) defines 'personal data' within the limitation of four intrinsic interconnected elements. It states that personal data is 'Any *information* relating to an *identified* or *identifiable* natural *person*'. Interestingly the four elements that constitute 'personal data' within the definition of GDPR speak to our earlier discussion on the identity connected to the resurfacing and emerging of a person in

[20] Karl De Leeuw and Jan Bergstra (2007). The History of Information Security A Comprehensive Handbook.

[21] Ibid 18

various events. The personal identity is then always in a perpetual state of *development* and is not a *static* idea. The sciences of data management, therefore, convey the idea that perhaps once 'identity' becomes data, there exists a system that can secure that data through a process of 'management', thereby giving the data subject a secure identity. The GDPR has paved for securing the '*identity*' through the personal data of natural persons within the EU and beyond in a transformational way.

d) GDPR Impact on ICTs

The GDPR has come into force recently since May 2018. It is far too early to critically examine if it has any tangible impact on the SMEs of the EU or its economically transformative nature. What is clear is the thoughts of the EU leadership[22] concerning the economic significance of the personal data of its citizens. The emphasis on the element of 'trust' in the development of the ICT-based use of personal data of the EU citizens started to echo more clearly. Large corporations view any data protection legislation as a stumbling block to the development of new ICTs.

Therefore, mega-corporations have not accepted the argument of individual data protection rights as a relevant consideration by the EU leadership. Balance was rather titled towards assigning top priority to a more robust legal framework for data protection in its use for economic benefits. It must be remembered that such reflective thought on the part of the EU lawmakers follows in the footsteps of Edward Snowden's revelations of covert mass data retention and access by US and UK intelligence agencies. It seems that the EU lawmakers did not discard the economic '*espionage*' element of the same data retained by the intelligence community.

UK remained and remains an opponent of the GDPR since the landmark decisions of Watson[23], Digital Rights Ireland[24] and Schrems[25] by the Court of Justice declaring mass data retention and access to be unlawful. A UK-based economic survey[26] of 504 businesses of all sizes published its finding that over 80% of the surveyed businesses could neither quantify the compliance cost of GDPR nor could they quantify their existing cost of any data protection measures. The survey was the result of the UK's Information Commissioner's office.

The economic relevance of the GDPR ***within*** the EU flows from Article 217 TFEU (Treaty for the Functioning of the European Union) which requires all Member States of the EU to abide by the law that states, "The Union may conclude with one or more third countries or international organisations agreements establishing an

[22] EU Vice-President Viviane Reding (2014). Source: http://europa.eu/rapid/press-release_SPEECH-14-62_de.htm

[23] CJEU: Watson & Other Joined Cases C-203/15 and C-698/15

[24] CJEU: Digital Rights Ireland C-293/12

[25] CJEU: Schrems C-362/14

[26] "Analysis of the potential impact of GDPR. Implications of the ICO's Draft Guidelines on consent". Source: https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

association involving reciprocal rights and obligations, common action and special procedure."

The European Economic Association (EEA)[27] through its European Free Trade Association (EFTA) Agreements formed the single largest economic market in the world. Under Article 7(a) of the EEA, all member states are obligated to adopt GDPR nationally. Article 288 TFEU makes GDPR *applicable* to all EU Member States in all matters including the economy. Article 288 TFEU refers to the *binding* nature of the EU's secondary source of law, that is the EU Regulations, of which GDPR is one such Regulation. Article 288 (2) makes GDPR binding on all, '*A **regulation** shall have general application. It shall be binding in its entirety and directly applicable in all Member States*.'

The EEA under its articles 102(1) through 102(6) prescribes ***five stages*** in compliance with EC Regulation No.2894/94 concerning enforcement of EU secondary law such as GDPR across the Member States signatory to the EEA. So far, Stage 1 has decided that GDPR is EEA-relevant. The subsequent phases involve participation by the representatives of the EEA Member States to provide consultative advice to the EU Commission that would then through the EU legislative process make the final proposal to the EU Parliament for necessary adjustments if required in the GDPR. It must be noted that GDPR has been fully adopted and enforced since May 2018. The purpose of this EU Legislative process concerning Europe's Economic Association (EEA) is to ensure that the process would result in the most transparent and predictable application of GDPR within the EEA.

This process will also ensure the continued stability and working of the European Economic and Information Markets. Our analysis of GDPR as a supranational law business law concludes that GDPR has a huge impact *within* the European markets through its adoption by the European Economic Association (EEA) under Articles 217 and 288 of TFEU will result in the transformation of the European economic landscape.

The last part of our analysis of the economic transformative nature of GDPR concerns its impact outside the legislative boundaries of EU law. In the international arena of law concerning data, identity and information, the issue concerns balancing the economic interests and innovation liberalization with the competing laws for fundamental freedom for privacy and data protection rights. This is a complex problem to solve for those entrusted with making global laws as there is no agreed-upon global framework for regulating data flow across the jurisdictional maze of often diametrically opposing regulatory regimes.

[27] EEA**:'** The Agreement on the European Economic Area, which entered into force on 1 January 1994, brings together the EU Member States and the three EEA EFTA States — Iceland, Liechtenstein and Norway — in a single market, referred to as the "Internal Market**".** Source: https://www.efta.int/eea/eea-agreement

e) International Business Strategies for Data Privacy

The latest literature on the topic of strategies to deal with this diametrically opposing jurisdictional complexity of legislation related to data handling and its flow for economic and trade internationally suggests three solutions[28]. For this thesis, we aim to look at the three leading strategies to enact and adopt privacy laws within the scope of international business. We will be comparing the approaches adopted by various jurisdictions with the approach adopted by the EU for GDPR adoption. And compare it with the EU's GDPR.

The United States Constitution does not provide any specific data protection rights. The Constitution of Japan also does not provide any such protections. Both the USA and Japan, who are leading trade partners of the EU adopted the **'*Market-Based*' strategy** to apply minimum restraints through legislative and regulatory interventions in the area of data protection. The ICT Industry leads the way in advising the legislature on policies that balance data privacy and protection rights versus the economic interest of the market.

China, Russia, France and the UK, all major trade partners of the EU have a **'*Cautious*' strategy** towards data protection and privacy concerning economic policies and regulations. Excluding France and the UK, China and Russia also use state censorship to strictly regulate the ICT which resultantly also impacts the economic activities connected with the flow of data and privacy rights. Cyber Security is treated as an exclusive policy-making domain of the national security institutions for all matters concerning the storage and excess of mass data.

The third strategy is the **'*Interventionist*' strategy** which aims to seek comprehensive coverage of all aspects of data and information regardless of its application such as economic, social or cybersecurity. Canada and Australia are leading countries that apply such legislation across the entire domain of data-based applications.

The GDPR falls under the **'Interventionist' strategy** as it is supranational legislation that does not concern itself with the existing legislation on data protection and privacy in any of its Member States. Due to its supranational nature, GDPR has a direct effect both vertically and horizontally all across Europe. While the legal discussion of the '*Vertical and Horizontal Effects'* of EU legislation is beyond the scope of this paper. It would suffice for the business to understate that the '*Vertical Effect'* concerns State Institutions that must comply with the legislation while the '*Horizontal Effect'* can include persons and organizations that are not part of the State. This includes EU SMEs that are part of the EU's digital economy.

It is this doctrine of the 'Horizontal Effect' of the GDPR that can catch EU SMEs that are not GDPR compliant. Such EU SMEs can be subjected to financial penalties prescribed under the GDPR. It must also be noted that SMEs must also fully comply with GDPR, unlike the common myth that not all provisions of GDPR are directly enforceable against SMEs.

[28] Mitchell and Mishra (2018)."Data at the Docks: Modernizing International Trade Law for the Digital Economy"

f) Specific Data Protections Applicable to Non-EU Business

Article 45(2) of the GDPR explains the assessment of the level of protection afforded to the data of EU residents by a third party or a third country. Again, the GDPR doesn't need to apply, if the non-EU SMEs are not located within the EU or the data storage, access or processing of the EU resident's data is outside the EU.

One of the elements for assessing the level of data protection under GDPR for non-EU SMEs under GDPR Article 45(2) concerns international commitments of the EU related to personal data protection. This is not a straightforward matter as the EU has many bilateral data exchange agreements around the world. There are thousands of EU SMEs and non-EU SMEs upstream and downstream of such business agreements that have to seek European Commission re-assessments for data protection concerning EU residents' data since the enforcement of GDPR.

The complexity of the *physical infrastructure* of global ICT communications networks where data jumps multiple jurisdictions within a nanosecond leaving data impressions that may or may not be permanent within the narrow definitions of 'storage' 'adequacy of protection' etc poses a huge complexity for such assessments. It would be relevant to this discussion to mention that such assessments may not only delay the process of assessments entrusted to the European Commission, but, they may also pose some international obligation issues concerning bilateral trade agreements affected by GDPR Article 45(2) compliance.

Also, the European Commission's position on adequacy requirements about data under Article 45 GDPR creates a preference for those countries outside the EU that fall in the list of countries that are already considered to satisfy the adequacy requirement under GDPR Article 45. The international obligations of the EU under the World Trade Organization's (WTO) GATS[29] MNF[30] structure may create potential violations under GATS Article XVII[31] if the EU decides to exclude such agreements for compliance with GDPR Article 45.

There is no provision for derogation from GATS Article XVII for the EU's positive obligation to give access to its national markets under GATS that concern services using data. We are avoiding a detailed legal discussion on this point and would only elucidate the fact that GDPR compliance may create possible violations of GATS by the EU in the foreseeable future as there is no existing case law to help navigate such

[29] GATS:WTO's General Agreement on Trade and Services (GATS). 'The creation of the GATS was one of the landmark achievements of the Uruguay Round, whose results entered into force in January 1995.' Source: https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm

[30] MNF: WTO's 'Most Favoured Nation' concept allows for equal trade advantages by the recipient country. Source: https://www.wto.org/english/tratop_e/region_e/regatt_e.htm

[31] GATS Article XVII: 'Provides for obligations on Members in respect of the activities of the state trading enterprises referred to in paragraph 1 of Article XVII, which are required to be consistent with the general principles of non-discriminatory treatment prescribed in GATT 1994 for governmental measures affecting imports or exports by private traders'.

potential violations concerning SMEs due to divergent legal obligations of SMEs under GDPR and WTO's GATS.

In the post-World War II world, the USA emerged as the new global power replacing the UK. The US placed significant importance on Turkey's role as a gateway to the Mediterranean and Aegean Sea trade routes to North America and Europe. Turkey is part of the European Common Market but not a member of the EU. Turkey's membership in the EU is a political matter and stems from the Cyprus issue[32].

Turkey is one of the High Contracting Parties to the Council of Europe's fundamental rights instrument ECHR. While ECHR does not have any specific right for data protection, Article 8 right to privacy and family includes the right to data protection as also discussed earlier. Turkey has recently legislated its data protection law which is based on the broad principles of the EU Directive 95/46/EC that has been replaced by the GDPR.

Turkey's data protection legislation followed Turkey's ratification of ECHR's Convention 108 for the protection of personal data. The new Turkish legislation for data protection has differentiated itself from the EU's GDPR for 'consent'. While GDPR does not stipulate 'consent' with any degree of severity, the Turkish legislation calls for 'strict consent' in cases of 'sensitive data' and changes in the scope of data for data protection. Both GDPR and Turkish data protection legislation give the data subject exclusive powers through the requirement of 'consent'.

The exceptions in both cases remain exclusively in the areas of law enforcement, fighting serious crime, terrorism, and national security. It seems that the Turkish data protection law is trying to follow the data protection trends of GDPR to ensure that its economy continues to benefit from the EU data business and the critical economic activities between Turkish and EU SMEs. The example of Turkey within the context of the international impact of GDPR highlights the critical role GDPR is playing in shaping international data protection laws concerning natural person data.

The EU is a unique experiment of a supranational nature that created the largest single economic market with its unique set of laws. The ensuing chaos that followed World War II created a new world order that shaped the geopolitical and socioeconomic realities of the present-day world. The supranational nature of the EU laws is a new legal order of international laws. GDPR is a continuation of that legal order of international laws. GDPR is not a law that stands merged within the wide body of the European Jurisprudence.

It is a unique legal instrument that is transformative and has yet unknown and perhaps infinite repercussions for not only the EU but the entire world. The European Convention of Human Rights and the European Charter for Fundamental Rights set the stage for various constitutional provisions for rights protection around the world. GDPR also has the potential for such a transformative impression to give rise to a new generation of international data protection rights globally.

[32] On-going dispute between Turkey and Greece since 1974. The dispute started with British occupation of the Islands from Ottoman's in 1925.

a) GDPR- EU SME Challenges within the Global Data Economy

The UK legislated in 1972 under its European Union Act that the Courts in the UK would enforce and translate all municipal laws under the definitions provided by the EU law. Now that the BREXIT is complete, the real challenge begins for the SMEs both within the EU and the UK to decouple the two bodies of law within the context of GDPR compliance for businesses. (Armstrong, 2018) EU is termed as one of the successful examples of international law that created frameworks for socio-economic development on a global scale.(Steffek et al., 2007)

The contemporary theories to understand the concepts of global governance within the international legal order rest on two systems. Scholars seeking to study international law within the context of global governance focused on two types of normative systems. The first system rests on laws promulgated *by* nation-states and the second system is laws promulgated *among* the nation-states.(Krisch & Kingsbury, 2006)

These two theories eroded over time with the inclusion of state-sanctioned organisations emerging as either International Organisations (IOs) or intergovernmental organisations (IGOs) and acceptance of human rights within municipal law. These three entities became stakeholders in international law as separate entities thus the laws by the states and among the states now included other actors. The power of the State through the sovereignty doctrine still held sway over these new actors within the normative international law. Eminent legal scholars like Dr F.A. Mann still firmly believe that "*laws extend so far as, but no further than the sovereignty of the State which puts them into force*".(Mann, 1984)

Scholarship has been struggling to come up with some clear ideas and theories that can help explain the customary norms that end up as part of international law. The last fifteen years of legal scholarship suggest that there is increasing attention being paid to the important and sometimes inchoate processes of international norm development within the international community. The earlier example of the US rejecting ICJ's judgment sets a norm that is not part of the customary law traditions about the respectability of the ICJ. Scholars are also trying to define and understand the transnational legal process in ways that can explain the behaviour of nation-states over time to accept the laws of other nations within their legal systems.

The same effort is being made to understand how nation-states internalize international or transnational norms. The reversal of enthusiasm for globalisation is seen as a setback in the study of these processes. (Michaels, 2013) The global governance concepts that were emerging at the rise of globalisation during the 1990s suggested the declining impact of territorial restraints of law and the increasing impact of transnational law on municipal regimes. This reversal of the fate of globalisation is increasingly impacting the development of customary norms to strengthen global governance through IOs and IGOs including individual rights under the Universal Charter.(Overbeek et al., 2010)

The emergence of powerful global corporates has added a new dimension to the challenges of global governance. Concepts such as Corporate Social Responsibility

(CSR) have entered the debate about the voluntary norms that are to be considered within the context of economic disparities that emerge from the working of these all-powerful global corporations. Amazon is one of the largest supply-chain companies in the world. Its budget and its global reach coupled with its capacity to control global data networks through cloud-computing share are remarkable. (Vlcek, 2017)

The CEO of Amazon.com was recently in India. He demanded a meeting with the Prime Minister of the country to discuss the role of the local economy concerning the business interests of his company. The Indian government ignored Jezz Bezos as the local retail markets of India have suffered acutely due to the vast reach of Amazon to the global supply chain.(Govindarajan et al., 2020) The rules of engagement for these powerful corporate entities are not defined within international law or any available framework for global governance.

Regulatory pluralism has been defined as a way to give impetus to the development of global governance that may entail multi-dimensional entities as a stakeholder. International legal scholars have sought to understand the multifaceted role of law in settings beyond States, IOs and IGOs. If such an understanding is to happen, then it would require serious insights into legal pluralism. The theory of legal pluralism offers the premise that people belong to and are affiliated with multiple groups.

This creates an understanding of rules that are bound by the norms of these multiple groups. (Hakimi, 2020)Over time, the jurisdiction of these non-state actors as groups that were formally limited to the boundaries of their particular communities and the norms, they articulate starts to seep into the decisions of state legal institutions and further into international law. The Uniform Commercial Code (UCC) is an example of a local merchant sale system becoming a normative customary law that governs international trade. Article 2 Revision of the UCC is now working towards an international standard for the internet economy. (Martin et al., 2016) It follows by analogy that any efforts for acceptable international legal order must address the interplay of a wide variety of normative commitments and law-giving entities.

b) GDPR Impacts International Business

International business is regulated by business law that is often described not as a body of law, but as a code of morals and ethics prescribed by the international community.[33] The reasonings for defining subjects that are specifically within the domain of international law are also not particularly clear in the literature. The *raison d'être* of international law, in terms of what societal functions are covered by international law and what role international politics and international morality play in creating those laws, is also an open debate. [34]

Any arguments that rest on the premise that a particular issue is not a problem of international law but of politics or international policy normally lead to the tendency to abandon any further inquiry of the question under the rules of law. It is then often

[33] John Austin, *Lectures on Jurisprudence: Or The Philosophy of Positive Law* (J. Murray, 1875).

[34] Francis Anthony Boyle, *World Politics, and International Law* (Duke University Press, 1985).

assumed that the problems should be taken up by scholars of international relations or international polity.

The reality is that international law continues to impact and perform distinct societal functions that are based on a political understanding of the problems that it intends to tackle. International law also acts to impact the political and legal perceptions within various branches of municipal law.

Scholarship is increasingly endeavouring to bridge the gap between international law and international business relations. For example, scholarship based on institutionalist and constructivist theories relies on international treaties and the resolutions of international organizations about international trade, climate change, and harmonisation of business laws that can allow SMEs to also leverage multinational presence through ICTs. These linkages cannot be bridged without fully understanding the business and economic dimensions underpinning the treaties and the resolutions of the international organisations. (Burley, 2017)

Scholarship considers international law to be ‘soft law’ due to its limitations in terms of enforcement. Consequently, municipal law is normally considered ‘hard law’ due to the enforcement mechanisms through the use of various enforcement agencies employed by the State. Some legal scholars hope that the ‘soft law’ element of international law can someday be turned into ‘hard law’. This notion is misplaced as both municipal law and international law serve distinct purposes that cannot be conflated.

International business has evolved and has been shaped by its deep linkages with the evolution of business science. Its purposes are linked with the interrelations predominantly economic in nature between States and international organisations. These distinct legal personalities beyond the scope of the municipal understanding allow international law to propose rules that are flexible, especially for business and can be negotiated through a bilateral and multilateral political dialogue. (Slaughter et al., 1998)

c) Conclusion

GDPR poses unique challenges for businesses in general and SMEs in particular due to their limited ability to financially reposition their resources to the rapid regulatory changes. The global data economy has complex interconnections that are not easily resolved by simple modelling suggestions. International business law scholars are constantly endeavouring to comprehend the changing landscape of legal rules that operate on the global stage and create challenges for businesses, especially SMEs. SMEs form the backbone of any economy and its especially true for the EU.

The global view of business and its related regulations keeps shifting with the shifts in the global polity that is sometimes hinged on the national economic agendas. GDPR is proposing and imposing international reach to protect the EU residents’ data used by non-EU businesses and other organisations. The idea that nation-states are the only relevant form of community affiliation is being constantly challenged due to the creation of ICT communities that transcend national boundaries. Social terms like ‘**tech nomads’** and ‘web citizens’ are now part of the technology business lexicon. There is

a rigorous question arising about the business geographical identity flowing from the nation-state.

GDPR has also provided an opportunity to critically examine the entire spectrum of business law, municipal as well as international concerning the data economy and its resultant impact on the business world, especially the SMEs. The challenge is to create a balance between the data subject rights to privacy and the business interests that offer services to the data subject in exchange for their business.

Such analysis will also help the SMEs to reveal the more inchoate ways in which business models and norms can be articulated concerning personalised content leveraging identity data. A deeper analysis of socioeconomic dichotomies often provides a more complicated picture of the business world than the top-down rules of business regulations portrayed in the academic literature. The scholarship is increasingly integrating a myriad of questions about space, place, boundaries, diasporas, migrations, and their impact on global business within the scope of the emerging personalised digital space. These research trend especially concerning GDPR and its impact on SMEs seems to justify the demand.

10) RESEARCH CONCLUSIONS

a) GDPR Preparedness

The GDPR preparedness of EU SMEs from the 600 fully answered survey questionnaires showed 45% fully prepared and 49% partially prepared SMEs. These results are consistent with other surveys conducted by researchers within the EU and non-EU researchers.

b) GDPR Implementation Challenges

The question of GDPR implementation challenges provided insights into EU SMEs that were already in compliance with previous EU legislation on data protection and EU SMEs that started the process of GDPR compliance in fear of the steep fines imposed for non-compliance. Thus, 49% of the 600 respondents from SMEs that had just started the process of data protection due to GDPR found some challenges faced by their SMEs for compliance with GDPR. Thus 42% of the respondents that found no challenges associated with GDPR compliance belonged to EU SMEs that were already complying with previous EU legislations for data protection. This data is also consistent with other surveys conducted on the topic.

c) GDPR Compliance Impact on EU SMEs

The business Impact of GDPR was framed in terms of (1) the financial costs of GDPR compliance (2) an Increase in the cost of doing business and (3) any reduction in the business volume due to GDPR compliance. 38% of the respondents found some pact of the three factors on their SMEs due to GDPR compliance, 29% of respondents found a great impact of the three factors due to GDPR compliance and 25% of respondents found no impact of the 3 factors due to GDPR compliance.

d) EU SMEs Investment for GDPR Compliance

GDPR has imposed a financial burden on EU SMEs to implement and comply with its various mechanisms to ensure the data protection and privacy of EU residents. 49% of the respondents confirmed that some investments were made by their SMEs to comply with GDPR. These respondents were part of EU SMEs that were already compliant with previous EU legislation on data protection. 31% of respondents confirmed major investments by their SMEs to comply with GDPR. 12% of respondents confirmed no investment was required by their SMEs as their GDPR preparedness with funded by sources other than their investment. These findings are consistent with other surveys.

e) GDPR Impact on EU SMEs

The question of GDPR's impact on EU SMEs is at the heart of this research. It is more so because 22 million EU SMEs are the backbone of the EU economy and employ 90% of the EU's workforce. Details were provided in the questionnaire to guide the respondents about the criteria of negative, positive or no impact choices. 23% of the respondents stated that GDPR harmed their SMEs. 53% of the respondents stated the

positive impact of GDPR on their business, and 23% stated no impact on their business. These findings are consistent with the other surveys conducted by researchers.

f) GDPR Offers Competitive Advantage to EU SMEs

The question of EU lawmakers creating supranational legislation with international reach to protect the personal data of EU residents has come under severe criticism from the EU's major trade partners like the USA. The major criticism is that the EU is trying to localise EU residents' data as a protectionist policy against the US tech giants that control the global data business. 69% of the respondents agreed that GDPR gives their EU SMEs a limited competitive advantage. 21% saw no advantage for EU SMEs due to GDPR compliance, and only 9% of the respondents saw a great competitive advantage for their SMEs due to GDPR compliance.

g) GDPR as Ideal Response to Data Protection

EU lawmakers consider GDPR as the most advanced and ideal solution to tackle the data protection needs of EU residents in the wake of emerging ICTs. Yet, scholars and critics have provided alternative evidence to support their thesis that emerging technologies like AI and Blockchain are absent from the EU lawmakers' vision as regards the framing of GDPR. "Right to be Forgotten' and 'localisation of data' within the EU are two key protections under GDPR. Both AI and Blockchain cannot be harnessed with the two protections. 35% of the respondents did not find GDPR to be the ideal data protection response but found it to improve the SME business within the scope of consumer confidence in their data protection. 52% of the respondents found GDPR to be the ideal response to data protection and also found GDPR to be a factor in improving their business. Due to the short period since the implementation of GDPR, there is not enough evidence to support or negate these conclusions. However, the existing data does support these results.

11) IMPACT & FUTURE RESEARCH

There are 22 million EU SMEs that employ more than 90% of the EU's workforce. This research is an attempt to draw attention to the various regulatory overturns towards the most important sector of the EU's economy. GDPR has certainly made a mark as a data protection law that concerns the privacy and protection of a natural person's data. However, the scope of GDPR impacts the largest business segment of the EU, the EU SMEs.

This research has shown the impact of GDPR from the perspective of the EU SMEs and the impact on their ability to survive such rigorous legislation that tried a one-size-fits-all approach to personal data protection. Limited research has emerged on the impact of GDPR on the EU SMEs and their ability to innovate and continue to play a vital role in the EU-27 socio-economic prosperity.

The impact of this research is its focus on GDPR's impact on EU SMEs and their competitive advantage. This research with its quantifiable data analysis has partially answered:

- GDPR has negatively impacted EU SMEs for cost compliance and potential fines.
- GDPR positively impacted the EU SMEs for improved customer personal data security and enhanced customer confidence in EU SMEs due better security of their data.
- EU SMEs are likely to face higher financial sanctions if they are found to be non-compliant with GDPR.
- The GDPR preparedness of EU SMEs is lacking due to their size and financial limitations.
- GDPR interpretation is legally complex, and EU SMEs lack the financial capacity to engage in legal services for GDPR understanding and compliance.
- GDPR does not provide any competitive advantage to EU SMEs.

Future research targeting the major EU-27 economies with detailed analysis of GDPR with country focus would perhaps highlight the challenges being faced by the EU SMEs in compliance with GDPR. With the emerging trends in AI and Blockchain, future research would perhaps guide EU lawmakers to address the existing gaps in GDPR that may potentially harm the growth of EU SMEs.

The statistical analysis of this research allows for data interpretation to further research topics such as:

- **GDPR impact on various income groups related to business models of EU SMEs within the EU data economy.**
- **GDPR impact on skill levels of the workforce within EU SMEs for better compliance .**
- **GDPR impact on EU SME data protection compliance and development of business strategies to mitigate potential fines**

12) APPENDIX A- SURVEY QUESTIONNAIRE

a) Scope & Purpose of the Survey

The GDPR Impact on EU SMEs Survey ("the survey") is being conducted as a part of the DBA thesis research to collect data from selected EU SMEs. The scope of the survey extends to collect data on EU SMEs GDPR preparedness, any investments related to its preparedness and compliance, its business impact and the competitiveness that it may offer.

The results obtained through the survey will be used to meet the data analysis aims and objectives defined for the thesis research. The survey conduct is protected complies with the GDPR guidelines for data protection and is completely confidential and anonymous. The data collected from the survey will be aggregated and used only for the scope and purpose defined ante.

b) Survey Structure

This document explains the structure of the survey and is divided into the following parts:

Part-1: No-Name/ No- Personal Information based on participants' general information as per the criteria for selection

Part 2: Survey Questionnaire with explanations

Part 3: Definitions and Supporting Information to Facilitate Questionnaire

c) Part1- General Instructions

Survey Completion Deadline: Saturday, April 11th, 2020, before midnight (23:59).

(The Survey was posted on https://www.pollfish.com/)

Participants General information

GENDER

- o Male
- o Female
- o Prefer not to state

AGE

- o 18-24
- o 25-34
- o 35-44
- o 45-54
- o >54
- o Prefer not to state

COUNTRY

- o Germany
- o Spain
- o France
- o UK

- Italy
- Poland

ORGANIZATION ROLE

- Technical Staff (ICT)
- Non-Management Staff
- Production Management
- Middle Management
- Chief Technical Officer (CTO)
- Partner/Owner/CEO

NUMBER OF EMPLOYEES

- 6-10 (Micro)
- 11-25
- 51-100
- 101-250

d) Part II- Questionnaire

Screening Question (Single Selection)

SQ-1. Are you an owner or work with an SME in Europe/EU-27/UK?

Choices: A1- Yes, A2- No

Notes: If the answer to this question is A1, you may proceed and complete the survey. If the answer is A2, please quit the survey.

Q1. What is the type of business that defines your SME?

A1- Part of Data Economy

A2- Other

Notes:

A1- Part of the data economy means that your SME is a direct participant in the web-based business or services that utilise EU residents' data which may directly involve, access, storage, and processing of such data using in-house or outsourced data housing and processing services.

A2- 'Other' means that your SME is producing goods and services that rely on web services but do not directly offer web-based services. Your SME is in the category of 'Other' if it may indirectly use the services of a company or individuals accessing, storing, or processing EU residents' data but has no in-house or outsourced data processing services for EU residents.

Q2. How would you describe the GDPR preparedness of your SME?

A1- Prepared

A2- Somewhat prepared

A3- Not Prepared

Notes:

A1- Preparation of your SME for GDPR means that your SME has mechanisms (written policies and systems) in place for handling the following mandatory areas of GDPR compliance:

- personal data
- data subject rights
- accuracy and retention
- transparency requirements
- other data controller obligations
- data security
- data breaches

o international data transfers

A2- If your SME is still in the process of preparing the mechanism as listed above in A1 and has covered 5 or more items out of 8 items listed in A1.

A3- If your SME is still in the process of preparing and has covered 4 or fewer items **listed in A1 above.**

Q3- Has your SME faced any legal challenges due to non-compliance with GDPR since May 2018?

A1- Some Challenges

A2- No Challenges

A3- DO not know

Notes:

A1- Some challenges mean that either your SME has (1) Not engaged any legal professionals to assist in preparing and implementing GDPR compliance within your SME or (2) the GDPR compliance preparations are not moving due to any existing legal challenges facing your SMEs business

A2- If your SME has (1) successfully implemented GDPR compliance or (2) a legal team is assisting your firm with GDPR compliance preparations without any known impediments to the process

A3- If your SME has not shared any legal challenges with the staff or has not proceeded to audit its legal compliance with the GDPR preparedness/ implementation.

Q4- Has the business volume of your SME been impacted by the GDPR compliance?

A1- Some Financial Impact

A2- Great Financial Impact

A3- No Financial Impact

A4- Don't know

Notes:

A1- GDPR Preparedness and compliance cost diverted the SME from its core business and resulted in the reduction of its business volume between 10 or less or up to 20% compared to the year before GDPR preparedness and compliance started for the SME

A2- GDPR preparedness and compliance costs diverted the SME from its core business including diverting its reserve investments for growth. The resultant reduction in the business volume of the SME was more than 25% and up to 40% or more.

A3- The SME was already in compliance with previous EU data protection laws and/or the cost of GDPR preparations and compliance neither reduced the business nor increased for more than 5% of its comparable volume a year before GDPR compliance.

A4- SME does not quantify such business volumes or no such information is made available to the staff.

Q5-Has your SME invested in GDPR preparedness and compliance?

A1-Some investment

A2-Lot of investment

A3-No investment

A4-Don't know

Notes:

A1- SME made investments that were already part of its ongoing GDPR preparedness plans and no extra funding had to be taken out of the business investments or the additional investments for GDPR preparedness did not exceed above 10% of the already anticipated/available budget.

A2- SME made additional investments through 100% borrowing/loans or SME had to supplement its existing budgeted investment for GDPR preparedness that exceeded 60% or more of the budget amount or SME had to divert 100% of its reserve investment funds to ensure GDPR preparedness.

A3- All investment required for SME's GDPR preparedness came in the shape of a national/regional/third-party grant/program that did not impose any financial burden on the SME for its GDPR preparedness.

A4- No such information is kept by the SME or SME staff is not provided with this financial information.

Q6- In your opinion, the GDPR has positively or negatively impacted your SME's business?

A1- Negative Impact

A2- Positive Impact

A3- No Impact

Notes:

A1- Has GDPR harmed your SME business (1) if the SME relied on international business within the data value chain and the upstream business reduced your business volume due to GDPR compliance matters (2) customer trust levels in your company's GDPR compliance efforts reduced the business (3) business is struggling to meet the cost of compliance (4) GDPR compliance had diverted the limited human resource to compliance readiness and reduced business productivity (5) any cost or customer-related adverse impact due to GDPR compliance are harming the SMEs business

A2- GDPR compliance has improved the customer's confidence and resultantly improved the SMEs business (2) GDPR compliance and readiness have brought new business (3) better ICT systems/ upgrades in software and hardware due to GDPR preparedness are also benefiting the business efficiency (4) staff motivation and confidence has improved with the improvements and upgrades due to GDPR preparedness.

A3- Such data is not maintained by the SME/ Staff does not have any such information/No evidence is seen of any negative or positive impact

Q7- The GDPR has changed the privacy policies of your SME?

A1- No change to privacy policies

A2- Some changes to privacy policies

A3- Major changes to privacy policies

Notes:

A1- SME has been keeping up with previous data protection laws of the EU and has been working with much more robust privacy policies that came out to exceed the requirements laid out in GDPR.

A2-SME has been working with the previous data protection policies of the EU and after auditing GDPR requirements, the existing policies are now in compliance with GDPR.

A3- SME did not have any existing data privacy policies/limited privacy policies and all the data privacy policies required under GDPR have been completely re-done.

Q8- Do you think that GDPR is the ideal response for data protection, and it will help improve your SMEs business prospects?

A1- Not ideal but will improve the business

A2- Ideal and will improve the business

A3- Not ideal and will not improve the business

Notes:

A1- GDPR is vague and complicated and its compliance cost is not suited to the SME, however, customer confidence will improve the business in the long run.

A2- GDPR is best suited to protect the customers' data and its compliance costs notwithstanding, it will be a win-win for the data subjects as well as the SME.

A3- GDPR is not suitable for SMEs due to its vague language, and high costs of compliance that are difficult for SMEs to absorb. The anticipated operating costs of the SME will rise with the GDPR ongoing compliance costs and will not be beneficial to the SME business.

Q9- Do you think that GDPR impacts the competitive advantage of EU SMEs?

A1- No advantage

A2- Some Advantage

A3- Great Advantage

Notes:

A1- GDPR favours tech giants like Google, Facebook, and Microsoft to take the investment capacity to comply and even fight the steep fines for GDPR compliance. Limited financial investment and the detrimental impact of GDPR fines do not offer any advantage to EU SMEs. GDPR is focused more on the data protection rights of the data subjects and does not balance the innovation needs of emerging technologies like AI and Blockchain etc. EU SMEs will be limited to any investments available within the EU only due to restrictions imposed by GDPR for data localisation within the EU.

A2- GDPR compliance costs and steep fines are negative for EU SMEs. US tech giants will be able to navigate the challenges imposed on their businesses due to their investment capacities. However, any limits on US tech giants are likely to improve the business opportunities for EU SMEs as the potential for growth through partnerships and synergy development within the EU will benefit in the long run.

A3-GDPR can harmonise data protection policies across EU-28. It will impose steep fines on any violations of GDPR and improve consumer confidence in their data protection by EU SMEs. Continued compliance with GDPR will improve the data protection systems within the EU and result in improved innovation and business opportunities.

Q10- GDPR will have a long-term impact on the SME's business?

A1- Negative Impact

A2- Positive Impact

A3- Some Impact

A4- No impact

Notes:

A1- GDPR is an overly restrictive data protection law that does not favour the EU SMEs/EU Data Economy due to its high costs of implementation and restrictions imposed on aggregated data products. GDPR does not consider advanced and emerging technologies like AI and Blockchain including personal identity-based customized web products. The venture capital markets of North America/Asia for technology innovation are going to ignore EU SMEs due to restrictive GDPR compliance and data localisation requirements.

A2- GDPR is going to improve the EU’s internal data innovation market through data protection law harmonisation. It will improve the flow of venture capital to EU SMEs for technology innovation due to their GDPR compliance edge.

A3- GDPR may improve the EU SMEs' ability to innovate in the long run if the consumers continue to demand higher standards of their personal data protection from tech giants external to EU-27.

A4- The global data economy is much larger and more resilient to any drastic changes within EU legislation for data protection demands. It is unlikely that GDPR will effectively rope in international tech giants for their non-compliance with GDPR concerning EU residents' data.

e) Part III- GDPR Explanation & Guide

(**Source:** "What Is GDPR, the EU's New Data Protection Law?," GDPR.EU, November 7, 2018, https://gdpr.eu/what-is-gdpr/.)

a) **Scope, penalties, and key definitions**

First, if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU. We talk more about this in another article.

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

b) Relevant Terms

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… and anything.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

c) Data protection principles

If you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2:

- **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization** — You should collect and process only as much data as necessary for the purposes specified.
- **Accuracy** — You must keep personal data accurate and up to date.
- **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).

• **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

d) Accountability

The GDPR says data controllers have to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how then you're not GDPR compliant. Among the ways you can do this:

• Designate data protection responsibilities to your team.

• Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.

• Train your staff and implement technical and organizational security measures.

• Have Data Processing Agreement contracts in place with third parties you contract to process data for you.

• Appoint a Data Protection Officer (though not all organizations need one — more on that in this article).

e) Data security

You're required to handle data securely by implementing "appropriate technical and organizational measures."

Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff training, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

f) Data protection by design and by default

From now on, everything you do in your organization must, "by design and by default," consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in Article 25.

Suppose, for example, you're launching a new app for your company. You have to think about what personal data the app could collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

g) When you're allowed to process data

Article 6 lists the instances in which it's legal to process personal data. Don't even think about touching somebody's data — don't collect it, don't store it, don't sell it to advertisers — unless you can justify it with one of the following:

• The data subject gave you specific, unambiguous consent to process the data. (e.g. They've opted into your marketing email list.)

• Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)

• You need to process it to comply with a legal obligation of yours. (e.g. You receive an order from the court in your jurisdiction.)

• You need to process the data to save somebody's life. (e.g. Well, you'll probably know when this one applies.)

• Processing is necessary to perform a task in the public interest or to carry out some official function. (e.g. You're a private garbage collection company.)

- You have a legitimate interest in processing someone's data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data.
- Once you've determined the lawful basis for your data processing, you need to document this basis and notify the data subject (transparency!). If you decide later to change your justification, you need to have a good reason, document this reason, and notify the data subject.

h) Consent

There are strict new rules about what constitutes consent from a data subject to process their information The rules are:

- Consent must be "freely given, specific, informed and unambiguous."
- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language."
- Data subjects can withdraw previously given consent whenever they want, and you have to honour their decision. You can't simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parents.
- You need to keep documentary evidence of consent.

i) Data Protection Officers

Contrary to popular belief, not every data controller or processor needs to appoint a Data Protection Officer (DPO). There are three conditions under which you are required to appoint a DPO:

- You are a public authority other than a court acting in a judicial capacity.
- Your core activities require you to monitor people systematically and regularly on a large scale. (e.g., You're Google.)
- Your core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR or data relating to criminal convictions and offences mentioned in Article 10. (e.g. You're a medical office.)

You could also choose to designate a DPO even if you aren't required to. There are benefits to having someone in this role. Their basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, conducting data protection training, conducting audits and monitoring GDPR compliance, and serving as liaisons with regulators.

j) People's privacy rights

You are a data controller and/or a data processor. But as a person who uses the Internet, you're also a data subject. The GDPR recognizes a litany of new privacy rights for data subjects, which aim to give individuals more control over the data they loan to organizations. As an organization, it's important to understand these rights to ensure you are GDPR compliant. Below is a rundown of data subjects' privacy rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights concerning automated decision-making and profiling.

13) APPENDIX B- GDPR ARTICLES

a) Chapter I – General provisions

- Article 1 – Subject matter and objectives
- Article 2 – Material scope
- Article 3 – Territorial scope
- Article 4 – Definitions

b) Chapter II – Principles

- Article 5 – Principles relating to the processing of personal data
- Article 6 – Lawfulness of processing
- Article 7 – Conditions for consent
- Article 8 – Conditions applicable to child's consent about information society services
- Article 9 – Processing of special categories of personal data
- Article 10 – Processing of personal data relating to criminal convictions and offences
- Article 11 – Processing which does not require identification

c) Chapter III – Rights of the Data Subject

Section 1 - Transparency and Modalities

- Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2 - Information and access to personal data

- Article 13 – Information to be provided where personal data are collected from the data subject
- Article 14 – Information to be provided where personal data have not been obtained from the data subject
- Article 15 – Right of access by the data subject

Section 3 - Rectification and erasure

- Article 16 – Right to rectification
- Article 17 – Right to erasure ('right to be forgotten)
- Article 18 – Right to restriction of processing
- Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Article 20 – Right to Data Portability

Section 4 - Right to object and automated individual decision-making

- Article 21 – Right to object
- Article 22 – Automated individual decision-making, including profiling

Section 5 - Restrictions

- Article 23 – Restrictions

d) Chapter IV – Controller and processor

Section 1 - General obligations

- Article 24 – Responsibility of the controller
- Article 25 – Data protection by design and by default
- Article 26 – Joint controllers
- Article 27 – Representatives of controllers or processors not established in the Union
- Article 28 – Processor
- Article 29 – Processing under the authority of the controller or processor
- Article 30 – Records of processing activities
- Article 31 – Cooperation with the Supervisory Authority

Section 2 - Security of personal data

- Article 32 – Security of processing
- Article 33 – Notification of a personal data breach to the Supervisory Authority
- Article 34 – Communication of a personal data breach to the data subject

Section 3 - Data protection impact assessment and prior consultation

- Article 35 – Data Protection Impact Assessment
- Article 36 – Prior consultation

Section 4 - Data Protection Officer

- Article 37 – Designation of the Data Protection Officer
- Article 38 – Position of the Data Protection Officer
- Article 39 – Tasks of the Data Protection Officer

Section 5 - Codes of conduct and certification

- Article 40 – Codes of conduct
- Article 41 – Monitoring of approved codes of conduct
- Article 42 – Certification
- Article 43 – Certification bodies

e) Chapter V – Transfers of personal data- third countries

- Article 44 – General principle for transfers
- Article 45 – Transfers based on an adequacy decision
- Article 46 – Transfers subject to appropriate safeguards
- Article 47 – Binding corporate rules
- Article 48 – Transfers or disclosures not authorised by Union law
- Article 49 – Derogations for specific situations

- Article 50 – International cooperation for the protection of personal data

f) Chapter VI – Independent Supervisory Authorities

Section 1 - Independent status

- Article 51 – Supervisory authority
- Article 52 – Independence
- Article 53 – General conditions for the members of the Supervisory Authority
- Article 54 – Rules on the establishment of the supervisory authority

Section 2 - Competence, tasks and powers

- Article 55 – Competence
- Article 56 – Competence of the Lead Supervisory Authority
- Article 57 – Tasks
- Article 58 – Powers
- Article 59 – Activity reports

g) Chapter VII – Cooperation and Consistency

Section 1 – Cooperation

- Article 60 – Cooperation between the lead supervisory authority and the other supervisory authorities concerned
- Article 61 – Mutual assistance
- Article 62 – Joint operations of supervisory authorities

Section 2 - Consistency

- Article 63 – Consistency mechanism
- Article 64 – Opinion of the Board
- Article 65 – Dispute resolution by the Board
- Article 66 – Urgency procedure
- Article 67 – Exchange of information

Section 3 - European Data Protection Board

- Article 68 – European Data Protection Board
- Article 69 – Independence
- Article 70 – Tasks of the Board
- Article 71 – Reports
- Article 72 – Procedure
- Article 73 – Chair
- Article 74 – Tasks of the Chair
- Article 75 – Secretariat
- Article 76 – Confidentiality

14) APPENDIX C- SURVEY RESPONDENT AGREEMENT

Data Processing Agreement

This Data Processing Agreement ("Agreement ") forms part of the Data Collection for DBA Research in compliance with GDPR Services ("Principal Agreement ") between

The respondents to the Survey

(the "respondent of the survey") and

DBA Researcher through Pollfish ("Company")

(the "Data Processor- DBA Candidate")

(Together as the "Parties")

WHEREAS

(A) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework concerning data processing and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of the Company according to or in connection with the Principal Agreement.

1.1.3 "Contracted Processor" means a Sub-processor.

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

1.1.5 "EEA" means the European Economic Area.

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679.

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the data collection survey hosting services the Company provides.

1.1.10 “Sub-processor” means any person appointed by or on behalf of the Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Company Personal Data, as strictly necessary for the Principal Agreement, and to comply with Applicable Laws in the context of that individual’s duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall concerning the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take into account in particular the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Considering the nature of the Processing, the Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of the Company or as required by Applicable Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as directed by the Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely concerning Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within

10 business days from the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Personal Data.

10. Audit rights

10.1 Subject to this section 10, the Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company concerning the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law.

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the

address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of the EU.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of the EU, subject to a possible appeal to CJEU.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

DBA Survey Respondent: I Agree (tick the box)/Consent

15) APPENDIX D- GDPR FINES

a) Explanation

GDPR fines are designed to make non-compliance a costly mistake for both large and small businesses. In this article, we'll talk about how much is the GDPR fine and how regulators determine the figure.

The European Union's General Data Protection Regulation (GDPR) was designed to apply to all types of businesses, from multinationals down to micro-enterprises. The fines imposed by the GDPR under Article 83 are flexible and scale with the firm. Any organization that is not GDPR compliant, regardless of its size, faces a significant liability.

Below we will look at the administrative fine structure, how fines are assessed, and which infringements can incur penalties.

b) Two tiers of GDPR fines

The GDPR states explicitly that some violations are more severe than others.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. They include any violation of the articles governing:

Controllers and processors (Articles 8, 11, 25-39, 42, and 43) — Organizations that collect and control data (controllers) and those that are contracted to process data (processors) must adhere to rules governing data protection, the lawful basis for processing, and more. As an organization, these are the articles you need to read and adhere to.

Certification bodies (Articles 42 and 43) — Accredited bodies charged with certifying organizations must execute their evaluations and assessments without bias and via a transparent process.

Monitoring bodies (Article 41) — Bodies that have been designated to have the appropriate level of expertise must demonstrate independence and follow established procedures in handling complaints or reported infringements impartially and transparently.

The more serious infringements go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR. These types of infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. These include any violations of the articles governing:

The basic principles for processing (Articles 5, 6 and 9) — Data processing must be done in a lawful, fair, and transparent manner. It has to be collected and processed for a specific purpose, be kept accurate and up to date and processed in a manner that ensures its security. Organizations are only allowed to process data if they meet one of the six lawful bases listed in Article 6. In addition, certain types of personal data, including racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, and health or biometric data are prohibited except under specific circumstances.

The conditions for consent (Article 7) — When an organization's data processing is justified based on the person's consent, that organization needs to have the documentation to prove it.

The data subjects' rights (Articles 12-22) — Individuals have a right to know what data an organization is collecting and what they are doing with it. They also have a right to obtain a copy of the data collected, to have this data corrected, and in certain cases, the right to have this data be erased. People also have a right to transfer their data to another organization.

The transfer of data to an international organization or a recipient in a third country (Articles 44-49) — Before an organization transfers any personal data to a third country or international organization, the European Commission must decide that that country or organization ensures an adequate level of protection. The transfers themselves must be safeguarded.

They also include:

Any violation of member state laws adopted under Chapter IX — Chapter IX grants EU member states the ability to pass additional data protection laws as long as they are under the GDPR. Any violation of these national laws also faces GDPR administrative fines.

Non-compliance with an order by a supervisory authority — If an organization fails to comply with an order from the monitoring bodies of the GDPR, they have set themselves up to face a huge fine, regardless of what the original infringement was.

And these are just the administrative fines. Article 82 gives data subjects the right to seek compensation from organizations that cause them material or non-material damage as a result of a GDPR infringement.

c) How much is a GDPR fine?

Under the GDPR, fines are administered by the data protection regulator in each EU country. That authority will determine whether an infringement has occurred and the severity of the penalty. They will use the following 10 criteria to determine whether a fine will be assessed and in what amount:

- Gravity and nature — The overall picture of the infringement. What happened, how it happened, why it happened, the number of people affected, the damage they suffered, and how long it took to resolve.
- Intention — Whether the infringement was intentional or the result of negligence.
- Mitigation — Whether the firm took any actions to mitigate the damage suffered by people affected by the infringement.
- Precautionary measures — The amount of technical and organizational preparation the firm had previously implemented to comply with the GDPR.
- History — Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.
- Cooperation — Whether the firm cooperated with the supervisory authority to discover and remedy the infringement.
- Data category — What type of personal data does the infringement affect?
- Notification — Whether the firm or a designated third party proactively reported the infringement to the supervisory authority.
- Certification — Whether the firm followed approved codes of conduct or was previously certified.

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

If regulators determine an organization has multiple GDPR violations, it will only be penalized for the most severe one, provided all the infringements are part of the same processing operation.

Source: "What Are the GDPR Fines?" GDPR.EU, July 11, 2018, https://gdpr.eu/fines/.

16) DEFINITIONS

Accountability

GDPR stipulates that organisations must be able to show evidence of their compliance with data protection laws. Accountability is the capacity of organisations to show that they are carrying out measures demanded by the regulations.

Accuracy Principle

The notion is that data controllers should keep personal data up to date and accurate, taking reasonable steps to ensure that inaccurate data is corrected.

Anonymous Data

Data that cannot be traced back to an identifiable individual, and hence falls outside the scope of the GDPR.

Article 29 Working Party

A non-regulatory EU-level data protection body that provided advice on how to comply with data protection law to the Member States before the introduction of GDPR. The organisation comprised members of national data protection authorities at the EDPS. It is now the EDPB under GDPR.

Binding Corporate Rules

Legally enforceable rules that enable a multinational company or organisation to transfer personal data from its entities in the EU to its entities (subsidiaries and affiliates but not third parties) in countries outside the EEA.

Biometric Data

Biometric data refers to any data derived from a data subject's biology or physical body. These data could include information regarding the physiological, behavioural or physical characteristics of a natural person, including iris scans, fingerprints, and facial images.

Breach

A security failure that leads to the accidental or unlawful access, disclosure, loss or destruction of personal data.

Breach Notification

The requirement for organisations to report the data breach to the supervisory authority within 72 hours of becoming aware of the breach. The individual data subjects impacted in the breach may also need to be notified in case of a risk to their rights or freedoms.

Consent

Any act by the owner of data indicates that they are willing to allow their data to be processed for a specific purpose. Consent must be unambiguous, informed, specific and freely given and can be retracted by the data subject at any time under GDPR.

Cross-Border Processing

Any situation in which the data processor or data controller operates across multiple Member States and processes personal information across those borders. Cross-border processing also refers to a situation in which a data controller operates in one country but receives data from data subjects in multiple countries.

Data Controller

The controller (organisation or individual) is the main decision-maker concerning personal data. They exercise overall control over the purposes and means of the processing of personal data. Employers are data controllers of their employees' data.

Joint controllers are two or more controllers that jointly determine the purposes and means of the processing of the same personal data.

Data Portability

Data portability is a scheme that makes it easier for individuals to transfer their data from one controller to another. GPDR gives data subjects the right to receive their data in electronic format and then pass it on to another controller (for example, if they want to change service provider).

Data Privacy Impact Assessment (DPIA)

A DPIA is a process that is used to help identify and minimise the data protection breach risks that come with processing any personal information. When it comes to processing, certain types require a DPIA. This is usually the case when any type of processing is considered to be high risk in terms of security leaks. Describe the data processing in place and the purpose for doing it. Assesses whether the processing is necessary. Identifies and assesses the risk to data subjects. Determines any measures that can be put in place to mitigate risk and help protect data from breaches.

Data Processing

In the context of data protection, processing covers a wide range of manual or automated operations performed on personal data, including the collection, recording, structuring, storage, adaptation or alteration, archival, retrieval, consultation, use, disclosure by transmission, dissemination or publishing, combination, restriction, and erasure or destruction of personal data.

Data Processing Agreement (DPA)

A legally binding contract (required under GDPR Article 28 Section 3) that states the rights and obligations of the data processor and data controller concerning the protection of personal data.

Data Processor

Any individual or organisation with authorisation to edit, modify, delete, transfer, use or change a data subject's data. A data controller can be the data processor too or may outsource processing to a third party (which then is the data processor).

Data Protection Act (DPA)

The Data Protection Act 2018 sets out the data protection framework in the UK, alongside the GDPR.

Data Protection Authority

Each member state of the EU has a data protection authority or supervisory authority. The job of the national DPA is to ensure that member states of the EU enforce data protection laws. Many DPAs have extensive enforcement powers, allowing them to impose fines on organisations and individuals who do not comply. The authority in the UK with these powers is the ICO.

Data Protection Officer (DPO)

A data protection officer is a person who works in an organisation to ensure that the business complies with data protection laws. Not all organisations have DPOs, but some have to by law, especially those who process special categories of data. The DPO is responsible for monitoring data protection compliance, keeping you informed about our data protection obligations, and providing any necessary advice for remaining compliant at all times.

Data Protection Principles

Seven key principles set out by the GDPR that should lie at the heart of any approach to processing personal data: Lawfulness, fairness and transparency, Purpose

limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.

Data Security

Data security is the term used for how digital data is protected from the unwanted actions of unauthorized users, including cyber-attacks and data breaches.

Data Subject

A data subject is any person to whom data can be attributed and, thus, falls under the jurisdiction of existing data protection laws. Subjects could include a customer, an employee, a third-party contact or any individual with whom a data controller interacts.

DPA 2018

Data Protection Act 2018

EDPS

The EDPS or European Data Protection Supervisor is an EU-level public body that ensures that institutions within the EU respect EU citizens' right to privacy and data protection while processing their data. The body is made up of representatives from member state national data protection institutions.

Encryption

Encryption is a mathematical operation to encode data in such a way that it can only be accessed by authorised users. Article 32 of the GDPR includes encryption as an example of an appropriate technical measure.

Fairness Principle

A principle states that a data controller should put in place facilities that enable the data subject to exercise rights about their data. Under the fairness principle, data controllers could include facilities that provide access, rectification and erasure of the data as well as those that allow the subject to place restrictions on processing or transferring the data from one controller to another.

GDPR

The General Data Protection Regulation (GDPR) is an EU law that concerns the privacy and data protection of all citizens in the EU and the European Economic Area (EEA).

Genetic Data

Any data that describes the biological characteristics of a subject at the level of DNA. Genetic information, for instance, could include a person's entire genome, their genetic markers, DNA information that can identify them, or information related to their characteristics or disease status.

Legality Principle

A legal paradigm states that organisations should only use personal data on the grounds specified by GDPR. The legitimate use of data includes situations in which an individual gives their consent, there is a contract with the individual, or using data allows the organisation to comply with an existing legal obligation.

Member States

Countries that are part of the European Economic Area (or European Union) and subject to GDPR.

Minimisation Principle

Data processors should keep as little information on data subjects as possible and only collect data that they require for their processing. They should not seek out additional data that is not necessary for them to carry out their objectives.

Natural Person

A natural person refers to an entity under the law classified as a human being. A non-natural person under the law could refer to an organisation, public or private, sometimes called a legal person.

One-Stop-Shop

Many businesses have locations across several EU Member States. The One-Stop-Shop concept allows companies to deal with the lead GDPR regulator in their home country, not all regulators in all countries in which they operate.

Parental Consent

In the UK, only children aged 13 or over can provide their consent for processing their data. Under this age, it is necessary to obtain consent from whoever holds parental responsibility for them.

Personal Data

Personal data includes any data that a third party could use to verify the identity of the data subject - the person to whom the data refers. It could consist of bank details, phone, numbers, addresses, names, photos or data gleaned from social networks.

Personal Data Breach

An event in which a subject's data is somehow lost, stored, disclosed or transmitted in a way that contravenes the GDPR. Personal data breaches can be either accidental or deliberate.

Principles of Data Protection

A set of basic statements describing the spirit and purpose of the GDPR. The principles also set out the main objectives of the regulations and the mission of the public bodies that will enforce them across the EU.

Privacy by Design

A concept whereby organisations build privacy into their processes from the outset, reducing the likelihood of a data breach in the future. Privacy by design, for instance, could involve the development of technical systems that better protect subject data compared to existing protocols ahead of time, rather than waiting for a data breach to make changes.

Privacy Impact Statement

GDPR rules state that data controllers must create a privacy impact statement (also called a Data Protection Impact Assessment) whenever processing data that might present a privacy risk. Data processing could be a privacy risk because of its purposes, scope or nature.

Privacy Notice

A privacy notice is a document in which a data controller tells people what they'll be doing with their data whom they'll share it with, etc.

Privacy Shield

The EU-US Privacy Shield is a scheme that is deemed by the European Commission to provide adequate protection to allow personal data to be transferred to entities in the United States that are registered under this scheme.

Profiling

Profiling is a tool that attempts to use patterns in data to discern secondary information about a subject. Companies often use profiling to analyse employee behaviour, preferences or capacity to perform reliably at work.

Pseudonymisation

A process that permits the processing of data such that the contents can no longer be traced back to the original data subject without the use of additional information. Organisations and data controllers who use pseudonymisation often keep identifiable and non-identifiable data separately.

Purpose Limitation Principle

Data processors should only collect data for explicit, legitimate reasons and not use it in further ways that are not compatible with the initial purpose.

Rectification

The correction and/or completion of inaccurate or incomplete data.

Regulation (EU) 2016/679

The official regulation code for the EU General Data Protection Regulation (GDPR) was approved by the European Parliament and Council on April 27, 2016. GDPR applies to member states without the need for national legislation implementation.

Restricted Transfers

GDPR puts in place restrictions for any organisation wanting to transfer data outside of the EEA. The rules define transfer as both the physical transportation of data outside of the EEA and also remote viewing of EU data subjects' data by international third parties, for example by digital means.

Restriction on Processing

The act of marking stored data to prevent the further use or processing of that data in the future. A data controller, for instance, might restrict processing, if he or she believes that further use of the data might put the privacy of the owner at risk.

Right to Access

Data subjects have the right to access all the data that we hold on them. Such a request is called a Subject Access Request (SAR). It can be given to us verbally or in writing on paper or any online channel.

Right to be Forgotten

See Right to Erasure.

Right to be Informed

Data subjects have the right to be informed about the purpose for which we are holding and processing their data. This is typically done with a privacy notice.

Right to Data Portability

Data subjects have the right to data portability - ie to obtain a copy of their data in a standard format, even if they are moving it to one of our competitors.

Right to Erasure

Data subjects have the right to the erasure of their data (also known as the right to be forgotten) unless we have a legitimate interest in holding the data.

Right to Object

If the data subject doesn't want their data to be used for a certain purpose - e.g. profiling - they have the right to object.

Right to Rectification

Data subjects have the right to rectify any inaccurate or incomplete data.

Right to Restrict Processing

In addition to the right to erasure, data subjects also have the right to restrict processing, whereby we may store the data but have to refrain from processing it.

Rights on Automated Decision-Making & Profiling

Data subjects also have rights concerning automated decision-making and profiling.

Sensitive Personal Data

Any form of personal data that the GDPR consider uniquely special or sensitive. These data include information relating to religious affiliation, sexual orientation, ethnic and racial origins, trade union membership, and biometric/DNA data that could identify a person.

Storage Limitation Principle

The storage limitation principle states that data controllers must only retain information for as long as they need it for processing purposes. Data controllers should not keep personal data for longer than is necessary. Long-term storage is only permitted for public interest archiving or statistical research purposes.

Subject Access

GDPR rules state that subjects have the right to access their data held by a data controller. A subject can request a data controller to give them access to any personal data that they hold.

Subject Access Request (SAR)

A subject access request is a request for access made by the data subject. The GDPR does not specify how to make a valid request. Therefore, it could be verbal or in writing. It can be made to any part of the organisation - it does not have to be to a specific person or contact point. It doesn't even need to formally say 'subject access request'. As long as it is clear that the individual is asking for their data, the organisation needs to recognise it as a SAR and respond to it within one month. Unless the request is manifestly unfounded excessive or repetitive, the organisation cannot charge a fee.

Supervisory Authority

See Data Protection Authority

Territorial Scope

The term territorial scope refers to the geographic region over which the EU GDPR rules apply. Currently, GDPR encompasses the European Economic Area (EEA), which includes all current 27 EU member states. It also covers additional territories, including Norway, Lichtenstein and Iceland. It does not include Switzerland.

Third-Party

In the context of GDPR, a third party is any person who legitimately interacts with protected data and is neither a data subject nor a data controller. Third parties receive authorisation to process or view data from either the data controller or the data subject.

Transparency Principle

The notion is that data controllers should give data subjects data on request that is accessible, understandable, intelligible and provided in written form. Thus, data subjects should be able to understand the data the organisations or data controllers have about them and be able to make requests based on those data.

Vulnerable Customers

Customers who are more vulnerable than others, for example, due to their state of mental capacity, or having been diagnosed with a terminal illness. The category and level of data that a firm could now hold on a customer, could far exceed their original expectations and be far more reaching into the personal life of the customer than they initially had established data storage and retention controls for.

Source: https://www.skillcast.com/gdpr-definitions

17) BIBLIOGRAPHY

About | European Data Protection Supervisor. (n.d.). Retrieved February 18, 2022, from https://edps.europa.eu/about-edps_en

ABOUT US - European DIGITAL SME Alliance. (n.d.). Retrieved February 11, 2022, from https://www.digitalsme.eu/about-us/

Accenture-cross-border-the-disruptive-frontier.pdf. (n.d.). Retrieved February 20, 2022, from https://www.accenture.com/_acnmedia/pdf-102/accenture-cross-border-the-disruptive-frontier.pdf

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Aleksandra, D. (2018, September 26). *SEO Trubunal Google Facts*. Seotribunal.Com. https://seotribunal.com/blog/google-stats-and-facts/

Amadeo, K. (2022). *What Is Competitive Advantage?* The Balance. https://www.thebalancemoney.com/what-is-competitive-advantage-3-strategies-that-work-3305828

Anand, G., Larson, E. C., & Mahoney, J. T. (2020). Thomas Kuhn on paradigms. *Production and Operations Management*, *29*(7), 1650–1657.

Apple and Google partner on COVID-19 contact tracing technology. (n.d.). Apple Newsroom. Retrieved February 20, 2022, from https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Armstrong, K. A. (2018). Regulatory alignment and divergence after Brexit. *Journal of European Public Policy*, *25*(8), 1099–1117.

Art. 4 GDPR – Definitions. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved February 18, 2022, from https://gdpr-info.eu/art-4-gdpr/

Art. 48 GDPR – Transfers or disclosures not authorised by Union law. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved February 18, 2022, from https://gdpr-info.eu/art-48-gdpr/

Austin, J. (1875). *... Lectures on Jurisprudence: Or, The Philosophy of Positive Law*. J. Murray.

Barnard-Wills, D. D., Cochrane, L., Matturi, M. K., & Marchetti, D. F. (2019). *Report on the SME experience of the GDPR*. 55.

Boswell, J. (1851). *The Life of Samuel Johnson: Including a Journal of a Tour to the Hebrides* (Vol. 1). Harper & Brothers.

Boyle, F. A. (1985). *World politics and international law*. Duke University Press.

Brodin, M. (2019a). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research*, *4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Brodin, M. (2019b). A Framework for GDPR Compliance for Small-and Medium-Sized Enterprises. *European Journal for Security Research*, *4*(2), 243–264.

Buckley, G., Caulfield, T., & Becker, I. (2021). "It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years. *ArXiv:2110.11905 [Cs]*. http://arxiv.org/abs/2110.11905

Burley, A.-M. S. (2017). International law and international relations theory: A dual agenda. *The Nature of International Law* (pp. 11–46). Routledge.

Campbell, J. D., Goldfarb, A., & Tucker, C. E. (2015). *Privacy Regulation and Market Structure* (SSRN Scholarly Paper ID 1729405). Social Science Research Network. https://doi.org/10.2139/ssrn.1729405

CJEU - Joined cases C 203/15 and C 698/15—Tele2/Watson. (n.d.). GDPRhub. Retrieved February 18, 2022, from https://gdprhub.eu/index.php?title=CJEU_-_Joined_cases_C_203/15_and_C_698/15_-_Tele2/Watson

COVID-19 and European small businesses | McKinsey. (n.d.). Retrieved February 20, 2022, from https://www.mckinsey.com/industries/public-and-social-sector/our-insights/covid-19-and-european-small-and-medium-size-enterprises-how-they-are-weathering-the-storm

CURIA - List of results. (n.d.). Retrieved February 20, 2022, from https://curia.europa.eu/juris/liste.jsf?num=c-131/12

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12 (ECJ April 8, 2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

Digital_Decade_Targets_2030_DIGITAL_SME_Consultation_Response.pdf. (n.d.). Retrieved February 11, 2022, from https://www.digitalsme.eu/digital/uploads/Digital_Decade_Targets_2030_DIGITAL_SME_Consultation_Response.pdf

Dimson, J., Mladenov, Z., Sharma, R., & Tadjeddine, K. (2020). COVID-19 and European small and medium-sized enterprises: How they are weathering the storm. *McKinsey & Company*.

DMA survey highlights gaps in SME GDPR knowledge and compliance | News. (n.d.). Research Live. Retrieved February 10, 2022, from http://www.research-live.com/article/news/dma-survey-highlights-gaps-in-sme-gdpr-knowledge-and-compliance/id/5065862

EC COM 2017. (n.d.). Retrieved February 11, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0495&from=NL

EDPS Answers to French Senate. (n.d.). Retrieved February 20, 2022, from https://edps.europa.eu/sites/edp/files/publication/20-04-27_edps_qa_fr_senate_en.pdf

Egress-research-report-gdpr-compliance.pdf. (n.d.). Retrieved February 11, 2022, from https://www.egress.com/media/v3xflemb/egress-research-report-gdpr-compliance.pdf

EU DSM Report. (2017). *Europe's Digital Progress Report 2017* [Text]. Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2017

EU: GDPR compliance spending in small businesses 2019. (n.d.). Statista. Retrieved February 11, 2022, from https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/

EU Research. (n.d.). *Digital economy and society in the EU - What is the digital single market about?* Digital Technologies and in Particular the Internet Are Transforming Our World and the European Commission Wants to Make the EU's Single Market Fit for the Digital Age – Moving from 28 National Digital Markets to a Single One. Retrieved February 20, 2022, from http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

Europe – Google Impact Report. (n.d.). Retrieved February 20, 2022, from https://googleimpactreport.publicfirst.co.uk/europe/

Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, *16*(3), 349–391.

GDP growth (annual %) | Data. (n.d.). Retrieved February 16, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG

GDPR Readiness Survey for Software and SMEs | ECOMPLY.io. (n.d.). Retrieved February 10, 2022, from https://www.ecomply.io/blog-en/gdpr-readiness-survey-software-and-smes

Gdpr_survey.pdf. (n.d.). Retrieved February 10, 2022, from https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/gdpr_survey.pdf?la=en

Goasduff, L. (2022). Data Sharing is a Key Digital Transformation Capability. *Gartner*. https://www.gartner.com/smarterwithgartner/data-sharing-is-a-business-necessity-to-accelerate-digital-business

Goldsmith, J. L., & Wu, T. (n.d.). Who Controls the Internet?, at xii (2006); Orin S. *Kerr, The Problem of Perspective in Internet Law*, *91*, 359–361.

Govindarajan, V., Srivastava, A., & Enache, L. (2020). Understanding India's Chilly Reception of Jeff Bezos. *Harvard Business Review*. https://hbr.org/2020/01/understanding-indias-chilly-reception-of-jeff-bezos

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Research*, *2*(163–194), 105.

Gudeta, Y. (2023). The Impact of Data and AI on a Modern Business. *Databricks*. https://www.databricks.com/blog/2023/01/10/impact-data-and-ai-modern-business.html

Hakimi, M. (2020). *The Integrative Effects of Global Legal Pluralism*.

Hallinan, D., De Hert, P., & Leenes, R. (2022). *Data Protection and Privacy, Volume 14: Enforcing Rights in a Changing World*. Bloomsbury Publishing.

Hazen, B. T., Boone, C. A., Ezell, J. D., & Jones-Farmer, L. A. (2014). Data quality for data science, predictive analytics, and big data in supply chain management: An introduction to the problem and suggestions for research and applications. *International Journal of Production Economics*, *154*, 72–80.

Heiman, M. R. (2019). The GDPR and the consequences of big regulation. *Pepp. L. Rev.*, *47*, 945.

Hofheinz, P., & Mandel, M. (2014). Bridging the data gap: How digital innovation can drive growth and create jobs. *Lisbon Council-Progressive Policy Institute Policy Brief*, *15*, 2014.

How To Balance Personalization With Data Privacy. (n.d.). Gartner. Retrieved February 17, 2022, from https://www.gartner.com/smarterwithgartner/how-to-balance-personalization-with-data-privacy

HRSolutions-SME-Challenges-Post-Covid19-Results.pdf. (n.d.). Retrieved February 20, 2022, from https://www.hrsolutions-uk.com/wp-content/uploads/2020/12/HRSolutions-SME-Challenges-Post-Covid19-Results.pdf

International funds focused on tech giants excel; should you invest in global MFs? (n.d.). Retrieved February 20, 2022, from https://www.moneycontrol.com/news/business/personal-finance/international-funds-focused-on-tech-giants-excel-should-you-invest-in-global-mfs-5319581.html

Ivankova, N. V., & Creswell, J. W. (2009). Mixed methods. *Qualitative Research in Applied Linguistics: A Practical Introduction*, *23*, 135–161.

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R., & Barnard-Wills, D. (2021). *The GDPR made simple (r) for SMEs*. ASP editions-Academic and Scientific Publishers.

Kelle, U., & Erzberger, C. (2003). *Making inferences in mixed methods: The rules of integration*. Sage: Thousand Oaks, CA, USA.

Kelly, B. (2020). Future of Sales 2025: Why B2B Sales Needs to Shift to Data-Driven Selling. *Gartner*. https://www.gartner.com/smarterwithgartner/future-of-sales-2025-data-driven-b2b-selling

Krasteva, S., Sharma, P., & Wagman, L. (2015). The 80/20 rule: Corporate support for innovation by employees. *International Journal of Industrial Organization*, *38*, 32–43.

Krisch, N., & Kingsbury, B. (2006). Introduction: Global governance and global administrative law in the international legal order. *European Journal of International Law*, *17*(1), 1–13.

Landreau, I. (2019). The Legal Basis for a Data Economy Based on Trust. *Augmented Customer Strategy: CRM in the Digital Age*, 241–255.

Layton, R. (n.d.). *The 10 Problems of the GDPR*. 19.

Li, H., Yu, L., & He, W. (2019). *The impact of GDPR on global technology development*. Taylor & Francis.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47–64.

Mann, F. A. (1984). *The doctrine of international jurisdiction was revisited after twenty years*. Martinus Nijhoff.

Martin, J. S., Marks, C. P., & Barnes, W. (2016). The Uniform Commercial Code Survey: Introduction. *Bus. Law.*, *72*, 1057.

Mason, A. D., & Shetty, S. (2019). *Developing East Asia: Retrospect and Prospects*.

Michaels, R. (2013). Globalization and law: Law beyond the state. *Law and Social Theory (Banakar & Travers Eds., Oxford, Hart Publishing, 2013), Forthcoming*.

Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, *1*(1), 48–76.

Morgan, S. (2022). Top 10 Cybersecurity Predictions and Statistics For 2023. *Cybercrime Magazine*. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

Overbeek, H., Dingwerth, K., Pattberg, P., & Compagnon, D. (2010). Global governance: Decline or maturation of an academic concept? *International Studies Review*, *12*(4), 696–719.

Parylo, O. (2012). Qualitative, quantitative, or mixed methods: An analysis of research design in articles on principal professional development (1998–2008). *International Journal of Multiple Research Approaches*, *6*(3), 297–313.

Porter, M. E. (1985). Technology and competitive advantage. *Journal of Business Strategy*, *5*(3), 60–78.

Position-Paper-GDPR-Review-2020.pdf. (n.d.). Retrieved February 19, 2022, from https://www.digitalsme.eu/digital/uploads/Position-Paper-GDPR-Review-2020.pdf

Press, G. (2016). Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says. *Forbes*.

https://www.forbes.com/sites/gilpress/2016/03/23/data-preparation-most-time-consuming-least-enjoyable-data-science-task-survey-says/

Press, G. (2020). *54 Predictions About The State Of Data In 2021*. Forbes. https://www.forbes.com/sites/gilpress/2021/12/30/54-predictions-about-the-state-of-data-in-2021/

Publisher's Terms of Use and Privacy Policy—Pollfish. (n.d.). Retrieved February 20, 2022, from https://www.pollfish.com/terms/publisher

Raynard, M., Johnson, G., & Greenwood, R. (2015). Institutional theory and strategic management. *Advanced Strategic Management: A Multi-Perspective Approach*, 9–34.

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *REGULATION (EU)*, *679*, 2016.

Slaughter, A.-M., Tulumello, A. S., & Wood, S. (1998). International law and international relations theory: A new generation of interdisciplinary scholarship. *American Journal of International Law*, *92*(3), 367–397.

Social Media Captures Over 30% of Online Time. (2017, September 11). GWI. https://blog.gwi.com/chart-of-the-day/social-media-captures-30-of-online-time/

Star II project. (n.d.). *Star2project.Eu*. Retrieved February 13, 2022, from https://star-project-2.eu/star-ii-project/

Steffek, J., Kissling, C., & Nanz, P. (2007). *Civil society participation in European and global governance: A cure for the democratic deficit?* Springer.

Strategic Research. (n.d.). *Deloitte 360 Global Survey of Data Business*. Retrieved February 20, 2022, from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-director-360-growth-from-all-directions-third-edition.pdf

Suominen, K. (2017). Fuelling trade in the digital era: Policy roadmap for developing countries. *Geneva, Switzerland: International Centre for Trade and Sustainable Development (ICTSD)*.

Tashakkori, A., & Creswell, J. W. (2007). The new era of mixed methods. In *Journal of mixed methods research* (Vol. 1, Issue 1, pp. 3–7). Sage Publications.

Teixeira, G. A., da Silva, M. M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*.

Trend Micro Survey on GDPR. (n.d.). Retrieved February 20, 2022, from https://www.trendmicro.com/vinfo/pl/security/news/online-privacy/the-general-data-protection-regulation-gdpr-highlights-privacy-in-the-digital-age

Vlcek, W. (2017). Multinational Corporations and the Digital Economy. In *Offshore Finance and Global Governance* (pp. 43–70). Springer.

Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, Joined cases C-92/09 and C-93/09 (ECJ November 9, 2010). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092

Vollmer, N. (2021, July 2). *Recital 14 EU General Data Protection Regulation (EU-GDPR)* [Text]. SecureDataService. https://www.privacy-regulation.eu/en/recital-14-GDPR.htm

WHO Coronavirus (COVID-19) Dashboard. (n.d.). Retrieved February 20, 2022, from https://covid19.who.int

Yoshino, N., & Taghizadeh Hesary, F. (2016). *Major challenges facing small and medium-sized enterprises in Asia and solutions for mitigating them*.

Zhong, W., Makridis, C. A., & Diddams, J. (2020). Emergency Executive Powers: Not Needed Indefinitely. *Mercatus Special Edition Policy Brief*.