Privacy Concerns in Cloud Computing: Consumer Data and Compliance Issues in the IT Sector in Ireland

# Abstract

This research focuses on the privacy and data security concern of cloud computing present in the Ireland IT industry, the assessment of GDPR conformance and the impact of consumer trust in cloud technologies. These key risk areas reveal traditional threats like data loss, unauthorized access, and improper configurations, as well as contemporary threats including ransomware and phishing attacks. Lack of clarity in cross-border data transfer and shared responsibility were reported to hinder effective protection of data under GDPR compliance. Consumer trust is also underlined as well as the importance of cooperation with Cloud Service Providers (CSPs) based on clear Service-Level Agreements (SLAs) and security assessment check-ups. Also worth mentioning is that AI, ML, and blockchain were discovered to have the capacity to both improve and exacerbate cloud privacy. The solutions also entail the implementation of technical controls, better regulatory frameworks, and enhanced cooperation between organizations and CSPs. The findings of this research can be useful for stakeholders to improve the privacy of data and build credibility for cloud solutions.

**Contents**

[Abstract 2](#_gjdgxs)

[Table of Figures 8](#_1fob9te)

[Chapter 1: Introduction 9](#_3znysh7)

[1.1 Research Background 9](#_2et92p0)

[1.2 Problem Discussion 12](#_tyjcwt)

[1.2.1 Problem Statement 13](#_3dy6vkm)

[1.3 Research Rationale 13](#_1t3h5sf)

[1.4 Hypotheses 15](#_4d34og8)

[1.5 Aims and Objectives 16](#_2s8eyo1)

[1.5.1 Aim 16](#_17dp8vu)

[1.5.2 Objectives 16](#_3rdcrjn)

[1.6 Structure of the Dissertation 16](#_26in1rg)

[1.7 Conclusion 17](#_lnxbz9)

[Chapter 2: Literature Review 18](#_35nkun2)

[2.1 Introduction 18](#_1ksv4uv)

[2.2 Evolution of Cloud Computing 18](#_44sinio)

[2.3 Benefits of Cloud Computing in the IT Sector 20](#_2jxsxqh)

[2.4 Privacy Concerns in Cloud Computing 23](#_z337ya)

[2.5 Regulatory Framework for Cloud Privacy 25](#_3j2qqm3)

[2.6 Cybersecurity Threats and Cloud Data Protection 28](#_1y810tw)

[2.7 Consumer Trust and Cloud Adoption 30](#_4i7ojhp)

[2.8 Industry Best Practices for Data Privacy and Compliance 32](#_2xcytpi)

[2.9 Literature Gap 33](#_1ci93xb)

[2.10 Conceptual Framework 34](#_3whwml4)

[Chapter 3: Methodology 35](#_2bn6wsx)

[3.1 Introduction 35](#_qsh70q)

[3.2 Research Philosophy 35](#_3as4poj)

[3.3 Research Design 36](#_1pxezwc)

[3.4 Sampling Strategy 37](#_49x2ik5)

[3.5 Data Collection Methods 38](#_2p2csry)

[3.6 Data Analysis Methods 39](#_147n2zr)

[3.7 Ethical Considerations 40](#_3o7alnk)

[3.8 Reliability and Validity 41](#_23ckvvd)

[3.9 Limitations of the Methodology 42](#_ihv636)

[3.10 Summary 43](#_32hioqz)

[Chapter 4: Results and Analysis 44](#_1hmsyys)

[4.1 Introduction 44](#_41mghml)

[4.2 Results 44](#_2grqrue)

[4.2.1 Theme 1: Privacy Risks and Consumer Trust in Cloud Environments 44](#_vx1227)

[4.2.2 Theme 2: Challenges in Compliance with GDPR and Data Protection Regulations 46](#_3fwokq0)

[4.2.3 Theme 3: Cybersecurity Threats and Mitigation Strategies 48](#_1v1yuxt)

[4.2.4 Theme 4: Role of Cloud Service Providers in Addressing Privacy Concerns 50](#_4f1mdlm)

[4.2.5 Theme 5: Emerging Technologies and Their Impact on Cloud Privacy and Security 51](#_2u6wntf)

[4.3 Analysis 53](#_19c6y18)

[4.3.1 Privacy Risks and Trust 53](#_3tbugp1)

[4.3.2 Compliance Challenges 54](#_28h4qwu)

[4.3.3 Cybersecurity Threats 55](#_nmf14n)

[4.3.4 CSP Collaboration 56](#_37m2jsg)

[4.3.5 Emerging Technologies 57](#_1mrcu09)

[4.4 Summary of the Chapter 58](#_46r0co2)

[Chapter 5: Discussion 59](#_2lwamvv)

[5.1 Introduction 59](#_111kx3o)

[5.2 Alignment with the Research Objectives 59](#_3l18frh)

[5.2.1 Objective 1: To identify the key privacy and data security risks, including potential data leakage, associated with cloud computing in Ireland. 59](#_206ipza)

[5.2.2 Objective 2: To evaluate the effectiveness of current legal frameworks, particularly GDPR, in addressing these data security and privacy risks. 60](#_4k668n3)

[5.2.3 Objective 3: To assess the role of consumer trust in the adoption of cloud services amid concerns of data security and leakage. 61](#_2zbgiuw)

[5.2.4 Objective 4: To provide recommendations for organizations to enhance data protection practices, prevent consumer data leakage, and comply with privacy regulations. 61](#_1egqt2p)

[5.3 Contrast and Comparison of Literature Review and Findings 62](#_3ygebqi)

[5.3.1 Privacy Risks 62](#_2dlolyb)

[5.3.2 GDPR and Legal Framework 63](#_sqyw64)

[5.3.3 Consumer Trust 63](#_3cqmetx)

[5.3.4 Emerging Technologies 64](#_1rvwp1q)

[5.4 Implications of Findings 64](#_4bvk7pj)

[5.5 Limitations of the Study 65](#_2r0uhxc)

[5.6 Conclusion 66](#_1664s55)

[Chapter 6: Conclusion and Recommendations 67](#_3q5sasy)

[6.1 Introduction 67](#_25b2l0r)

[6.2 Summary of Key Findings 67](#_kgcv8k)

[6.2.1 Privacy and Data Security Risks 67](#_34g0dwd)

[6.2.2 Compliance Challenges 68](#_1jlao46)

[6.2.3 Cybersecurity Threats 68](#_43ky6rz)

[6.2.4 CSP Collaboration 69](#_2iq8gzs)

[6.2.5 Emerging Technologies 69](#_xvir7l)

[6.3 Contributions of the Study 70](#_3hv69ve)

[6.3.1 Theoretical Contributions 70](#_1x0gk37)

[6.3.2 Practical Contributions 70](#_4h042r0)

[6.4 Recommendations 71](#_2w5ecyt)

[6.4.1 Recommendations for Organizations 71](#_1baon6m)

[6.4.2 Recommendations for Policymakers 72](#_3vac5uf)

[6.4.3 Recommendations for Cloud Service Providers (CSPs) 72](#_2afmg28)

[6.5 Final Conclusion 73](#_pkwqa1)

[References 75](#_39kk8xu)

[Appendices 86](#_1opuj5n)

[Appendix 1: Interview Questions 86](#_48pi1tg)

# Table of Figures

[Figure 1: Privacy Risks and Consumer Trust in Cloud Environments 41](#_1302m92)

[Figure 2: Challenges in Compliance with GDPR and Data Protection Regulations 43](#_3mzq4wv)

[Figure 3: Cybersecurity Threats and Mitigation Strategies 45](#_2250f4o)

# Chapter 1: Introduction

## 1.1 Research Background

Cloud computing has revolutionalised the IT industry and is now a fundamental part of many organizations and personal computing environments. Promising numerous advantages including lower costs, scalability, flexibility, and improved collaboration it has changed the approach to data storage and retrieval. The convenience of on-demand computing resources, scope of application, and minimum capital investment have made cloud computing a necessity for modern rapidly developing digital world. The cloud computing market size is estimated to value at US$ 405,295.8 million in 2022 and reach US$ 1,465,818.2 million by 2028; it is expected to grow at a CAGR of 23.9% from 2022 to 2028 (The Insight Partners, 2023). This phenomenal growth is because most businesses are migrating to the cloud due to drivers such as digitalization, work-from-home policies and real-time access to information.

Specifically, cloud computing adoption in Ireland has been quite active, thanks to the first-class IT industry and the state’s focus on digital transformation. Cloud solutions have become a popular tool in financial services, healthcare, retail and technology companies as a way of enhancing their operations and the experiences of their customers for increased revenue. The increase in the adoption of cloud services has been driven by Ireland’s status as a European technology market along with a thriving data centre market. The report also shows that the market of cloud computing in Ireland is expected to increase by more than 5.4 billion US dollars (+132.67%) over the next five years while companies continue moving to cloud solutions to stay relevant and adaptable (Statista, 2020).

However, as the use of cloud computing expands, so does the problem of data protection and security. Cloud environments by their nature include storing information within a cloud service provider’s servers, which might be in different regions with different levels of data protection legislation. This is a big problem for organizations, especially for those that work within industries that are heavily regulated such as financial services and healthcare. When Irish organisations are implementing cloud solutions, they are faced with numerous legal and regulatory issues that need to be complied with about data protection laws while at the same time having to deal with growing threats from cyber criminals (Carcary et al., 2014).

Ireland being part of the European Union follows the GDPR, which is one of the most rigorous and extensive data protection laws globally. The GDPR which started being implemented in May 2018 set high standards on how organizations handle personal data including that which is stored in the cloud. The regulation requires companies to apply suitable technical and organizational measures for the protection of personal data and the free movement of data. Noncompliance with the GDPR attracts stiff penalties which are fines up to 4% of the company’s total annual global turnover or €20 million, whichever is greater (GDPR, 2018). Consequently, GDPR has become a major challenge to companies in the Irish IT sector especially those that use cloud services in meeting this challenge while dealing with the emerging issue of data privacy.

The Irish Data Protection Commission (DPC) (2022) has pointed out that it has received more complaints regarding data privacy breaches after GDPR implementation with a 20% increase in the complaints in 2022 than in the past three years. Many of these complaints are related to cloud service providers, thus indicating the current problems organizations experience in protecting cloud data (The Irish Data Protection Commission, 2022). The fact that cloud data storage is global and the specific nature of cloud service contracts has made it progressively challenging for firms to guarantee that consumer data is secure and that they are in complete compliance with the GDPR.

In addition to compliance, security issues are a critical problem in the context of cloud computing environments. Since more and more organizations are moving their data to the cloud, the threat of cyberattacks still rises and cases of data breaches, ransomware attacks, and unauthorized access. A recent report on Ireland found that 75% of organizations suffered at least one cyber-attack in the last year, with many of these targeting cloud solutions (PricewaterhouseCoopers, 2023). This shows how cloud infrastructures are exposed to cyber threats and should be of great concern to the security measures currently in place.

Perhaps the most threatening development of recent years is the increasing number of ransomware attacks on cloud service providers. Ransomware is a form of malware that encrypts a victim’s data and then demands a ransom for the decryption of the data and this has now become common in cloud environments. According to the Computer Security Incident Response Team (CSIRT) in 2023, ransomware attacks on cloud-based structures were rife, leading to huge losses and major organizational shocks (O’Dowd, 2023). Besides, it may hurt the company’s financial and operational performances and, more importantly, it reshapes consumer confidence in cloud services.

Since consumer trust is an essential factor in the uptake and sustained use of Cloud computing services, the increasing cases of data breaches and cyber-attacks pose a serious threat to the public’s confidence. Irish consumers’ attitude towards cloud services revealed that they are concerned about the privacy of their data and many of them have fears that their data might be used in the wrong way or perhaps accessed by the wrong people (Sisodia et al., 2024). This reluctance in the adoption of cloud solutions is felt most keenly with the older consumer and where the data security concerns are higher such as in the health care and financial services industries. Consumer distrust does not only impact the CSPs’ image but also slows down the development of cloud technologies in Ireland.

## 1.2 Problem Discussion

As cloud computing is becoming even more popular, there are a lot of issues concerning the confidentiality and protection of consumer data. Cloud services work by uploading data to remote servers that are located far from the user with the help of third-party service providers which poses a high risk of the exposure of sensitive information to hacking, unauthorized access, and loss of data. This is compounded by the fact that cloud data storage is cross-border in nature as data may be stored in countries that do not follow the same legal and regulatory framework as the organizations seeking to comply with GDPR and other privacy regulations (Han, 2011).

Another one of the main threats of cloud computing is data leakage where the data is accessed by an unauthorized person. This can be a result of misconfiguration, poor security measures or holes in the cloud infrastructure (Al-Ali, 2017). Such data leakages also lead to monetary loss to the business organizations, but the worst effect that they have on the organizations is loss of reputation which leads to loss of consumers. For instance, a massive cyber-attack on one of Ireland’s leading cloud service providers leaked the details of thousands of consumers to hackers and caused an enormous public outcry.

One more crucial question is the question of the policy that cloud service providers use to manage and store the consumer’s data. Most consumers have no idea where their data is being hosted, to whom this data belongs, and how it is being utilized. This lack of transparency is a cause for increasing anxiety regarding privacy as customers never know what is being done with their data and who may be getting their approval to get entry to it. According to A survey conducted in 2023 among Irish consumers, 63% of them are worried about the amount of control they have over their data when using cloud services (Accenture, 2023).

Another factor contributing to privacy risks in cloud computing is the advancement in the type of attacks; ransomware and phishing attacks. This is because cybercriminals are always devising new ways through which they will attack cloud systems, and organizations are in most times unable to cope up with the new developments. According to the Irish Computer Security Incident Response Team (CSIRT) in 2023, ransomware attacks on cloud service providers of the Irish business were identified as having caused extensive data and monetary losses (O’Dowd, 2023).

### 1.2.1 Problem Statement

The increasing privacy concerns in cloud computing pose significant risks to consumer trust and the adoption of cloud services in Ireland’s IT sector.

## 1.3 Research Rationale

The rationale for this research is driven by the growing concern over the vulnerability of individuals’ personal data in today’s digital landscape, particularly in light of the rapid adoption of cloud computing. As businesses increasingly rely on cloud services for storage, processing, and data management, concerns around data privacy and security have become more pronounced. Cloud computing, while offering scalability, flexibility, and cost efficiency, also introduces significant risks related to data protection (Han, 2011). These risks are particularly critical in jurisdictions such as Ireland, where the General Data Protection Regulation (GDPR) has set stringent rules for data handling, requiring organizations to not only ensure compliance with legal obligations but also to align with the evolving privacy expectations of customers (Hjerppe et al., 2019). With organizations facing the dual challenge of maintaining business efficiency and safeguarding consumer privacy, this research is essential in exploring how companies can effectively navigate these issues.

A key motivation for this study is the increasing frequency and severity of data breaches, security incidents, and privacy violations associated with Cloud Service Providers (CSPs). Such breaches are not merely an inconvenience but can lead to substantial financial losses, damage to brand reputation, and legal consequences for organizations. More critically, these incidents erode consumer trust in digital services, leading to hesitations or reluctance in adopting cloud technologies. According to Puljak et al. (2020), the impact of data breaches on consumer trust is profound, with many individuals growing more skeptical about sharing personal data online. This mistrust can hinder the broader adoption of cloud computing technologies and undermine the growth potential of the digital economy. Therefore, understanding the nature of privacy threats in cloud computing and offering actionable recommendations for businesses to improve data protection is critical to addressing these challenges. This research aims to identify the specific privacy threats tied to cloud services, including potential vulnerabilities in data storage, transmission, and access, and propose practical measures to mitigate these risks (Hjerppe et al., 2019).

Furthermore, this study seeks to make a significant contribution to the existing body of knowledge by focusing on the Irish IT sector, which presents a unique set of circumstances. Ireland has become a global hub for multinational tech companies, with many organizations adopting cloud solutions to streamline their operations. However, these companies also face distinct challenges due to Ireland’s regulatory framework, which is heavily influenced by EU directives such as GDPR. While GDPR sets a clear standard for data protection, the application of these regulations in the context of cloud computing introduces complexities, particularly regarding cross-border data transfers and multi-jurisdictional compliance (Annan and Filippaios, 2017). Despite the growing importance of cloud security, much of the academic literature has been focused on broader global trends or case studies from larger markets, offering limited insights into the specific challenges faced by organizations in smaller, yet highly regulated, jurisdictions such as Ireland. By focusing on the Irish market, this research aims to bridge this gap in the literature and provide targeted insights into how Irish organizations can address cloud security challenges while ensuring GDPR compliance (Hjerppe et al., 2019).

Besides, the results of this study will be useful for policymakers and top managers in improving the protection of personal data and enhancing the trust of users in cloud solutions. Through the analysis of the gathered data and the provision of policy suggestions, this research should provide a contribution to the continuous improvement of data privacy in Ireland’s IT industry.

## 1.4 Hypotheses

1. Organizations in Ireland’s IT sector is not fully compliant with GDPR and other legal frameworks concerning cloud data privacy.
2. Consumers are hesitant to adopt cloud services due to concerns over data privacy and security.
3. Enhanced security measures and stronger legal compliance can significantly improve consumer trust in cloud computing services.

## 1.5 Aims and Objectives

### 1.5.1 Aim

The aim of this research is to investigate data security and privacy concerns in cloud computing, specifically focusing on consumer data protection and the prevention of data leakage, and their impact on consumer trust and adoption in Ireland’s IT sector, with the goal of identifying solutions that enhance data protection and regulatory compliance.

### 1.5.2 Objectives

1. To identify the key privacy and data security risks, including potential data leakage, associated with cloud computing in Ireland.
2. To evaluate the effectiveness of current legal frameworks, particularly GDPR, in addressing these data security and privacy risks.
3. To assess the role of consumer trust in the adoption of cloud services amid concerns of data security and leakage.
4. To provide recommendations for organizations to enhance data protection practices, prevent consumer data leakage, and comply with privacy regulations.

## 1.6 Structure of the Dissertation

This dissertation is organized as follows:

* **Chapter 2: Literature Review** will provide a comprehensive review of the academic literature on privacy concerns in cloud computing, with a focus on data protection laws and consumer trust.
* **Chapter 3: Research Methodology** will outline the research design, data collection methods, and analytical techniques used to investigate privacy issues in cloud computing.
* **Chapter 4: Data Analysis and Findings** will present the results of the primary research conducted through semi-structured interviews with IT professionals in Ireland.
* **Chapter 5: Discussion** will interpret the findings in relation to the research questions, hypotheses, and existing literature.
* **Chapter 6: Conclusion and Recommendations** will summarize the key findings of the research and provide recommendations for organizations and policymakers to improve privacy protection in cloud computing.

## 1.7 Conclusion

In conclusion, the increasing adoption of cloud computing in Ireland’s IT sector brings with it significant privacy and data security concerns that need to be addressed to maintain consumer trust and regulatory compliance. The growing threats of data breaches, ransomware attacks, and cross-border data transfers create a complex challenge for organizations seeking to protect sensitive consumer information. By exploring these risks, evaluating current legal frameworks like GDPR, and identifying best practices, this research aims to provide actionable solutions to improve data protection and foster confidence in cloud services.

# Chapter 2: Literature Review

## 2.1 Introduction

Cloud computing has become a game changer in the field of IT by providing benefits like scalability, cost-effectiveness and flexibility of operations. Nevertheless, as more and more organizations embrace the use of big data, the issue of data protection has become very sensitive or crucial, particularly in sensitive organizations. Ireland has become a country that depends much on cloud solutions where issues concerning compliance with the GDPR and other data protection laws and the constantly rising threat of data breaches arise.

This literature review aims to evaluate critically the current literature on factors affecting privacy concerns in cloud computing with emphasis on the Irish IT sector. Its objectives are to determine the major privacy concerns, assess the current regulation environment, and determine the link between the privacy concerns and consumers' trust in cloud solutions.

Some of the key areas under consideration in this review are current regulation, consumer confidence, industry benchmarks, and types of risks inherent in cloud computing in Ireland. But it doesn’t include specifics about cloud infrastructure or any other issues of computer security that are not of privacy concern. This paper aims to add a clear understanding of how to tackle privacy issues and enhance consumer confidence in cloud computing through a review of the literature.

## 2.2 Evolution of Cloud Computing

Cloud computing has quickly moved from the status of being considered a concept to being a vital part of current IT solutions. The concept of cloud computing can be traced back to the 1960s when J.C.R. According to Waldrop (2018), Licklider envisioned an interconnected network of computers—a concept now referred to as the "intergalactic computer network". The next advancement of time-sharing systems brought the essence of today’s cloud computing into practice. The technological development in the 21st century especially in virtualization and high-speed internet brought commercial cloud service into existence, AWS was launched in 2006 as one of the key players in the cloud service providing on-demand scalable resources (Kant, 2019).

Cloud computing has become popular all over the world due to increasing business transformation programs and the requirement of adaptive IT services. As stated in the Gartner report (2024), the cloud computing market should be 20.4% of the total in 2024 being $678,8 billion, while in 2023 it was $563,6 billion. This growth is due to various new business models such as the Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) that are flexible for businesses. Some of the drivers include cost reduction, scalability and collaboration leading to cloud becoming strategic in IT across the healthcare, finance and retail sectors.

The usage of cloud computing has been even stronger in Ireland because of the country’s focus on the strategic role of IT and a developed IT industry noted by Ali et al. (2021). Ireland has become one of the leading European technology markets, and the rapidly growing data centre market has driven the use of cloud services throughout the healthcare, retail, and financial industries. According to Deloitte (2021), cloud deployment in Ireland is growing at a compounded annual growth rate of 54% and organisations are turning to the cloud to be relevant in the dynamically changing business landscape. The high level of regulatory compliance in Ireland, including data protection through GDPR has also ensured that cloud computing security is standard.

Like the United States, the UK has also witnessed a high rate of cloud adoption due to the government’s policies aimed at enhancing the digitalisation of businesses in both the public and private domains. The UK Government's "Cloud First" policy, introduced in 2013, encouraged public sector organizations to consider cloud solutions as a primary option for IT projects as stated by Gov.uk (2017). According to the ‌digitalisationworld (2015), it was established that about 90 percent of enterprises in the UK are currently using the cloud service where the adoption has been enhanced by scalability requirements, cost efficiency, and the new focus on remote operations. This adoption rate is generalizable to the current state of digital transformation across Europe, where the use of cloud technologies to improve business performance and respond to new market conditions has become more widespread among Irish and UK businesses.

The framework for understanding the development of cloud computing through a theoretical lens involves using Diffusion of Innovations (DOI) Theory developed by Wood (2019). These two concepts assist the theory of explaining how, why and at what rate, the cloud computing innovations diffuse in societies and industries. In Ireland and the UK, the pioneers from the financial and technological sectors, primarily, set an example of how cloud computing may be useful, which defined the further market development. The theory explains how perceived usefulness (observability – the advantages of utilizing cloud services) and perceived advantage (relative advantage over traditional IT frameworks) have informed the quick implementation of cloud services.

## 2.3 Benefits of Cloud Computing in the IT Sector

The use of cloud computing in the IT industry has been of great importance as has been described below as a way of benefiting organizations. The benefits of cloud computing which include cost optimization, elasticity and versatility have made cloud computing the foundation of IT planning in the current world.

**Cost Efficiency:** Indeed, cost savings are one of the most important advantages of cloud computing as a paradigm. The conventional infrastructure of it typically entails large capital investments such as purchasing hardware, managing servers, and employing its staff. On the other hand, through the utilization of cloud services, organizations can turn capital-intensive costs into operational costs by using the pay-as-you-go model hence making the costs more manageable in terms of financing. The Deloitte (2021) report reveals that the companies in Ireland that have implemented cloud solutions experienced up to 30% savings on IT expenditures and shifted focus to other parts of their business. In addition, cloud providers manage hardware and software ensuring that they are up to date and relieving an organization of the operational costs of IT systems.

**Scalability:** Another important strength is the scalability that has ensured organizations consider cloud computing as an essential technology, especially for businesses with the changing traffic needs. Liu et al. (2018) pointed out that Cloud platforms make it possible for the firms to add or reduce resource capability depending on the actual demands; the ability to accommodate heavy workloads at certain times without the need for permanent installation. This is especially helpful for Ireland’s tech startups and SMEs since they can quickly grow and require more space in IT infrastructure. This explains why cloud services can be scaled up or down to meet the changing needs of the business environment.

**Flexibility:** This is also one of the greatest strengths of cloud computing, because it provides flexibility in the access of computing resources and in collaboration. Gammelgaard and Nowicka (2024) noted that Since cloud-based tools enable employees to work from anywhere, they have been vital in the context of the post-pandemic hybrid and remote work. This flexibility has been one of the main reasons for cloud adoption in the IT sector in Ireland as the use of remote working becomes more prevalent in order to attract talent especially in the technology sector where competition is high. Cloud platforms include access to various applications and data which allows for better cross-location cooperation and also better project management. For example, cloud collaboration tools have helped firms such as Microsoft Ireland to enhance productivity and sustain communication between distributed teams, which in turn have made it easier to manage projects Microsoft (2024).

**Specific Benefits in the Context of Ireland's IT Industry:** The advantages of cloud computing are especially suitable for the IT industry of Ireland, which has recently demonstrated high rates of digitalization, and the presence of many international IT companies. ‌According to fDi Intelligence (2020), Ireland has become a centre of attraction for such tech giants such as Google, Amazon, Microsoft, etc., and a rich data centre sector has contributed to the development of a competitive cloud services market in the country. It is an environment that offers Irish companies the opportunity to adopt advanced cloud solutions enabling business change and competitiveness. The cloud computing infrastructure also enables other sectors of Ireland’s economy such as the financial services and healthcare industries that require a dependable and expandable environment that can meet the regulatory standards of the GDPR noted by Microsoft (2024).

Further, trade (2022) revealed that Ireland’s National Digital Strategy has called for the digitization of services in both the public and private domain with a focus on the use of cloud technology as a way of enhancing delivery of services as well as strengthening business continuity. The Irish government’s "Cloud Computing Strategy 2022" explicitly aims to migrate public services to the cloud, thus encouraging private sector cloud adoption as well. It has assisted in developing a solid environment that enables the provision of IT services with greater value to both business and consumers.

## 2.4 Privacy Concerns in Cloud Computing

Despite the numerous advantages that cloud computing presents, it presents numerous privacy concerns most of which are as a result of remote and cross border data storage. One of the main concerns of cloud computing is the privacy, particularly in instances where organizations deal with sensitive consumers’ data such as the health and the financial sectors.

**Types of Privacy Issues**

Data leakage is one of the biggest privacy challenges that cloud computing faces; this is where sensitive information is made available to the wrong parties through poor security measures. CSPs frequently store data for many customers on the same computing environments, which raises the possibility of information disclosure or inadvertent sharing of one client’s data with another. An example that can be recalled is the data breach early this year, where one of the popular CSPs left a cloud storage bucket open to the public resulting in the leak of customers’ data affecting thousands of users in Ireland Powell (2022).

To mitigate such risks, data protection protocols such as encryption during data storage and transmission are critical. Multi-factor authentication (MFA) is an essential additional security layer that prevents unauthorized access, even if login credentials are compromised. Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a system, application, or account. Unlike traditional single-factor authentication, which relies on something the user knows (e.g., a password), MFA adds layers of security by incorporating multiple types of authentication factors. Regular vulnerability assessments and audits can help identify weak points and improve the robustness of cloud systems. According to Powell (2022), Another common privacy threat type is unauthorized access and can be acquired from internal and external attackers or even from the unsecured cloud environment. This is different from the on-premises model where most of the data security policies are offered by the CSPs. Such a dependence can led to a situation where an organization has limited control over data security instruments. Most of the unauthorized access cases are as a result of either stolen login credentials, or weak IAM controls. Singh et al. (2023) observed that of data breaches in Irish companies utilizing cloud services were due to insufficient access control, which led to hackers getting past the weak passwords or unguarded endpoints.

**Challenges Due to Remote and Cross-Border Data Storage**

The primary concerns of cloud data storage are privacy issues which are mainly caused by the distance of the data storage servers noted by Yang et al. (2020). In cloud computing, data is located in data centers in various geographic locations and owned by different service providers. This leads to issues about cross-border data transfers and data privacy whereby different laws are used in the regulation of the flow of data across borders. For example, Ireland is a member of the EU, which means that companies operating in the country must follow the GDPR, which has strict data protection standards. However, data stored in jurisdictions other than the EU may not have the same compliance to the GDPR Enterprise (2018).

To address these compliance challenges, CSPs need to adopt transparent data governance practices, disclosing information about data storage locations and processing. Data localization strategies and adherence to cross-border data transfer agreements, such as Standard Contractual Clauses (SCCs), are essential for maintaining compliance. Many organizations using cloud services struggle to gain a clear understanding of where their data is stored, who has access, and how it is processed. This lack of transparency poses significant challenges, especially for businesses in heavily regulated sectors. A survey by Accenture (2023) revealed that 63% of Irish businesses reported difficulties in understanding the data handling practices of their CSPs, hampering their ability to meet regulatory requirements and maintain consumer trust.

## 2.5 Regulatory Framework for Cloud Privacy

This is why regulation of data privacy is important so as to ensure that cloud computing services are used securely and rightfully. The sets of rules governing data protection within the European Union, including Ireland are the General Data Protection Regulation (GDPR) and its impacts are especially important for cloud computing.

**Overview of GDPR and its Implications for Cloud Computing**

The General Data Protection Regulation (GDPR), enforced in May 2018, is one of the most comprehensive data protection regulations worldwide, designed to safeguard personal data and enhance individuals' control over their information. As highlighted by Li et al. (2019), GDPR applies to all organizations that handle the data of European Union (EU) citizens, regardless of their physical location. For cloud service providers (CSPs), the GDPR presents both challenges and opportunities, as it imposes strict obligations regarding the processing, storage, and transfer of personal data.

One of the key provisions of GDPR is the requirement for transparency. CSPs must clearly inform their clients about how personal data will be processed, stored, and protected, and obtain explicit consent from individuals whose data is being processed. This includes providing adequate technical and organizational measures to ensure data protection, such as encryption, access controls, and regular audits to detect vulnerabilities. Data minimization, another core GDPR principle, requires that only the minimum necessary amount of personal data is collected, stored, and processed (Li et al., 2019).

A significant challenge for cloud computing in the context of GDPR compliance is the geographical distribution of data. Since cloud data is often stored across multiple data centers in different jurisdictions, ensuring compliance with GDPR provisions can become complex. Specifically, GDPR imposes strict regulations on transferring personal data outside the EU. As cloud services involve the processing and storage of data across different borders, CSPs must ensure that they have appropriate safeguards in place, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), when transferring data internationally as highlighted by General Data Protection Regulations (2018).

Article 28 of GDPR places a significant responsibility on CSPs, who act as data processors, to enter into Data Processing Agreements (DPAs) with their clients. These agreements must specify obligations related to data protection, including the scope of data processing, security measures, and protocols for handling data breaches. CSPs are also required to ensure that any sub-processors they use comply with the same data protection standards. As noted by Li et al. (2019), this creates a layered responsibility system, where CSPs, businesses, and third-party sub-processors all share responsibility for ensuring GDPR compliance.

**Compliance Challenges Faced by Irish Companies**

There are several major issues that Irish companies have to deal with in terms of GDPR compliance when they decide to use cloud services. First, the problem of cloud data management and visibility or, in other words, the inability to see and manage the data stored in the cloud. Since CSPs may be located in any part of the world the data may be stored in a data centre in a country that has a different legal regime. Cory et al. (2020) affirmed that the 2020 Schrems II decision has added uncertainty to cross-border data transfers and left Irish organisations struggling to confirm GDPR compliance if they depend on the services of their US-based cloud service providers. This has resulted in rising concern over the sufficiency of SCCs as the only means of legal data transfers from the EU noted by Iapp (2024).

The other issue is the one of shared accountability. Far from just the CSPs, organizations who are using cloud services are equally responsible for making sure that data processing activities are GDPR compliant. This shared responsibility model often leads to much confusion on where the CSP responsibility begins and where the customers’ responsibility begins. A survey by ‌PricewaterhouseCoopers (2023) revealed that 44% of the Irish organizations struggled to understand their compliance obligations when using cloud solutions from vendors, thus losing protection over their data.

Furthermore, the 72 hours’ reporting requirement of data breaches under the GDPR provides further difficulties for Irish organisations using cloud services. According to Bhatia (2021), Since cloud environments comprise distributed and multi-tenant infrastructure, identifying, analysing, and reporting breaches often takes more time than permitted. These challenges were evident in 2022 when an Irish financial services firm was hit by a breach; the firm received hefty fines after not informing the Data Protection Commission (DPC) on time regarding a breach involving a third-party cloud provider; this is even though the firm relied on third-party vendors, it was unable to meet GDPR’s strict timelines Data Protection Commission (2024).

## 2.6 Cybersecurity Threats and Cloud Data Protection

Cloud computing has provided manifold advantages but has introduced the challenges of security threats to data; hence, CSPs and clients are concerned about data security. Security is one of the biggest issues in the context of cloud computing because threats are in direct relation to data data access, data content, and data existence.

**Types of Threats**

The most common danger that can become a problem for cloud computing is ransomware – the malicious software that encrypts the data and offers the decryption key for a certain sum of money. Ransomware attacks have also evolved and are commonly aimed at weak spots in the clouds, where companies often share resources. According to Ireland’s Irish Computer Security Incident Response Team (CSIRT) in 2023, over 200 ransomware attacks targeted cloud-based infrastructures, financially damaging and disrupting Irish businesses First Response (2022). They provide an example of the increasing risks within multi-tenant cloud environments as a compromised tenant can easily impact others.

Another significant cybersecurity threat is unauthorized access, where the attackers use a vulnerability of an organization and get unauthorized access to the cloud systems. Cloud environments are mostly prone to misconfiguration because it is complex and requires continuous updates. A report by ‌Thalesgroup (2024) that approximately 39% of data breaches on cloud systems were associated with misconfigurations and weak access control. These vulnerabilities make cloud services more appealing to attackers who want to take advantage of insecure settings to gain access to information or interrupt service.

**Importance of Stringent Security Measures and Compliance**

Preventing data breaches, unauthorized access, and ransomware attacks requires the implementation of robust security measures. Encryption of data, both in transit and at rest, ensures that even if data is intercepted, it remains protected. Cory et al. (2020) affirmed that multi-factor authentication (MFA) adds an extra layer of security to prevent unauthorized access, even when login credentials are compromised. Continuous monitoring and threat detection solutions help identify and mitigate risks before they escalate into severe incidents. Adherence to compliance frameworks like GDPR is crucial for maintaining consumer trust and ensuring that CSPs meet stringent data protection standards. Abrera (2024) noted that the GDPR requires CSPs to implement strong data protection measures, enforce data minimization, and maintain transparency regarding data handling practices. Compliance with these regulations not only supports legal obligations but also builds confidence among users who are wary of potential data vulnerabilities.

**Impact on Consumer Trust and Cloud Adoption**

The increasing number of cybersecurity threats has affected consumer trust in cloud services significantly. Khayer et al. (2021) stated that incidents of ransomware attacks, data breaches and unauthorized access increase consumers’ perception of risk in regards to their personal information. Trust is a key ingredient in cloud computing; people will not use cloud services, particularly for mission-critical applications such as finance or health.

Consumer distrust is most apparent in areas that require the protection of their information and data. Lynn et al. (2020) survey of Irish consumers also revealed that data privacy was a concern when using cloud services because many people were aware of constant cyber threats and incidents that made them reluctant to embrace cloud services. These threats affect not only the end users but also entire industries where the pros of cloud use are compared to the cons that may come from data leakages which affects organizations reputation.

To address these threats, CSPs and their clients need to employ strict security measures, such as encryption, MFA, and threat detection solutions As mentioned by Abrera (2024), the compliance with the GDPR legislation, along with the application of the aforementioned security measures can help restore consumer confidence and drive cloud solutions uptake in Ireland. However, trust in such services cannot be built only on technical measures; CSPs need to report on their data protection policies and measures they take to ensure consumers’ data privacy.

## 2.7 Consumer Trust and Cloud Adoption

Consumer trust is therefore a critical determinant of the use of cloud computing services. Concerns for privacy are strongly correlated to the level of trust which consumers have in any given product, or service provider especially in today’s world where data theft and cyber-attacks are the order of the day.

**Privacy Concerns and Consumer Trust: A Literature Review**

According to Tabrizchi and Kuchaki Rafsanjani (2020), Security has become one of the main issues that have been cited as a constraint to cloud computing, these straight impacts consumers’ trust in cloud service providers. Some of the issues that make people worried about using cloud environments are due to distributed nature of cloud where data is stored in different geographic locations. They also have become more conscious of the privacy of their data especially in relation to the possession of their data and utilization. A survey by Deloitte (2023) revealed that 67% of consumers are reluctant to adopt cloud services because of issues to do with data privacy, and the notion that CSPs cannot protect their data.

The relationship between privacy concerns and consumer trust can be understood through "trust-building factors," which include transparency, control, and accountability. Michler et al. (2020) noted that Compliance frameworks such as the GDPR play a pivotal role in reinforcing these trust-building factors. GDPR mandates that CSPs enhance data protection measures, ensuring consumers' right to decide how their data is processed and holding CSPs accountable in the event of a data breach. Proper compliance frameworks establish a foundation for trust; when CSPs demonstrate adherence to such regulations, they foster consumer confidence. The significant data breach in 2022 involving a major CSP in Ireland, which led to the exposure of thousands of consumers’ personal details, underscores how privacy issues can drastically impact trust and reduce cloud service adoption (economictimes.indiatimes, 2024). This breach highlights the importance of compliance and robust security measures to maintain consumer trust.

**Consumer Perception of Cloud Service Providers in Ireland**

When consumers make decisions as to which CSP to use in Ireland, they are likely to consider the security of the cloud environment, legal requirements on data protection, and reputation of the CSP. Dempsey and Kelliher (2018) stated that GDPR has been an improvement that has put strict responsibility on CSPs to protect consumer data and has been good for consumer trust. However, compliance alone does not address privacy issues where there are no clear directives on where the data is stored and how data sharing is done.

In a survey carried out by PwC Ireland (2023), 59% of Irish consumers perceive that CSPs are not very clear on how and where their data is being stored. Such perception is especially evident among the elderly and the customers belonging to the health and financial industries. Consumers also have concerns about shared responsibility model in cloud environments most of which are unclear on who is responsible for what. These issues explain why people are rather sceptical about using cloud services, especially for the applications containing valuable or personal information.

To solve these problems cloud service providers in Ireland should pay more attention on the following aspects: The trust building measures that include the policies of data, security, and the proper communication of policies for handling data. To promote the use of cloud computing in Ireland IT sector it is important to show GDPR compliance, excellent security measures, and transparency.

## 2.8 Industry Best Practices for Data Privacy and Compliance

Several best practices have been taken by organizations to mitigate privacy risks and practice compliance in cloud computing. One of the key control measures is information encryption, that is, data protection in storage and during transmission. Ometov et al. (2018) also observed that multi-factor authentication (MFA) is also used commonly to enhance the security for cloud systems access. Also, almost all the organizations carry out routine audit and vulnerability assessment to prevent future risks to security.

One of the best examples of the use of the privacy strategy is the case of Microsoft Ireland, which has developed a proper data governance model that is supported by encryption, IAM protocols, and principles of zero trust mentioned by Plumer (2024). This model has helped Microsoft to meet the GDPR compliance and make customers confident about their data. According to Wittig and Wittig (2023), Another case is Amazon Web Services (AWS) that enhanced privacy features, as well as data localization and compliance with international security standards that allow companies in highly regulated industries to meet local data protection requirements.

These best practices show that data privacy today is a combination of both technical and administrative controls for compliance and consumer trust in cloud services.

## 2.9 Literature Gap

Although there are extensive investigations on data privacy in cloud computing, there are still several important research areas. There is also one significant knowledge gap: a scarcity of the Irish studies that would address the privacy issues unique to the Irish environment, including the effects of the cross-border data flows in compliance with the GDPR stated by Voss (2019). Much of the current work in this field focuses on the cloud privacy on a global or EU level and does not offer a detailed insight into how the aforementioned challenges impact Irish organizations, including SMEs.

Future research is also needed to examine the consumer perception that influences cloud adoption and the way privacy issues affect various industries in Ireland. Hence, a further analysis of the practical implementation issues arising from the Irish businesses’ GDPR compliance and their use of cloud services to address these gaps is essential.

## 2.10 Conceptual Framework

This research concerns privacy in cloud computing where the conceptual framework is developed from the GDPR compliance model and trust-mediating strategies. Some of the features of the framework are data encryption, IAM protocols, elements that affect consumer trust including transparency, control, and accountability and compliance.

The relationships within the model concern the positive impact of proper application of privacy measures and compliance with the laws on the trust of consumers, which will in turn promote the use of cloud services. The framework seeks to demonstrate that, with proper data governance and targeted consumer involvement, privacy risks can be controlled, and trust established in cloud systems in the Irish IT context.

# Chapter 3: Methodology

## 3.1 Introduction

This chapter provides a framework of the research undertaken to answer the studies aims and objectives with particular emphasis of privacy issues and compliance in cloud computing within the IT sector in Ireland. Such a strong methodological approach will guarantee the reliability, validity of the results, as well as the relevant response to the literature gaps. Therefore, the study adopts a qualitative method to understand the detailed responses from the IT professionals and data protection experts on the privacy risk, regulation, and consumer trust. The methods presented in this chapter enable a systematic approach to data collection and processing in order to obtain significant and practical outcomes.

## 3.2 Research Philosophy

This research adopts an interpretivist paradigm that recognizes and tries to uncover perceptions of individuals within their environments. Interpretivism is indeed advisable for the research topic focusing on various multifaceted socially constructed objects, including privacy concerns or compliance in cloud environment. Through centering the views of IT professionals and data protection professionals, this philosophy allows the researcher to explore the nuanced nature of these issues and how they are experienced in the field (Alharahsheh and Pius, 2020). The interpretivist approach is, therefore, congruent with the overall qualitative approach of the research because it focuses on the quality rather than the quantity of data collected.

Privacy issues and compliance deficiencies associated with cloud computing are equally not solely technical problems; they depend on the organizational processes, laws, and perception of users. Thus, such processes and their interactions must be described with research methods that do not dismiss or marginalize personal observations. This philosophical stance also justifies the adoption of the semi-structured interviews in that, it ensures that the participant is able to express him or herself while at the same time allowing the researcher to follow up new trends within the research findings (Nickerson, 2022). Through the use of interpretivism, this study seeks to offer findings that are realistic, relevant, and meaningful in addressing some of the consumer trust and regulatory issues in Ireland’s IT industry.

## 3.3 Research Design

This research work uses a qualitative research paradigm since the end goal is to capture the views and experiences of professionals in the cloud computing domain. Unlike the quantitative methods that use large numbers and amount values, the qualitative methods place a lot of emphasis on the quality of the data collected and the complexity of the people’s perceptions and behaviours. Since privacy concerns and compliance issues in cloud computing are relative and depend on certain factors, it will be more appropriate if the research design of the study is qualitative (Kamal, 2019).

More specifically, the research design of study is exploratory since it aims to uncover the complex phenomenon of privacy risks, regulation and consumer trust. Exploratory research is applicable in situations where not much information or insights are available or where new ideas are required. Privacy and compliance challenges in the context of cloud computing are dynamic and are informed by advances in technology, legal standards, and changing customers’ preferences (Muzari et al., 2022). This design enables the researcher to focus on these dynamic aspects and explain how they affect the decision-making process in the Irish IT industry. Semi structured interviews, as the main data collection tool, also buttress this exploratory approach since it affords flexibility for the respondent to provide elaborated experience accounts, while simultaneously availing the researcher the opportunity to follow evolving themes. This research design would provide a broad perspective on the issues and benefits related to cloud data privacy and legal compliance (Yadav, 2021).

## 3.4 Sampling Strategy

The target population for this research includes IT and data protection personnel practicing in Ireland. Some of these people are responsible for the protection of the consumers’ information within the cloud and they therefore better understand the vulnerabilities, the regulatory hurdles, and how best to assure the consumers. Thus, by overlaying focus on this group, the research seeks to obtain pertinent and knowledgeable views. In terms of recruitment strategy, the study uses purposive sampling to sample the participants (Campbell et al., 2020). This technique is more appropriate in qualitative research endeavor since it helps in identifying participants with sufficient background and experience in contributing towards addressing the research goals. Through purposive sampling, the researcher can target different professionals involved in cloud data protection, hence attaining a high-quality contextually sampled data.

The proposed sample size of at least 10 participants to participate in the study meets the standard sample size range for qualitative research studies that aim to provide detailed information. This size is reasonable enough to achieve the aim of gaining diverse perspectives while still being practical in terms of data management and analysis of qualitative data. The emphasis is placed not on the probability of the results’ general applicability but on the quality of the insights gathered (Denieffe, 2020). It also enables the study to provide a broad perspective of the privacy and compliance outlook in the IT industry in Ireland without compromising on the methodological soundness of the study.

## 3.5 Data Collection Methods

This research adopts interviews as the main data collection technique, although they are semi-structured. Semi-structured interviews are suitable for qualitative research because of the flexibility that it has and at the same time has structure. The use of interview protocols helps in being consistent with the kind of questions posed to participants thus enhancing the comparability of the interviews despite giving the participants a chance to explain their answers further (Adeoye‐Olatunde and Olenik, 2021). It allows for obtaining high-quality and detailed information, which is vital for researching multifaceted topics such as risks and legal requirements for cloud computing. Recruitment will be conducted through professional sites that include LinkedIn with an interest in IT and data protection specialists. The target respondents will be introduced to a brief description of the research and all of them will be encouraged to participate in the study on a voluntary basis. This study will adopt both face-to-face and online interviews depending on the participant preferences and accessibility. Online interviews also guarantee wider access and prospects to maintain set time limits (Naz et al., 2022).

An interview guide will be used to guide the discussions with participants regarding privacy threats, legal requirements, and consumer confidence, but participant responses will be unscripted. This ability enables information that may have been overlooked or not considered relevant at the onset to be revealed at some point during the analysis. The participants will be given informed consent information which provides them with details about the study such as its aims and objectives and them as participants. Consent forms will be given to the participants and the participants will sign them before the interviews commence (Ruslin et al., 2022). Privacy concerns will be addressed by eliminating any identifying information from participants and properly storing all data that is collected from participants. All these steps are compliant with the ethical standards and make the participants to be assured that their information is well protected with much regard to the ethics upheld.

## 3.6 Data Analysis Methods

Semi-structured interviews are used concurrently with the interviews and thematic analysis is used as the main method of analysing the data that is collected. It is because this study’s qualitative research approach is appropriate for pattern recognition and description when investigating typical issues with privacy concerns, compliance, and consumer trust concerning cloud computing.

**Coding Process**: The first step is to produce a comprehensive text corpus for analysis from the recorded interviews. Transcriptions will be reviewed repeatedly to familiarise the researcher with the material under analysis. The data will then be systematically coded by dichotomizing it into meaningful units of analysis that reflect specific ideas or insights. Codes will be sorted into subcategories that will then generate initial main’s themes (Swain, 2018). For example, topics can be “perceived risk deficiency,” “loss of trust due to data leakage,” and “risk mitigation to improve data security.”

**Identification of Themes**: Once the initial themes have been generated, the working themes will be elaborated based on their connections and the extent of their coverage towards addressing the objectives of the study. Themes will be categorized and sub-divided, with the main themes being, for instance, compliance, while sub-themes being the shared accountability under the GDPR (Proudfoot, 2022).

**Validation**: For the purpose of increasing validity, the identified themes will be compared with highlighted literature regarding cloud computing privacy and compliance. It helps establish coherence with prior work and use this comparison to spotlight some of the study’s new discoveries (S. Rajashekar and Jain, 2023). Moreover, back checks may be given to the participants on the preliminary findings in order to ensure the validity of the identified themes.

## 3.7 Ethical Considerations

This research respects ethical practices to ensure that the rights of the participants are respected throughout the completion of the research.

**Informed Consent and Communication**: Each participant will be provided with a clear information sheet on the aim and aim, objective and expectation of the study. This will include their rights information like the freedom to withdraw at any one time and any preconditions that are associated with the withdrawal. Consent forms will be handed to the participants and participation will only take place after the participants has signed the consent form (Mirza et al., 2023). As an additional precaution, for online interviews, both the verbal consent will be recorded.

**Confidentiality and Data Security**: Participant anonymity will be observed through the process of removing any personal details from the recorded data and analysis of results. Data will be kept on password-protected devices and encrypted storage devices and will be only within the researcher’s access. Any prepared hard copies will also be locked up to ensure that they cannot be accessed by unauthorized persons (Anna-Maija Pietilä et al., 2019).

**Institutional Ethical Approval**: The research will conform to the ethics of the institution and the conventional ethical standards as they will be followed. Before actually going for data collection, approval from the ethics review board will be sought to ensure propriety of all the processes by the institutional and professional ethical standards (Mirza et al., 2023).

## 3.8 Reliability and Validity

**Reliability**: To maintain inter-subjectivity during data collection, a developed interview schedule will be used in all the semi-structure interview. A potential solution is to prepare a list of questions and topics for the interview and to make sure that all participants are asked closely similar questions, which would allow for elaboration. Thus, the outcome of the study will be consistent since the data collected from the interviews will not be inflicted with a lot of variations due to the difference in the interview procedures (González et al., 2021). Also, all interviews will be conducted with the use of audio-recorders and the tapes will be transcribed word by word.

**Validity**: To increase the validity in the study the following approaches will be used. First, triangulation will be done through comparing the results of the study with previous research studies in the area of privacy concerns, compliance issues, and customers’ trust in cloud services. This ensures that the findings of the given study align with the existing trend of research while providing novel advancements. Second, member checking will be considered whereby the participants may be required to review the preliminary findings and verify the accuracy and credibility of their responses (Coleman, 2022). Last, steps will be taken to enhance the clarity of conclusions along with using the verbatim reports of the participants’ observations. In combination, these measures enhance the validity of the study outcomes.

## 3.9 Limitations of the Methodology

It is important to note that, although this research utilised a strong qualitative research method, there are several caveats to this work. First, the small sample size, with at least 10 participants, may reduce the external validity of the results to the community level. However, the study compromises on the quantity to focus on the quality of responses from IT and data protection professionals that would ideally have advanced knowledge of different solution types and their implications (Kamal, 2019). This approach makes sure that contextualised data is collected so that best understanding of privacy concerns and compliance issues is made.

Second, qualitative research relies on potential limitations in participants’ answers, for example, the tendency to give political answers or develop own interpretations of the questions. To address these biases, more structured and less guided interviews are conducted in such a way that the participant is able to expand on thoughts and ideas freely. Further, the use of the interview guide helps to minimize variability within the data collection techniques since the same questions are asked throughout the interviews (Adeoye‐Olatunde and Olenik, 2021).

Lastly, using qualitative data like the thematic coding may also bring researcher bias into play since its assessment is dependent on the analyst’s interpretations. To address this, themes will be validated through comparison with other literature and, where possible, participant feedback. Although these are critical factors and may somewhat limit generalized results, the richness and depth of the findings provided outweigh the disadvantages, especially when researching multifaceted topics such as cloud privacy and compliance (Kamal, 2019).

## 3.10 Summary

This chapter has described the methodology appropriate for evaluating the privacy perceptions and compliance risks associated with the cloud computing paradigm in Ireland’s IT community. To gather rich information from IT and data protection professionals, a qualitative research approach, underpinned by an interpretivist paradigm, was adopted. Through the purposive sampling and focusing on the objectives of the research, semi-structured interviews enable elaborate answers. Thematic analysis remains systematic, and applying ethical considerations and measures of reliability and validity raises the study’s credibility. All of these choices are consistent with the objective of the study to offer a broad perspective on risk, regulations, and ways to establish consumer confidence.

# Chapter 4: Results and Analysis

## 4.1 Introduction

This chapter contains the interview results and analysis within the software, highlighting the themes regarding privacy, security, and responsibility for cloud computing. Overall, the findings are relevant to the research goals regarding key issues and trends related to data protection and cloud services usage. Thematic synthesis and NVivo software also revealed five emergent themes each representing a frequent pattern and participant viewpoints. These themes will help to gain insight about certain intricacies of cloud computing issue, in particular, it will focus on technology, compliance, and people aspects. The analysis serves as the basis for further consideration of the generalization in the next chapter.

## 4.2 Results

### 4.2.1 Theme 1: Privacy Risks and Consumer Trust in Cloud Environments

Security issues are one of the factors that affect consumers regarding trust in cloud computing as pointed by the participants of the interviews. Cross-border data transfer, data leakage, and unauthorized access to the consumers’ data were named by the participants as the key reasons for the decreased trust in cloud services. This concern is supported by studies conducted in the literature, which indicate that trust is central to the use of cloud solutions. It was mentioned by participants that data leaks especially those related to compromised cloud environments and poor access security measures are very frequent. For instance, one of the participants mentioned that vulnerabilities that result from misconfigurations in shared multi-tenant cloud systems allow unauthorized users to access sensitive data. This observation can be explained by trends in cloud computing, and the fact that misconfiguration of systems is among the main reasons for leakage of data. Another learner noted that there are threats posed by insiders and mishandling of customers’ data by employees that could potentially erode the consumer trust.

A white board with colorful text

Description automatically generated with medium confidence

Figure 1: Privacy Risks and Consumer Trust in Cloud Environments

Another important problem that was raised was the unauthorized access. People provided instances of poor identification controls which include the use of basic passwords without MFA, which allows an attacker to infiltrate cloud systems illicitly. One of the participants said, “Weak passwords and inadequate access control are easy targets for the attackers,” explaining why effective access controls are essential for developing consumer trust. Another concern arises with the sharing of data across borders. Some of them had a problem with certain CSPs which do not clearly indicate places where the data is being stored and processed. Some of them noted that consumers do not necessarily know where their data is stored and if it is stored in areas that offer weak protection as in areas outside the EU. Such risks, driven by the already challenging endeavor of achieving compliance with the GDPR across borders, weaken trust. Furthermore, several participants touched upon the psychological aspect of violations where risks are often overestimated in comparison with actual occurrences. A participant noted, “Even where data is safe, consumers are still worried of the misuse or unauthorized access and this makes them avoid cloud services.”

### 4.2.2 Theme 2: Challenges in Compliance with GDPR and Data Protection Regulations

Data protection legislation such as GDPR and others and how best to meet them was found to be a major concern among the participants. They found cross-border data transfer restrictions, changes, and complexity in the nature of shared responsibility for cloud services as challenges. These challenges make it difficult to guarantee proper data protection and privacy, especially in Ireland’s highly regulated technology industry. Among the most concerning topics was the question of how to deal with cross-border transfers of data. Some of the responses pointed out that cloud means data is hosted and processed in various locations, some of which may not afford the GDPR level of data privacy protection required. An observer noted, “Currently many companies face the problem of identifying whether their data is processed according to GDPR in case it is located in non-EU country.” This lack of transparency from Cloud Service Providers (CSPs) poses enormous compliance risks especially in the backdrop of the Schrems II decision which declared the EU-US Privacy Shield and hence delayed the transatlantic data transfers.

Another drawback was the facts that both CSPs and their clients were held equally responsible for the breaches. Some of the participants observed that there is some confusion within CSPs and organizations on who has the responsibility of data protection. This results in compliance gaps because some organisations still erroneously believe that CSPs are solely responsible for GDPR compliance. One participant said, “Several organisations lack sufficient knowledge on GDPR requirements and are over-reliant on CSPs in compliance, which leads to gaps.” The findings confirm literature that has called for elaboration of roles and responsibilities in cloud contracts to help avoid these risks. Many of the participants also complained that it was challenging to keep up with the ever-changing regulations.

A close-up of words

Description automatically generated

Figure 2: Challenges in Compliance with GDPR and Data Protection Regulations

As one of the participants put it, ‘The change often occurs with the data protection laws and hence the need to update the system frequently and also conduct audits that can be time-consuming and therefore difficult to cope with’. This resonates with literature in the sense that there is increased pressure on organizations to manage change in regulations especially for multi-tenant cloud environments for compliance monitoring are already challenging. Last, participants highlighted the GDPR’s 72-hr response time on breach notification as a recurring concern especially on organizations that use CSPs. The identification and reporting of breaches within the required timeframe is challenging in the case of distributed cloud infrastructures. One participant opined that, “Though the breach may originate from our end or within the CSP, the onus is on us to report, and this is unreasonable and inconceivable at times.”

### 4.2.3 Theme 3: Cybersecurity Threats and Mitigation Strategies

The cyber threats were an issue of focus among the participants, with stakeholders pointing at an increased attack on the cloud configurations owing to the rising need for effective protection measures. Some of the most common causes of data breaches in the cloud systems include ransomware, phishing attacks, and system misconfiguration, which were singled out by participants as a significant threat to organizational security and consumer trust. Our participants pointed to ransomware as a consistently emerging threat. The threats include instances of attackers encrypting important data with the aim of obtaining ransoms from the CSPs or their clients. A participant noted, “These are highly evolved ransomware attacks that are prepared to take advantage of multi-cloud environments.” This observation is backed by the literature, which asserts that multi-tenant cloud architectures introduce organizational risks if a tenant’s security is threatened.

Phishing attacks were also mentioned to be a significant threat because they are not based on weaknesses of computer systems but people’s misbehavior. The participants noted that the attackers go for the employees since most of the cloud systems are infiltrated from inside. A participant remarked, “Phishing is nothing that get you credentials and lets you in — that more of an entry point for subsequent attacks, such as ransomware and data theft.” These findings support other works highlighting the need to promote user education and awareness to help deal with the phishing threats. Another common problem considered was system misconfigurations. Interviewees mentioned instances where the wrong settings on the cloud led to compromising of people’s information. A user noted, “Misconfigurations, especially to access controls, top the list of causes of data breaches in cloud environments.” This is why more organizations ought to strengthen their configuration management practices when embracing such solutions.

A white rectangular object with black text

Description automatically generated

Figure 3: Cybersecurity Threats and Mitigation Strategies

The following strategies were recommended by the participants in addressing these threats: Encryption was highlighted as an important layer and a large number of the participants stated that their data is secure while stored and while being transferred. Another proactive measure mentioned included the active use of multiple factor authentication (MFA) because it is dangerous to give the password or login details to unauthorized persons. The methods which were given a special focus of real-time monitoring namely intrusion detection systems were deemed essential for early threat identification. As one of the participants expressed, “Though it may be called management of crises, what we are doing here is a way of preventing some of those conditions that could have degraded into crises.” Another approach that was depicted was API safeguarding. They contended that great emphasis should be placed on choosing identifiers that should be widely recognized and utilized to avoid having to work with APIs that contain loops which may be manipulated by assailants. It also suggested that organizations should perform penetration testing as well as security audit in order to identify weakness in cloud systems.

### 4.2.4 Theme 4: Role of Cloud Service Providers in Addressing Privacy Concerns

From the interview with the stakeholders, it emerged that CSPs were the only ones dealing with privacy and compliance. According to the interviewees, though CSPs offer relevant technologies like data encryption, threat detection, and data safekeeping, the problem is secrecy, shifting responsibility, and lack of cooperation. Such a strategy as the enhancement of relations with CSPs was viewed as a direction to minimize risks of violating privacy and adhering to compliances such as GDPR. One of the complaints that frequently appeared in the discussions was the lack of information that CSPs offer about their policies. Concerns were raised on how organizations are unaware or unable to know where exactly their data is stored if it is adequately processed and if it respects the local and global privacy laws. An interviewee said, “There is lack of clarity from cloud providers about the data location and their specific compliance strategies – this puts us at risk of non-compliance of regulations we have to follow”. This is in line with the literature because the opacity of cross-border data flows aggravates compliance issues and consumer skepticism.

Participants also urged on enhancement of Service-Level Agreements (SLAs) so that to state clearly the roles and responsibilities between CSPs and their clients. The roles and responsibilities mentioned in the shared responsibility model were also cited as a source of confusion, with regards to the confusion on which party should be held responsible for privacy and security issues. As one participant noted, “SLAs should clearly outline who is supposed to do what to make it clear to both parties, for example, in cases of a violation or non-compliance.” This statement refers to an important problem of contracts and the lack of clear accountability, which has led to an increased demand for clear and concrete contractual agreements. Other critical aspects that were also mentioned included routine evaluations and combined security efforts to enhance partnership with CSPs. It was underlined that compliance checks and security audits should be performed on a regular basis to define main risks and to control whether CSPs follow the set of agreed requirements.

A participant stated, “We also engage our cloud provider to conduct combined audits in order to harmonize our approaches to data protection and compliance to GDPR.” These were regarded as crucial to develop the trust base and to support the shared responsibility model. Respondents requested CSPs to go on the offenses by informing their clients about data privacy risks and compliance needs. This includes providing a user friendly and interactive dashboard to monitor the data activity, setting alert mechanisms to identify potential data breaches, and creating compliance reports. In this respect, participants underlined that successful cooperation with CSPs involves not only technical assistance but also accountability. The major approaches to alleviate privacy concerns and enhance trust in cloud services include: enhanced transparency, clear SLAs, auditing, and integrated security.

### 4.2.5 Theme 5: Emerging Technologies and Their Impact on Cloud Privacy and Security

AI, ML, and blockchain were mentioned by the participants as innovative but somewhat challenging techniques used in cloud privacy and security. These technologies were identified as double-edged swords: While these dimensions enhance threat recognition and information credibility and ensure optimal organization functioning, it is still a challenge owing to their connection with big data and complexity. AI and ML were recognized as the capabilities that can improve cloud security if used to improve threat and anomaly identification. The participants also noted that it allows for the tracking and analysis of usage patterns that lead to deviations and possible security compromises. Another participant said, “AI and ML help us in threat modeling a situation for example, will be to determine if there is a prohibited access attempt or unnecessary file transfer.” Such capabilities support the idea of literature, that AI and ML are becoming critical to automate the security process and minimize human influence. Nevertheless, participants also noted concerns about privacy issues regarding use of AI and ML. Such technologies may involve the use of large datasets in the training of algorithms, raising issues of privacy breaches in data management.

Blockchain was found to be an underexplored but potentially valuable approach to improving data confidentiality and accuracy in clouds. Some of the points that were highlighted by the participants are that, blockchain has the ability to bring about increased transparency and accountability of data management system due to decentralized ledger format it uses. One of the participants averred that, "Blockchain brings the ability to organisations and consumers to control data by recording every transaction through a secured and a sealed way.” This capability may be useful especially when dealing with regulating frameworks such as GDPR as it provides the ability to track data access and processing. However, participants were aware that there are some constraints to the use of blockchain in cloud services because of scalability issues and technical integration. It was also possible to identify certain levels of confusion about the feasibility of incorporating these new technologies into known cloud environments. Concerns were raised by some participants regarding the difficulty and the costs associated with the adoption of AI, ML or blockchain for business. One participant noted, “Despite the fact that these technologies are effective, there is always the challenge of high costs, and skills that are required to implement these technologies.”

## 4.3 Analysis

In this section, the findings from the interview themes are discussed in light of the literature and aims and objectives of the study.

### 4.3.1 Privacy Risks and Trust

The results on privacy risks and consumer trust resonate with previous studies, which emphasize that trust is an essential factor affecting the use of cloud services. Participants in the interviews shared a common sentiment: security issues such as privacy leakage, hacking, and inadequate disclosure of the procedures used across borders are main reasons why consumers still fear cloud services. This is in line with the previous research where privacy concerns are viewed as the main cause of apprehension among users especially touching on the sectors of health and economical facilities (Powell, 2022). The absence of information about the locations where data is stored, as well as the access privileges, was another common point raised in the interviews. Some participants pointed out that many customers lack basic knowledge about the location of their data or whether it is governed by sufficient laws.

This problem reflects another topical question within the existing literature: cross-border data transfer and the ensuing challenges in compliance, which include following GDPR and other similar regulations, are cited as the main concerns for both business and CSPs. The results suggest that as long as CSPs do not provide more information, the level of trust in cloud services will be limited. Specifically, respondents pointed out that privacy-related issues are escalated by concerns of data abuse or leakage. Although data theft is not always occurring in the future, the possibility to misuse data makes people avoid using cloud services (Singh et al., 2023). This observation supports previous findings that consumers’ sentiments toward data privacy are governed by perceived threats instead of actual incidences of data stripping. As such, mitigation of these concerns requires more than just better security of cloud environments but also rebuilding trust by making CSPs trustworthy.

### 4.3.2 Compliance Challenges

One of the emerging themes from the study is that the shared responsibility model poses a challenge in GDPR and other data protection laws to organizations. In this model, the liabilities for protection and management of data are shared between the organization or company (the data controller) and the CSP (the data processor). However, participants complained that there was lack of clarity regarding roles and responsibilities specifically in terms of adherence to GDPR regulations, which are strict in data protection and reporting. This results in compliance gaps, due to organizations believing that CSPs manage all data protection responsibilities, including compliance (Li et al., 2019). This is a well-known problem in the literature, where the shared responsibility model is mentioned as one of the most contentious issues in cloud computing contracts. This area of research explores contractual relationships that should portray the intended scope of work, which the client and the CSP expect to deliver and receive, respectively.

The participants in the interview argued that there is a lack of awareness of organisations understanding their GDPR requirements especially in relation to DPAs and ensuring that CSPs deploy adequate technical and organisational measures for personal data protection. One of the main difficulties that participants noted about GDPR implementation is that organizations have to make sure that data transfers across borders respect regulation. This issue is even more challenging for companies employing multi-jurisdictional cloud services where the laws governing data protection vary. Both identified that in these processes, coordinating these intricacies together with constant changes in regulation is time-consuming and challenging to coordinate (Iapp, 2024). This is a major challenge organizations face when trying to adopt cloud solutions to their optimum potential, more so in industries like finance, healthcare and public sector where compliance is core.

### 4.3.3 Cybersecurity Threats

The cybersecurity threats named by participants in the interviews match with global trends in cloud computing. Some of the most often quoted risks are ransomware attacks, phishing, and system misconfigurations, which are even more problematic in the cloud environment because of the intricate and distributed natures of the cloud architectures. Some of the respondents reported that ransomware attacks are increasing in complexity, for example, they can target shared cloud environments, where multiple tenants potentially have the same level of exposure ‌(Thalesgroup, 2024). This aligns with the Global Cybersecurity Index where cloud computing cybersecurity notes that due to the multiple-tenancy model of the cloud infrastructure, it is more exposed to big-data attacks. Phishing attacks, used to gain unauthorized access to cloud environments were also considered significant threats. These attacks are principally aimed at the employees with the purpose of acquiring login credentials and obtaining data from cloud systems.

Some of the threats which have been highlighted by participants include new schemes such as phishing attacks where perpetrators employ social engineering tricks to compromise security. The literature emphasizes that the human factor is still one of the main sources of cyber threats, and participants’ fears regarding phishing incidents support this statement. An important factor highlighted by the participants was that of misconfiguration of cloud systems. All these misconfigurations, with respect to access control or security settings, put the cloud environments at the risk of external threats (Abrera, 2024). People stated that a lot of organizations have issues setting up Cloud correctly and this leads to vulnerabilities. This is in line with the literature where it is argued that misconfiguration is among the leading root causes of cloud security breaches.

### 4.3.4 CSP Collaboration

Collaboration with CSPs was another theme identified in the interviews as important, especially regarding responsibility and trust. Especially, participants pointed to the lack of clarity of the agreements with CSPs, weak SLAs, and the absence of audits to clarify mutual expectations or identify those responsible for data security and compliance. This resonates with the previous studies which posit that it is important for firms to cultivate openness and cooperation with CSPs to mitigate privacy and compliance risks. Participants also suggested that CSPs be more forthcoming on security features, matters to do with data privacy and adherence to regulatory policies (Tabrizchi and Kuchaki Rafsanjani, 2020). This is in accordance with the literature that states that CSPs should be very transparent to the consumer so as to build trust and hence long-term relationships.

Some of the key findings included the fact that while CSPs offer functional infrastructure components like encryption and threat detection, they also need to assist organizations in determining their compliance with components they are liable for in the shared responsibility model. The need for periodic audits and collaborative security measures were also discussed. CSPs mean that IT organizations can mitigate risks that threaten their cloud environments through improved collaboration (Michler et al., 2020). This approach simplifies risks and helps both parties inform each other of weaknesses that may be exploited by the other side. Such outcomes contribute to literature that calls for the constant interaction of organizations and CSPs to solve the problem of privacy and security.

### 4.3.5 Emerging Technologies

AI, ML, and blockchain, were categorized as technologies that have pros and cons of cloud privacy and security. Namely, all the participants recognized the great potential of these technologies in enhancing the security of cloud systems, such as threat pattern identification, data encryption, and robust data authentication. It is seen that the highest interest was shown to those AI/ML solutions which would help in analysing the security threats in real-time mode because of their capability to go through large sets of data and come up with previously unnoticed features (Ometov et al., 2018). They also raised concerns on the impact these technologies will have on the privacy of individuals, especially the use of the big data in AI and ML. This creates concerns when large quantities of personal and sensitive information is applied to improve these systems.

Some inevitable issues such as difficulty involved in integrating new AI and ML systems into cloud environments and biases in algorithms were also recognized as the issues that deserve the right solutions. Meanwhile, blockchain was regarded as a tool that can help make data more transparent and secure, especially in the cases of multi-actor cloud data processing. The participants appreciated how the blockchain technology characteristics of decentralization and immutability could be leveraged to efficiently record and manage data (Plumer, 2024). But they also accepted the present-day problems with digital currency and specifically the issues of its scaling and the problems of incorporating it into current cloud platforms.

## 4.4 Summary of the Chapter

In this chapter, the findings of the interview data are discussed to show pertinent privacy risks, compliance issues, cybersecurity threats, and future CSP involvement. The findings further support the need for trust, clear responsibility, and cooperation between organizations and CSPs to promote various regulations, especially GDPR. AI, ML, as well as the blockchain were noted to be arising technologies that provide solutions alongside presenting challenges. These insights shed light on the challenge and opportunities of Resource protection for cloud-based technologies and hence the Irish IT based organizations, policymakers and CSPs.

# Chapter 5: Discussion

## 5.1 Introduction

This chapter presents the research findings in light of the study objectives, LR and conceptual framework. These include discussions of core privacy and data protection threats, comparisons of GDPR efficacy, consumers’ cloud trust, and suggestions for improving data security and compliance. Every research aim is discussed, and the results are compared with previous works to highlight commonalities, discrepancies, and contributions. A comparison is made between the literature review and the study’s discoveries to identify similarities and disparities. The following chapter expands more on the implications of the findings on organizations, policymakers, and CSPs.

## 5.2 Alignment with the Research Objectives

### 5.2.1 Objective 1: To identify the key privacy and data security risks, including potential data leakage, associated with cloud computing in Ireland.

The study showed that threats in cloud computing services are data leak, unauthorized access, and system misconfiguration, which the participants stressed as vital risks. Some respondents pointed that misconfiguration in uncovered hence providing unauthorized access to data. Singh et al. (2023) also noted that misconfiguration is a primary reason for breaches in cloud systems. Moreover, weak authentication controls, which include basic passwords that are not protected with MFA, were cited as an area of risk with regards to unauthorized access. The new threats, like ransomware attacks or schemes that phish for information, were also often mentioned, explaining that cybercriminals capitalize on human weaknesses to compromise cloud networks. These findings are backed up by the literature; Powell (2022), discussed that there is a rise in complexity of ransomware attacks more so for multiple organizations sharing various resources in cloud environments. The existence of such risks is consequential for Irish IT organizations as it negatively affects their financial status, brand image, and consumers’ trust. Based on these findings, it is recommended that organisations place emphasis on security settings, security assessments and training for users as they prepare to deal with future threats.

### 5.2.2 Objective 2: To evaluate the effectiveness of current legal frameworks, particularly GDPR, in addressing these data security and privacy risks.

These results pointed out key difficulties Irish organization experiences while adopting GDPR compliance in cloud computing. Data transfers to third countries were identified as an issue, with respondents citing challenges of applying GDPR where data is located or processed in other countries. This is consistent with Li et al. (2019) who pointed that one of the major GDPR challenges is cross border data transfers because there is difference in legal requirements on the protection of data from one country to another. Further, burden distribution between CSPs and organizations causes confusion in the handling of data protection responsibilities and results in compliance weaknesses. According to participants, organizations tend to rely heavily on CSPs for implementing GDPR compliance solutions, believing that CSPs handle everything on their end. The study also highlighted challenges of addressing the 72-hour breach reporting regulation where the environment is complex and has multiple tenants in the clouds. Lapp (2024) maintained the same sentiment regarding the impossibility of timely reporting in a distributed system. Although GDPR offers a strong set of rules concerning data protection, several practical issues in its enforcement can still be identified. In order to meet GDPR requirements effectively there is a need to address SLAs in organizations, compliance audits, and forcing CSPs to come clean.

### 5.2.3 Objective 3: To assess the role of consumer trust in the adoption of cloud services amid concerns of data security and leakage.

The study revealed that trust from the consumer proved to be the significant driver for the adoption of cloud with data transparency, security and issues of unauthorized access as the main inhibitors. The research also showed that most people have no idea where their data is hosted and processed, which breeds distrust. Targets concerned the lack of CSPs’ transparency and explained that they received limited information on security and GDPR conformity. This is in line with what Michler et al. (2020) pointed out where trust drivers include transparency, accountability, security among others. In line with this, Deloitte (2023) revealed that more than half of the consumers are hesitated to use cloud services because of the open questions about privacy. That is why additional security features, including encryption, MFA, and real-time monitoring, were mentioned as the foundation for trust. The most significant enablers found involved cooperation between organizations and CSPs, for instance enhanced SLAs and shared security assessments. However, the insights focused on the peculiarities of the Irish market, and the essential role that GDPR compliance performs. This clarifies that transparency and accountability are crucial to improving the rate of cloud adoption, which requires trust.

### 5.2.4 Objective 4: To provide recommendations for organizations to enhance data protection practices, prevent consumer data leakage, and comply with privacy regulations.

The study revealed numerous suggestions for improving the protection of personal data and adherence to GDPR principles. Encryption was highlighted by participants as crucial to protect data when it is being transmitted and when stored but it was also noted that there was the need to adopt MFA. Security audits and security monitoring were seen as effective measures by which security risks need to be identified and to prevent them as far as possible. These findings are consistent with the literature presented in Ometov et al. (2018), where the authors recommended the multiple-layered protective model to secure cloud resources. Amendments to the Service-Level Agreements (SLAs) were a significant recommendation, where participants urged for adding more depth to the way CSPs and organizations allocate responsibilities. Another aspect was increased thoroughness of the compliance audits with a focus on repeated checks, joint security testing, and providing more information regarding the geolocation of data and data handling. Similar measures were outlined by Plumer (2024) where CSPs play a part of offering transparent compliance frameworks. The following recommendations give practical approaches to Irish IT organisations to contain technical threats, curb data leakage and meet the requirements of the upcoming GDPR policies.

## 5.3 Contrast and Comparison of Literature Review and Findings

### 5.3.1 Privacy Risks

Data leakage, misconfigured systems, and unlawful access were established as the leading risks in cloud computing, which was consistent with the existing research. The participants also echoed the findings of Singh et al. (2023) and Powell (2022) that misconfiguration in multi-tenant cloud environments result in data breaches due to misconfigured access controls. Likewise, another new prevalent threat identified in both the research and in the literature were ransomware attacks and phishing schemes with enhanced complexity. However, the findings provided a nuanced insight: the participants noted that individuals’ mistakes like the creation of fragile passwords and poor IAM implementation still play a crucial role, a factor that previous research often neglects. This means that together with the technical solutions, there is a need for increased efforts to educate users about threats.

### 5.3.2 GDPR and Legal Framework

Consequently, the study findings and literature concur with GDPR being an effective legal framework for data privacy, albeit with a practical application problem. For example, Li et al. (2019) and IAPP (2024) pointed out the cross-border data transfer challenges, a concern reflected by participants who had issues regarding GDPR compliance while using cross-border cloud solutions. Another issue brought into focus was the shared responsibility model as a source of confusion, where the organisations lean too much on CSPs for GDPR compliance, this was also as evident from literature. Participants augment to the 72-hour breach reporting requirement by pointing to it as seriously implausible within dispersed cloud structures, an absurdity highlighted in earlier analyses. Such a gap indicates that GDPR is effective but needs better implementation guidance in the cloud context.

### 5.3.3 Consumer Trust

The study’s results upheld that the levels of consumer trust rely on transparency, security, and clarity of how data is managed which supports the research done by Michler et al. (2020) and Deloitte (2023). The participants stressed the importance of CSPs to declare data storage and compliance policies as discussed in literature where there is a call for more transparency of firms to rebuild consumer trust. The research is novel in demonstrating that consumer scepticism is higher in Ireland because of GDPR concerns and continuously emerging risks such as ransomware. Participants revealed trust deficiencies unique to sectors often associated with high risk, for example, the health and financial sectors. This is why it is important to look into sector specific solutions as far as issues of consumers are concerned in these sectors.

### 5.3.4 Emerging Technologies

The study reaffirmed the literature’s assertion that AI, ML, and Blockchain can go a long way to improve cloud privacy and security. Ometov et al. (2018) listed AI/ML in threat detection and anomaly detection, which the participants recognised as helpful features for live monitoring. However, the findings added a unique dimension: participants expressed some concern with privacy issues they anticipated due to training an AI algorithms, with large data sets, something that literature has often ignored. In the same manner, both the findings and literature review recognized the efficiency of blockchain in enhancing transparency and accountability within data. However, they highlighted some practicality issues and drawbacks, including scale up and its relatively high implementation cost.

## 5.4 Implications of Findings

The implication for Irish organizations, policymakers and the CSPs are as follows. In terms of risks mitigation, it is clear that organizations should focus on such critical measures as data encryption, multi-factor authentication, and regular security assessments to mitigate such threats as data leakage, misconfigurations, and ransomware. Within Service-Level Agreements (SLAs), organizations should define responsibilities and avoid outsourcing GDPR compliance to CSPs. Employees need to be made more aware of the risks of cyber security and must also be trained on how to avoid them some of which are key causes of cloud security threats.

To policymakers, it presents a reality that there is a need for more actionable and practical guidance on GDPR implementation to organizations using cloud services, especially on cross-border data transfers and breach notification time frames. Authorities should also enhance structures for the relations between CSPs and organizations to combat non-compliance while addressing transparency issues. Additional measures that would provide increased consumer confidence include other specific regulations, for sectors such as healthcare and financial services.

The research results for CSPs focus on better data openness, providing compliance navigations, and making the information about data usage clearer. When incorporating tools like the interactive compliance dashboards as well as conducting security audits together with the organizations, then trust and accountability is instilled. The general implications of such findings are related to the enhancement of GDPR enforcement and consumer trust. They need to address privacy concerns, increase transparency, and manage new risks which will assist organisations to meet GDPR standards and gain more consumer trust. Lastly, these measures will lead to the increased use of cloud solutions in Ireland’s IT industry as well as safe data protection.

## 5.5 Limitations of the Study

1. **Small Sample Size**: The study involved only 10 participants from the IT and data protection fields, which limits the applicability of the research findings to the overall IT sector in Ireland. The qualitative study gave detailed information but having more cases could have given different perspectives and enhanced the credibility of the study findings.
2. **Qualitative Approach**: The use of semi structured interviews is a source of bias since the findings are interpreted from participants’ experiences or opinions. This could bring bias and numeracy could be impacted on while determining privacy risks or even compliance with GDPR. It also means that using a mixed-methods approach that includes quantitative data could give more accurate results.
3. **Participant Bias**: The participants were restricted to IT professionals this may explain why the study was biased towards technical factors. Engaging other stakeholders, for instance, policymakers or consumers might have provided a more inclusive view on the concerns and trust issues related to cloud adoption.
4. **Focus on Irish Context**: The research was conducted only in the Irish context, and therefore, it could not have reached the same conclusions for other jurisdictions with dissimilar regulatory regimes to that of Ireland. Future research could include a cross-country analysis of GDPR implementation and Cloud privacy concerns.
5. **Dynamic Nature of Cloud Security**: Some of the results might also be somewhat static since cloud technologies develop rapidly and new threats appear frequently. Constant research is required to put up with new risks and regulations, but also development in cloud privacy technology.

## **5.6 Conclusion**

In this chapter, the research findings have been presented and made a connection with the study objectives, review of the literature, and conceptual framework. Data leakage, misconfiguration and ransomware risk cases were discussed along with GDPR compliance issues like cross-border transfer and shared accountability. Consumer trust and responsibility of cloud adoption were highlighted, as well as strategies for improving data security and compliance. The results obtained are relevant to the research objectives and present the core concern of cloud privacy in Ireland. In the final chapter, the study conclusions and practical implications for organisations, policies and CSPs are presented.

# Chapter 6: Conclusion and Recommendations

## 6.1 Introduction

This final chapter presents an overview of the study results, their theoretical implications, practical implications, and recommendations for organisations, policymakers, and CSPs. The study presented crucial privacy and security concerns in cloud computing, assessed the suitability of GDPR, as well as investigated the part of the consumer trust in cloud usage in Ireland’s IT market. Realistic measures were recommended to improve the protection of data and increase compliance. Further, this chapter also presents the limitations of the study and recommendations for further research to invest continued effort in researching cloud privacy, security, and regulation as technologies evolve and advance further.

## 6.2 Summary of Key Findings

The analysis focused on the key issues concerning cloud computing privacy and security, however, the results were linked to the objectives established at the beginning of the study.

### 6.2.1 Privacy and Data Security Risks

This research established that data leakage, unauthorized access, and system misconfiguration were the critical risks for cloud computing environments. They noted that the leakage of data is common in multi-instance shared cloud platforms where the possibility of exposing data to unintended parties is higher due to misconfigurations. Furthermore, poor IAM controls, including non-existent password and MFA policies also featured as aggravating factors for unauthorized access. Human error, which is often a cause, deepens these vulnerabilities repeatedly. The threats that are on the rise were also indicated, including ransomware and phishing. Several participants pointed out that ransomware designed to attack cloud-based solutions has advanced to infect multi-tenant cloud environments. These results accentuate the fact that, while cloud technologies provide scalability and flexibility, security settings have to be strong and maintained consistently to protect privacy.

### 6.2.2 Compliance Challenges

The findings showed that several challenges exist when it comes to GDPR compliance in cloud services including on issues of cross-border data transfers and shared responsibility model. They highlighted challenges with regard to compliance of data in the clouds located outside EU, especially after Schrems II ruling which rejected the EU-US Privacy Shield. Lack of clarity on who does what between CSPs and the client organization was a common issue of debate. Several organizations lean heavily on CSPs for compliance, believing that the providers take full responsibility for data protection. Thirdly, the 72-hour breach notification was keyed out as ineffective given that it is practically impossible to detect and report breaches in distributed cloud systems. These studies inform the need to establish objective and consistent compliance standards and to improve organizational efficiency and cooperation between CSPs and organizations in the context of GDPR compliance.

### 6.2.3 Cybersecurity Threats

The study noted ransomware attacks, phishing schemes, and misconfigurations of cloud systems as the most pertinent cybersecurity threats. Ransomware for instance was cited as an emerging threat which attacks multiple tenants in the cloud where the infection of one renter is capable of affecting others. Phishing attacks, leveraging human vulnerability, continue to be a frequent approach towards unauthorized access to cloud environments. Employees were also reported as easy subjects for phishing, and hence the importance of raising awareness among the users. The use of system configurations, which include bad access controls, wrong security settings as well as other security flaws, were found out to have contributed to a big extent to these breaches. Such studies’ results imply that to mitigate cybersecurity risks, some advanced technical solutions (encryption, real-time monitoring) should be complimented with more general approach, including training programs and anticipating threats.

### 6.2.4 CSP Collaboration

The findings pointed out that it is imperative to engage CSPs in order to mitigate risks associated with privacy and compliance with relevant regulations. To ensure truth in advertising, participants recommended enhancements to the disclosure of CSP data storage facility, confidentiality, and legal compliance policies. Specific issues that were questioned include the shared responsibility model, which means that there are no clear breakdowns of the parties responsible for data protection. Some suggested that SLAs should be improved to outline expectations of the involved parties for action in case of the occurrence of breaches or non-compliance. Other important strategies of enhancing security and cooperation between an organization and CSPs also included the need to engage in joint security audits and collaborated efforts in threat detection. Another implication of the study is that for cloud security to be strong, CSPs and their clients need to be engaged in trust and cooperation.

### 6.2.5 Emerging Technologies

The use of AI, ML, and blockchain solutions to improve cloud privacy and security was another important trend. It was suggested that AI and ML could enhance the success of threat detection by providing real-time data anomaly detection and analytical insights. Some people said that big datasets could be used to train Al and this may become a threat to people’s privacy. Blockchain was described as a viable method for achieving data transparency and making the data trail accountable especially in multi-actor cloud contexts. However, scalability and integration difficulties were mentioned as the issues that prevent the use of this approach. The results stress that despite technologies’ novelty, they present opportunities for development, yet they are still accompanied by technical, cost and privacy issues.

## 6.3 Contributions of the Study

### 6.3.1 Theoretical Contributions

From a theoretical perspective, the significance of this study lies in the fact that it fills gaps in the literature concerning privacy concerns and GDPR implementation in the context of the Irish IT sector. Though earlier literature explores the global or EU-based threats, this study offers setting-specific insights into privacy threats experienced by Irish companies, including data leaks, system misconfigurations, and unauthorized access. The study also improves the understanding of GDPR’s real-life applicability in cloud environments by examining issues such as cross-border data transfers and shared responsibility models. Another significant focus of the study is on the future solutions and advances in cloud security, in particular AI, ML, and blockchain. Whereas prior literature focuses on their benefits, this work focuses on both of these aspects, revealing threat and data-related benefits as well as privacy and implementation downsides. These insights enrich the theoretical body of knowledge about new technologies and their roles in the emerging nature of cloud security.

### 6.3.2 Practical Contributions

The conclusion reveals the practical recommendations that can guide organizations in enhancing their data protection and GDPR compliance. Measures including the deployment of encryption, MFA, periodic security assessments, and enhanced SLAs are effective in tackling technical flaws and defining roles and responsibilities. The following are some of the ways through which it would help organizations to deal with the privacy risks and bring about a compliance to the regulations. For policymakers, the study presents a roadmap on how to reinforce the overall enforcement of GDPR by clarifying how cross-border data transfers work, improving the breach notification rules and designing industry-specific standards for sectors such as healthcare and finance. Focussing on CSPs as the object of research, it highlights the need to enrich data and increase collaboration with client organizations. Engaging ideas like using interactive compliance dashboards, performing security audits together, and increasing awareness regarding Data processing promote trust and responsibility.

## 6.4 Recommendations

### 6.4.1 Recommendations for Organizations

1. **Implement Technical Safeguards**: Technological safeguards including data encryption, MFA, and monitoring must be employed as part of a strong security strategy for organisations. Encryption protects information at rest and in motion, while MFA allows only an authorized user to access the data. Using tools such as intrusion detectors, real-time monitoring helps in detection of weaknesses and counter acts that can prevent advance breaches. Such measures are crucial in managing threats such as data spills, invasions of privacy, and ransomware threats.
2. **Conduct Regular Security Audits and Penetration Tests**: Organizations should conduct periodic security reviews and vulnerability scans to assess cloud configurations and permissions. Scheduling helps to identify and fix potential weaknesses due to misconfiguration or outdated levels of protection. Audits also improve compliance with GDPR and other privacy rules because technical protections match best practices. These are proactive measures that should be employed to minimize risks and enhance the confidence of consumers in the cloud solutions.

### 6.4.2 Recommendations for Policymakers

1. **Develop Sector-Specific GDPR Guidelines**: Government officials should develop compliance standards for sectors, which can involve working with consumer data like healthcare and finance. Such guidelines can offer possible practical recommendations to solve potential and existing privacy problems and conform to GDPR rules. For instance, enhanced restrictions on data processing and storage, encryption, and audit requirements can be significant in deterring organizations in risky industries from non-compliance.
2. **Streamline the 72-Hour Breach Reporting Process**: Another issue is that the 72-hour breach notification described in GDPR needs to be developed taking into consideration the specifics of cloud environments. This encompasses offering realistic advice on how to discover and report breaches especially in multifaceted systems. This will alleviate the compliance burden on organizations while at the same time enhance their reporting efficiency. There is also a need for policymakers to engage CSPs to develop a single framework of reporting on cloud infrastructures.

### 6.4.3 Recommendations for Cloud Service Providers (CSPs)

1. **Improve Data Transparency**: CSPs need to improve the oversight of location, processing, and compliance related to data storage and processing necessities. Explaining in detail where the data is held and how the storage is compliant with GDPR will help to assuage the fears of organizations with regards to cross-border transfer. Self-service solutions that provide near real-time visibility into data flows, as well as compliance with or violations of privacy initiatives, can greatly enhance trust and accountability.
2. **Strengthen Service-Level Agreements (SLAs) and Collaboration Tools**: CSPs should adjust the SLAs to precisely describe the extent of responsibilities under the shared responsibility model so that organizations fully grasp their role under the GDPR. Providing services like integrated security assessment and shared service solutions like true-time threat identification systems will boost CSP and client engagement. It will be helpful in timely informing about new threats and privacy risks to allow organizations promptly adapt to new cybersecurity threats.

## **6.5 Final Conclusion**

This research focused on an important area of enquiry which is the privacy threat and GDPR regulation in cloud computing amongst the IT firms in Ireland. The research focused on issues of data leakage, unauthorized access, and ransomware attacks that are inhibiting the use and trust in cloud services. It also further examined the difficulties that organisations experience in implementing the GDPR, especially the transfer of data across borders, shared liability frameworks, and breach notifications. These findings accentuated the significance of technology as the key enabler while promoting more stringent data protection measures.

The challenges of managing knowledge work are clearly highlighted in this study, and the conclusions and recommendations are practical guidelines to the issue. The adoption of measures such as encryption, MFA, and recurrent security assessments can improve the security of cloud solutions and compliance with regulations for organizations. Policy makers can bolster GDPR frameworks by providing industry specific guidance and aligning breach notification procedures to cloud environments. To Cloud Service Providers (CSPs), data transparency, security tools and workable SLAs would help to increase accountability and credible relationship with organisations which are clients.

Implementing these recommendations can help reduce cloud privacy risks, address compliance deficiencies, and, most importantly, bring more people into the fold, which is essential for the widespread use of cloud technologies. An effective relationship between organizations and CSPs can help reduce the privacy issue significantly especially in sectors with high regulatory requirements such as health and financial. Enhancing protective measures for data and legal requirements will not only protect the personal information of consumers but also contribute to the enhanced safety and reliability of the cloud environment in Ireland. Building confidence in cloud solutions will foster the growth of the IT sector’s capability in Ireland and bolster Ireland as a champion of secure cloud expertise resulting in effective and sustainable economic progress within the digital age.

# References

Abrera, J., (2024). Data Privacy and Security in Cloud Computing: A Comprehensive Review. *Journal of Computer Science and Information Technology*, *1*(1), pp.01-09.

Abrera, J., (2024). Data Privacy and Security in Cloud Computing: A Comprehensive Review. *Journal of Computer Science and Information Technology*, *1*(1), pp.01-09.

Accenture (2024). *The Empowered Consumer*. [online] Accenture.com. Available at: <https://www.accenture.com/bg-en/insights/consulting/empowered-consumer> [Accessed 26 Oct. 2024].

Adeoye‐Olatunde, O.A. and Olenik, N.L. (2021). Research and scholarly methods: Semi‐structured interviews. *JACCP JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY*, [online] 4(10), pp.1358–1367. doi:https://doi.org/10.1002/jac5.1441.

Al-Ali, A. (2017) ‘The Cloud Computing Security Issues and Challenges (In the SaaS Delivery Model)’, *Journal of Social Affairs*, 34(135), pp. 241–252. doi:10.12816/0042909.

Alharahsheh, H. and Pius, A. (2020). A Review of Key paradigms: Positivism Vs Interpretivism. *Global Academic Journal of Humanities and Social Sciences*, 2(3), pp.39–43. doi:https://doi.org/10.36348/gajhss.2020.v02i03.001.

Ali, O., Shrestha, A., Osmanaj, V. and Muhammed, S., (2021). Cloud computing technology adoption: an evaluation of key factors in local governments. *Information Technology & People*, *34*(2), pp.666-703.

Anna-Maija Pietilä, Nurmi, S.-M., Arja Halkoaho and Helvi Kyngäs (2019). Qualitative Research: Ethical Considerations. *Springer eBooks*, [online] pp.49–69. doi:https://doi.org/10.1007/978-3-030-30199-6\_6.

Annan, D.F. and Filippaios, F. (2017) ‘Multinational Firms’ Motivations and Foreign Direct Investment Decisions: An Analysis of the Software and IT and Financial Services Sectors in the Irish Context’, *Thunderbird International Business Review*, 59(6), pp. 739–755. doi:10.1002/tie.21896.

Bhatia, K., (2021). Data Protection Overview in Ireland. *Supremo Amicus*, *27*, p.246.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D. and Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of research in nursing*, [online] 25(8), pp.652–661. doi:https://doi.org/10.1177/1744987120927206.

Carcary, M., Doherty, E. and Conway, G. (2014) ‘The Adoption of Cloud Computing by Irish SMEs -- an Exploratory Study’, *Electronic Journal of Information Systems Evaluation*, 17(1), pp. 3–14. Available at: https://research.ebsco.com/linkprocessor/plink?id=5286ec1f-ce3d-3acc-8546-377c4cda0053 (Accessed: 26 October 2024).

Coleman, P. (2022). The Open University. *Open.ac.uk*. [online] doi:https://oro.open.ac.uk/81588/1/Coleman%20Validity%20and%20Reliability.pdf.

Cory, N., Castro, D. and Dick, E. (2020). *‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*. [online] Itif.org. Available at: <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/#:~:text=The%20ECJ's%20ruling%20invalidated%20the,must%20use%20alternative%20transfer%20mechanisms>. [Accessed 26 Oct. 2024].

Data Protection Commission. (2024). *Data Protection Commission*. [online] Available at: <https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million> [Accessed 26 Oct. 2024].

Deloitte . (2021). *Cloud Index Survey*. [online] Available at: <https://www.deloitte.com/ie/en/services/consulting/analysis/cloud-index-survey.html> [Accessed 26 Oct. 2024].

Deloitte. (2021). *Cloud Index Survey*. [online] Available at: <https://www.deloitte.com/ie/en/services/consulting/analysis/cloud-index-survey.html> [Accessed 26 Oct. 2024].

Dempsey, D. and Kelliher, F., (2018). Industry trends in cloud computing. *Pallgrave McMillian, New York*.

Denieffe, S. (2020). Commentary: Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, [online] 25(8), pp.662–663. doi:https://doi.org/10.1177/1744987120928156.

‌digitalisationworld.com (2015). *Nearly 90% of UK businesses now use cloud services*. [online] Digitalisation World. Available at: <https://digitalisationworld.com/news/46709/nearly-90-of-uk-businesses-now-use-cloud-services> [Accessed 26 Oct. 2024].

economictimes.indiatimes.com (2024). *Ireland fines Meta €91 million over EU data breach*. [online] The Economic Times. Available at: <https://economictimes.indiatimes.com/tech/technology/ireland-fines-meta-91-million-over-eu-data-breach/articleshow/113768009.cms?from=mdr> [Accessed 26 Oct. 2024].

Enterprise.gov.ie. (2018). *Data Protection and the General Data Protection Regulation (GDPR)*. [online] Available at: <https://enterprise.gov.ie/en/who-we-are/corporate-information/data-protection/> [Accessed 26 Oct. 2024].

‌esoftskills (2024). *The Growth of Cloud Computing in Ireland*. [online] ESOFT Lifelong Learning. Available at: <https://esoftskills.ie/the-growth-of-cloud-computing-in-ireland/> [Accessed 26 Oct. 2024].

‌fDi Intelligence (2020). *Big tech picks Ireland as data centre hub*. [online] Fdiintelligence.com. Available at: <https://www.fdiintelligence.com/content/data-trends/big-tech-picks-ireland-as-data-centre-hub-78473> [Accessed 26 Oct. 2024].

‌First Response (2022). *Incident Response for Ransomware*. [online] First Response. Available at: https://first-response.co.uk/articles/incident-response-for-ransomware/ [Accessed 26 Oct. 2024].

First Response (2022). *Incident Response for Ransomware*. [online] First Response. Available at: https://first-response.co.uk/articles/incident-response-for-ransomware/ [Accessed 26 Oct. 2024].

Gammelgaard, B. and Nowicka, K., (2024). Next generation supply chain management: the impact of cloud computing. *Journal of Enterprise Information Management*, *37*(4), pp.1140-1160.

Gartner. (2024). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024*. [online] Available at: <https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240> [Accessed 26 Oct. 2024].

GDPR.eu. (2018). *What are the GDPR Fines? - GDPR.eu*. [online] Available at: <https://gdpr.eu/fines/> [Accessed 26 Oct. 2024].

General Data Protection Regulation (GDPR). (2018). *General Data Protection Regulation (GDPR) – Final text neatly arranged*. [online] Available at: <https://gdpr-info.eu/art-28-gdpr/#:~:text=Processing%20by%20a%20processor%20shall,type%20of%20personal%20data%20and> [Accessed 26 Oct. 2024].

González, D.A., Gonzales, M.M., Resch, Z.J., Sullivan, A.C. and Soble, J.R. (2021). Comprehensive Evaluation of the Functional Activities Questionnaire (FAQ) and Its Reliability and Validity. *Assessment*, [online] 29(4), pp.748–763. doi:https://doi.org/10.1177/1073191121991215.

Gov.uk (2017). *Government Cloud First policy*. [online] GOV.UK. Available at: <https://www.gov.uk/guidance/government-cloud-first-policy> [Accessed 26 Oct. 2024].

Han, Y. (2011) ‘Cloud Computing: Case Studies and Total Costs of Ownership’, *Information Technology & Libraries*, 30(4), pp. 198–206. Available at: https://research.ebsco.com/linkprocessor/plink?id=7b07f93f-d953-32e4-ae13-02ace2b6f5c0 (Accessed: 26 October 2024).

Hjerppe, K., Ruohonen, J. and Leppänen, V., (2019). The general data protection regulation: requirements, architectures, and constraints. In *2019 IEEE 27th International Requirements Engineering Conference (RE)* (pp. 265-275). IEEE.

Iapp.org. (2024). *IAPP*. [online] Available at: <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act> [Accessed 26 Oct. 2024].

Kamal, S.S.L.B.A., (2019) Research paradigm and the philosophical foundations of a qualitative study. *PEOPLE: International Journal of Social Sciences*, *4*(3), pp.1386-1394.

Kant, H.K., (2019). Cloud Computing. BPB Publications.

Khayer, A., Jahan, N., Hossain, M.N. and Hossain, M.Y., (2021). The adoption of cloud computing in small and medium enterprises: a developing country perspective. *VINE Journal of Information and Knowledge Management Systems*, *51*(1), pp.64-91.

‌Li, H., Yu, L. and He, W., (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), pp.1-6.

Liu, S., Chan, F.T., Yang, J. and Niu, B., (2018). Understanding the effect of cloud computing on organizational agility: An empirical examination. *International Journal of Information Management*, *43*, pp.98-111.

‌Lynn, T.G., Mooney, J., Lisa and Fox, G. (2020). *Data Privacy and Trust in Cloud Computing*. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/344810026_Data_Privacy_and_Trust_in_Cloud_Computing> [Accessed 26 Oct. 2024].

Michler, O., Decker, R. and Stummer, C., (2020). To trust or not to trust smart consumer products: a literature review of trust-building factors. *Management Review Quarterly*, *70*(3), pp.391-420.

Microsoft.com. (2024). *Collaboration Tools and Solutions for Business | Teams*. [online] Available at: <https://www.microsoft.com/en-us/microsoft-teams/collaboration> [Accessed 26 Oct. 2024].

Mirza, H., Mirza, C. and Bellalem, F., (2023) Ethical considerations in qualitative research: Summary guidelines for novice social science researchers. *Social Studies and Research Journal*, *11*(1), pp.441-449.

Muzari, T., Shava, G.N. and Shonhiwa, S. (2022). *Qualitative research paradigm, a key research design for educational researchers, processes and procedures: A theoretical overview*. [online] Available at: <https://indianapublications.com/articles/IJHSS_3(1)_14-20_61f38990115064.95135470.pdf>.

Naz, N., Gulab, F. and Aslam, M., (2022) Development of qualitative semi-structured interview guide for case study research. *Competitive Social Science Research Journal*, *3*(2), pp.42-52.

Nickerson, C., (2022) Interpretivism paradigm & research philosophy. *Simply Sociology*, *5*.

O’Dowd, J. (2023). *Cybersecurity Week in Review (27/10/2023) - Smarttech247*. [online] Smarttech247. Available at: <https://www.smarttech247.com/news/cybersecurity-week-in-review-27-10-2023-2/> [Accessed 26 Oct. 2024].

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), p.1.

Plumer, N., (2024). *Cybersecurity Maturity Assessment: Integrating IAM into Zero Trust Model for Peruvian Universities* (Doctoral dissertation, St. Thomas University).

Powell, O. (2022). *The biggest data breaches and leaks of 2022 | Cyber Security Hub*. [online] Cyber Security Hub. Available at: <https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022> [Accessed 26 Oct. 2024].

PricewaterhouseCoopers (2023). *Digital Trust Insight Survey 2023 — Report | PwC Ireland*. [online] PwC. Available at: https://www.pwc.ie/reports/global-digital-trust-insight-survey-2023.html [Accessed 26 Oct. 2024].

‌PricewaterhouseCoopers (2023). *Digital Trust Insight Survey 2023 — Report | PwC Ireland*. [online] PwC. Available at: <https://www.pwc.ie/reports/global-digital-trust-insight-survey-2023.html> [Accessed 26 Oct. 2024].

Proudfoot, K. (2022). Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research. *Journal of Mixed Methods Research*, [online] 17(3), pp.308–326. doi:https://doi.org/10.1177/15586898221126816.

Puljak, L. *et al.* (2020) ‘Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions’, *Biochemia Medica*, 30(3), pp. 1–8. doi:10.11613/BM.2020.030201.

Ruslin, R., Mashuri, S., Rasak, M.S.A., Alhabsyi, F. and Syam, H., (2022) Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR Journal of Research & Method in Education (IOSR-JRME)*, *12*(1), pp.22-29.

S. Rajashekar and Jain, A. (2023). A Thematic Analysis on ‘Employee Engagement in IT Companies from the Perspective of Holistic Well-being Initiatives’. *Employee Responsibilities and Rights Journal*, [online] 36(2), pp.165–187. doi:https://doi.org/10.1007/s10672-023-09440-x.

‌Singh, C., Thakkar, R. and Warraich, J., (2023). IAM identity Access Management—importance in maintaining security systems within organizations. *European Journal of Engineering and Technology Research*, *8*(4), pp.30-38.

Sisodia, S. *et al.* (2024) ‘Navigating the Cloud: Choosing the Right Cloud Computing Services for Your Business’, *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Humanitarian Technology Conference (KHI-HTC), 2024 IEEE 1st Karachi Section*, pp. 1–8. doi:10.1109/KHI-HTC60760.2024.10481894.

Statista. (2020). *Ireland: public cloud market revenue 2020-2029 | Statista*. [online] Available at: <https://www.statista.com/forecasts/963866/cloud-services-revenue-in-ireland> [Accessed 26 Oct. 2024].

Swain, J. (2018). A Hybrid Approach to Thematic Analysis in Qualitative Research: Using a Practical Example - UCL Discovery. *Ucl.ac.uk*. [online] doi:https://discovery.ucl.ac.uk/id/eprint/10042537/1/Swain\_Sage%20analysis%20article%20July%2020171\_.pdf.

Tabrizchi, H. and Kuchaki Rafsanjani, M., (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.

‌Thalesgroup.com. (2024). *2023 Cloud Security Report Shows Many Data Breaches - Press Release*. [online] Available at: <https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release> [Accessed 26 Oct. 2024].

The Insight Partners (2023). *Cloud Computing Market Share Size and Trends 2028*. [online] The Insight Partners. Available at: <https://www.theinsightpartners.com/reports/cloud-computing-market> [Accessed 26 Oct. 2024].

The Irish Data Protection Commission (2022). *Data Protection Commission.* Available at: <https://www.dataprotection.ie/sites/default/files/uploads/2024-05/DPC%20EN_AR%202023_Final%20.pdf>

‌trade.gov (2022). *Ireland Digital Transformation Strategy*. [online] International Trade Administration | Trade.gov. Available at: <https://www.trade.gov/market-intelligence/ireland-digital-transformation-strategy> [Accessed 26 Oct. 2024].

Voss, W.G., (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, p.485.

Waldrop, M.M., (2018). *The dream machine*. Stripe Press.

Wittig, A. and Wittig, M., (2023). *Amazon Web Services in Action: An in-depth guide to AWS*. Simon and Schuster.

‌Wood, W.J., (2019). *Exploring Firm-Level Cloud Adoption and Diffusion*. Walden University.

Yadav, D. (2021). Criteria for Good Qualitative Research: A Comprehensive Review. *The Asia-Pacific Education Researcher*, [online] 31(6), pp.679–689. doi:https://doi.org/10.1007/s40299-021-00619-0.

Yang, P., Xiong, N. and Ren, J., (2020). Data security and privacy protection for cloud storage: A survey. *Ieee Access*, *8*, pp.131723-131740.

# Appendices

## Appendix 1: Interview Questions

1. Can you describe your responsibilities and role in your current organization?
2. How long have you been working in the field of cloud computing and data security?
3. How do you define security and privacy in the context of cloud computing?
4. What is the primary privacy concerns related to storing customer data in the cloud?
5. In your experience, define what are the most common causes of data breaches within a cloud environment?
6. Can you share any examples or case studies of significant data breaches, data theft, and malware attacks you have encountered or studied?
7. How do you collaborate with cloud service providers to address shared responsibility challenges, and what improvements do you think are needed in these partnerships to enhance data security?
8. What measures do you think are the most effective to ensure that customers maintain control over their data?
9. What are the biggest challenges you face to ensure compliance with data privacy regulations?
10. What technical measures do you implement to protect customer data in the cloud?
11. How do emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, affect data privacy and security within cloud computing environments?
12. In your opinion, how aware are customers of the data privacy risks associated with cloud computing, and what role should cloud service providers play in educating consumers about these risks?