

**Digital Transformation of Tourism and Corporate Digital
Responsibility:
A case study of the tourism industry in Aotearoa**

Ying-Can Chen

**A dissertation submitted to
Auckland University of Technology
in partial fulfilment of the requirements for the degree of
Master of International Tourism Management (MITM)**

**Supervisor: Dr Pola Wang
Faculty of Culture and Society**

2025

Abstract

With the rise of digital transformation across industries, Corporate Digital Responsibility (CDR) emerges as a concept for ensuring ethical digital practices within organisations. Effective implementation of CDR helps organisations stay ahead of digital transformation. It creates broad social and economic value while minimising the potential risks posed by digital technologies. However, the implementation of CDR in the New Zealand tourism industry still faces many challenges, including the complexity of data governance, legal compliance requirements, and the difficulty of deeply integrating CDR into core strategies.

This study adopts a qualitative research methodology, collecting data from the official websites of New Zealand travel agencies. Using thematic analysis, the research examines publicly available content—particularly privacy policies, terms and conditions, and digital communication practices—to assess the extent to which CDR principles are reflected in practice. The findings show that while some travel agencies demonstrate partial engagement with CDR principles, many fall short in areas such as transparency, accountability, and stakeholder inclusion. A significant gap remains between legal compliance and the proactive implementation of digital responsibility.

The study highlights the need for stronger CDR frameworks, clearer governance structures, and industry-wide best practices to support ethical digital transformation.

Overall, it underscores the crucial role of CDR in promoting long-term sustainability and trust within the tourism sector.

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signed: YING - Can - CHEN

Date: 25 / 02 / 2025

Acknowledgements

Upon completing this study, I would like to express my sincerest gratitude to all the individuals and institutions who provided support, help, and guidance throughout this study.

First, I would like to extend my heartfelt thanks to my supervisor, Dr. Pola Wang, for her invaluable guidance and advice during the research process. Her professional expertise and patience helped me overcome many challenges and provide clear direction for my research.

I am deeply grateful to my university, Auckland University of Technology, for providing an excellent research environment and access to resources, enabling me to complete the literature review and analysis. Special thanks to the relevant departments and teams for their assistance and understanding during critical times.

I would also like to thank the travel agents in New Zealand whose open data contributed significantly to this study. The information shared on their websites was essential in understanding the complexities of Corporate Digital Responsibility (CDR) in the tourism industry.

Finally, I would like to thank my family and friends for their unwavering encouragement, understanding, and support throughout the research process.

This study could not have been completed without the contributions of everyone involved. Once again, I express my deepest gratitude to all the individuals and organisations who have supported and contributed to this study.

Table of Contents

ABSTRACT	1
ATTESTATION OF AUTHORSHIP	3
ACKNOWLEDGEMENTS	4
LIST OF FIGURES	8
LIST OF TABLES	8
INTRODUCTION	10
1.1 RESEARCH BACKGROUND.....	10
1.2 RESEARCH OBJECTIVES AND QUESTIONS.....	12
RESEARCH QUESTIONS:	13
1.3 SIGNIFICANCE OF THE STUDY	14
1.4 STRUCTURE OF THE DISSERTATION	16
LITERATURE REVIEW	18
2.1 TOURISM INDUSTRY IN NEW ZEALAND	18
2.2 DIGITAL TRANSFORMATION IN TOURISM INDUSTRY	23
2.3 CORPORATE DIGITAL RESPONSIBILITY	28
2.4 KEY ELEMENTS FOR THE IMPLEMENTATION OF CDR	32
2.4.1 <i>PRIVACY</i>	37
2.4.2 <i>LEGISLATION</i>	41
2.4.3 <i>GUIDANCE</i>	43
2.5 SUMMARY.....	45
RESEARCH METHODOLOGY	47
3.1 RESEARCH PARADIGM	47
3.2 RESEARCH METHOD	50
3.3 DATA COLLECTION	51
3.4 SAMPLING.....	53
3.5 DATA ANALYSIS TECHNIQUES	55
3.6 ETHICS CONSIDERATIONS	60
FINDINGS	62
4.1 PRIVACY	62
4.1.1 <i>PRIVACY POLICY VISIBILITY</i>	62
4.1.2 <i>COMPLIANCE WITH LEGAL OBLIGATIONS</i>	64
4.1.3 <i>SCOPE AND PURPOSES OF PERSONAL DATA COLLECTED</i>	67
4.1.4 <i>DATA DISCLOSURE</i>	71
4.1.5 <i>ADDITIONAL FINDINGS</i>	76

4.2	LEGAL COMPLIANCE	78
4.3	GUIDANCE	84
4.4	DATA MANAGEMENT	87
4.5	SUMMARY	93
	DISCUSSION	98
5.1	DISCUSSION OF FINDING	98
5.2	RESEARCH QUESTIONS	101
5.3	THEORETICAL IMPLICATIONS	105
5.4	PRACTICAL IMPLICATIONS	107
5.5	LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH.....	111
5.6	CONCLUSION.....	112
	REFERENCES.....	114

List of Figures

FIGURE 1: MONTHLY OVERSEAS VISITOR ARRIVALS, MAY 2014-2024	21
FIGURE 2: CDR IMPLEMENTATION.....	36
FIGURE 3: PHASES OF THEMATIC ANALYSIS	56
FIGURE 4: TABLE WITH CODED EXAMPLES.....	57
FIGURE 5: EXAMPLE OF CODING DEFINITION AND NAMING THEME.....	58
FIGURE 6: SAMPLE COMMERCIAL WEBSITE	63
FIGURE 7: EXAMPLE OF TRRAVEL AGENCY PRIVACY POLICY PAGE	66
FIGURE 8: CDR PRACTICE IN NEW ZEALAND TOURISM.....	94

List of Tables

TABLE 1: SAMPLE SELECT	53
TABLE 2: TRAVEL AGENCIES WITH PROVIDE DISCLOSED	71
TABLE 3: TRAVEL AGENCIES DATA MANAGEMENT AND SECURITY PRACTICES.....	88

Introduction

1.1 Research Background

Tourism, especially international tourism, has traditionally been a significant driver of national and regional economic development (Li et al., 2018). With the end of the COVID-19 pandemic, cross-border leisure and business travel volume has been increasing, and tourism is gradually returning to pre-pandemic levels. Tourism generates employment, stimulates economic growth, and attracts investment. Moreover, tourism is a vital source of income for a country and plays a crucial role in promoting global awareness of its local culture and natural environment (Chambers, 2009). Therefore, the tourism industry holds significant importance in a country's development and needs to innovate and grow steadily. This study examines the growth trends of the tourism sector in New Zealand and explores how Corporate Digital Responsibility (CDR) contributes to its sustainable and ethical digital transformation.

In recent years, the rise of digital technology has further accelerated the growth of industries worldwide, and the tourism industry is no exception. As technology evolves, digitalisation has opened up numerous possibilities for businesses to interact with customers (Warner & Wäger, 2019). The personalisation and convenience offered by technology play a critical role in enhancing customer experience and satisfaction (Foroudi et al., 2018). Digital technology has equipped the tourism industry with various tools to optimise its services (Pencarelli, 2020). From online booking systems

to big data personalisation, innovative technologies enable travel companies to analyse consumer behaviour and preferences effectively, allowing businesses to tailor their products to meet specific needs (Li et al., 2018). Despite these advancements, digital transformation has also introduced challenges for the tourism industry. As more companies adopt digital strategies, individuals increasingly rely on digital tools, exposing personal information and data to platforms (Quach et al., 2022). Incidents of data breaches, misuse of customer information, and algorithmic bias have raised significant concerns about data privacy, cybersecurity, and the ethical use of technology. These issues have led to a decline in customer trust.

Consequently, as the digital transformation progresses, tourism businesses must embrace digital technologies and address the ethical challenges that accompany them (Flyverbom et al., 2019). The digital transformation has led to CDR's emergence, emphasising the need for ethical behaviour in the digital space. CDR is an ethical framework that guides organisations on using digital technologies responsibly and positively, contributing to all stakeholders, including customers, employees, and the wider community (Lobschat et al., 2021). The tourism industry, which often involves collecting large amounts of personal data—from booking information to travel preferences—faces the challenge of managing such data ethically and securely. As consumers increasingly demand transparency and ethical practices, modern travellers are becoming more aware of how their data is used. Consequently, travellers are more likely to choose travel companies with robust privacy protections, strong security

measures, and effective CDR practices (Kim et al., 2007). By proactively implementing CDR and demonstrating a commitment to digital responsibility, companies can build stronger customer relationships, enhance their brand reputation, and ultimately gain a competitive advantage in the market. This is particularly crucial for travel companies.

Therefore, this study aims to review CDR frameworks and elements through existing literature, identify key barriers to its implementation, and examine current CDR practices in the New Zealand tourism industry using official data. As CDR is a relatively new concept, one of the primary challenges in its implementation is the lack of awareness and understanding among tourism businesses. Many companies, particularly small and medium-sized enterprises (SMEs), may not be familiar with CDR or fully grasp its importance. However, businesses must balance the opportunities and risks of digital transformation through CDR implementation. Travel companies must recognise the importance of CDR in protecting customer privacy and security and ensure that their digital practices contribute positively to society.

1.2 Research Objectives and Questions

This study explores the impact of digital transformation and CDR on the New Zealand tourism industry and its future development. As tourism organisations increasingly rely on digital tools to attract customers and enhance marketing and operational efficiencies, the ethical implications of digitalisation become ever more

critical. Through an in-depth examination of digital transformation and CDR, this research underscores the importance of CDR implementation and identifies key elements and barriers to its adoption. Focusing on the context of the New Zealand tourism industry, this study investigates the challenges tourism companies face in adapting to the digital age. By collecting and analysing data on New Zealand tourism businesses, the research examines current CDR practices within the industry in the context of digital transformation. The findings provide a detailed analysis of existing practices and the obstacles to effective CDR implementation. This research aims to inform the New Zealand tourism sector of the necessity of integrating CDR into its digital strategy to promote sustainable tourism development. The significance of this study lies in its potential to offer valuable insights to tourism stakeholders. By addressing both the benefits and challenges of digital transformation, the research contributes to developing strategies that support ethical digital innovation within the tourism industry.

Research Questions:

1. How are privacy practices and data management strategies implemented by tourism agencies in New Zealand to align with CDR principles?
2. What are the key challenges faced by tourism organisations in New Zealand in achieving compliance with privacy legislation and integrating ethical digital practices into their operations?

The first research question examines how travel organisations present their handling of customer data and data security on their websites and policies. It also explores the data management strategies they use to address the challenges of digitalisation. This question aims to provide insight into how New Zealand travel organisations implement privacy protection and data management strategies to ensure compliance with CDR principles.

The second research question examines the main challenges faced by New Zealand tourism organisations in implementing CDR. The research will explore the difficulties these organisations face in complying with privacy legislation, for example, New Zealand's Privacy Act, and integrating ethical digital practices into their day-to-day operations. These challenges may include technological barriers, resource constraints, and a lack of understanding of CDR principles.

By identifying the current practices of New Zealand tourism organisations in implementing privacy practices and data management strategies and by analysing the main challenges faced by these organisations in implementing CDR, this study aims to provide specific recommendations for the New Zealand tourism industry. These recommendations will support CDR adoption and contribute to sustainable tourism development through continuous adaptation to CDR principles.

1.3 Significance of the study

The significance of this study lies in its provision of valuable insights for tourism industry stakeholders, including policymakers, tourism organisations, and technology developers, to support the development of an effective CDR framework for the New Zealand tourism industry. By exploring the opportunities and challenges of digital transformation and bridging the gap between technological innovation and corporate responsibility, this study offers practical recommendations for tourism organisations to integrate CDR into their daily operations. The findings suggest that implementing CDR can contribute to the sustainable development of New Zealand's tourism industry by enhancing consumer trust, securing data, and improving long-term competitiveness.

From a theoretical perspective, this study enriches the industry applicability of the existing CDR framework by analysing its practical implementation within the tourism sector. By examining the concept of CDR in existing studies, the research identifies shortcomings in the tourism industry regarding digital ethics, privacy, and governance, emphasising the need to incorporate CDR into long-term strategic planning rather than merely treating it as a compliance-driven obligation. Furthermore, this study proposes a CDR implementation framework specifically applicable to the tourism industry, providing new directions for future academic research.

For tourism stakeholders, this study offers practical recommendations for enhancing digital responsibility practices. By assessing travel agents' compliance with the New Zealand Privacy Act 2020, the research highlights the importance of appointing a privacy officer, developing a clear data policy, and promoting consumer

empowerment through digital literacy. The findings provide strategic guidance for tourism organisations to strengthen their CDR practices.

This study not only provides theoretical support and practical guidance for the digital transformation of the tourism industry but also offers multi-level insights for policymakers, industry practitioners, and consumers. By promoting responsible digital practices, this research aims to help New Zealand's tourism industry achieve sustainable development in the face of globalised competition while also serving as a reference for CDR implementation in other industries.

1.4 Structure of the dissertation

The remaining chapters of this dissertation are structured as follows: Chapter 2 provides a comprehensive literature review covering the context of New Zealand's tourism industry, the theoretical underpinnings of CDR, and the key challenges the tourism sector faces. This chapter offers an overview of previous research on digital transformation and privacy practices within the tourism industry. Chapter 3 outlines the research framework and methodology. This chapter introduces the research philosophy, followed by an explanation of the methodology used for data collection and analysis. It also includes the rationale for sample selection, the measurement approach, and the methods used to assess the integration of privacy practices and digital responsibility within New Zealand tourism organisations. Chapter 4 presents the study's findings,

including examples of current privacy practices, regulatory compliance, guidance frameworks, and data management strategies within New Zealand's tourism industry. The results are examined using descriptive statistics, comparative analyses, and thematic coding of qualitative insights. Chapter 5 discusses key findings concerning the research questions and existing literature. This chapter also highlights the theoretical contributions of the study and its practical implications for tourism businesses and policymakers. Finally, Chapter 6 concludes the dissertation by summarising the key insights, acknowledging the study's limitations, and suggesting directions for future research. This chapter emphasises the importance of proactive digital responsibility in the tourism industry.

Literature Review

2.1 Tourism industry in New Zealand

New Zealand's tourism industry is known for its natural beauty, outdoor adventure opportunities and film locations. New Zealand has a pristine and diverse landscape. New Zealand is known as 'Clean and Pure' (Bell, 2008). The unique landscape and scenery created by volcanic eruptions provide an unrivalled experience of New Zealand's scenery (Campbell et al., 2012). The rugged terrain and diverse environment of New Zealand make it a popular location for adventure travelling.

Additionally, Queenstown, known as the 'adventure capital' of the world, offers a wide range of extreme activities (Cater, 2006). Queenstown is the birthplace of bungee jumping. On 12 November 1988, the first commercial bungee jump was launched at the Kawarau Bridge, and bungee jumping has since become a popular activity. This innovation has also inspired more world-first anti-gravity adventures, such as canyon swings and zip-lining, complementing the natural landscape (Cloke & Perkins, 2002).

The beauty of New Zealand's outdoor landscapes has also attracted many filmmakers. The country is internationally renowned as the setting for *The Lord of the Rings* and *The Hobbit* film trilogies (New Zealand Tourism, 2024). As a result, many film fans worldwide have chosen to visit New Zealand. Locations such as Hobbiton in Matamata, filming sites near Queenstown, and Tongariro National Park attract film enthusiasts who want to immerse themselves in the fantastical scenery of the films.

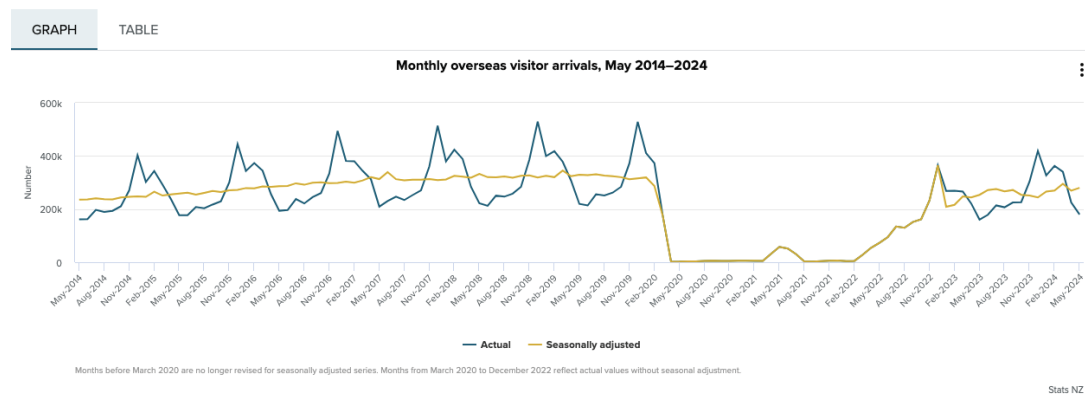
However, New Zealand's tourism industry attracts many tourists (Stanford, 2008). Some seek relaxation in natural beauty, others desire a romantic getaway, and some enjoy scenic travel. Adventurous travellers are drawn to extreme activities and the great outdoors, while movie fans visit to experience the iconic film locations.

According to the Markets Overview released by the New Zealand Tourism Board (Tourism New Zealand, 2024), the top five source countries of tourists are Australia, which is New Zealand's most prominent tourist market, accounting for nearly half (44%) of all international tourists; followed by the United States of America. The United States is New Zealand's second-largest tourist market in terms of the number of inbound visitors. China is New Zealand's third-largest inbound tourist market. In 2019, China was New Zealand's second-largest international tourist market and one of the countries with the highest spending by holiday tourists. Next is the UK, with 169,300 British tourists visiting New Zealand between April 2023 and April 2024, of which 68,300 were holidaymakers. Fifth is Germany, where tourists tend to stay longer and spend more per trip than tourists from other countries (Tourism New Zealand, 2024).

Tourism is recognised as an important part of New Zealand's economy and culture (McIntosh, 2004). Tourism's generally recognised economic benefits include its labour intensity and the regional distribution of expenditure (Simmons, 2013). International tourism is one of the key drivers of New Zealand's growth and economic development. In March 2019, international tourism expenditure accounted for 20.4% of New Zealand's total exports of goods and services, and tourism contributed approximately

5.8% of the country's GDP (Stats NZ, 2019). New Zealand's international tourism markets have boosted economic growth (Jaforullah, 2015). Before the outbreak of COVID-19, the year ended March 2020, tourism generated 5.5 per cent of New Zealand-Aotearoa's GDP and 20.1 per cent of exports (MBIE, n.d.). The sector also employed 225,000 people, which significantly positively impacts the regional economy and promotes employment. However, the impact of COVID-19 on the tourism sector has been severe. International visitor arrivals to New Zealand decreased by 98.6%, and the number of people directly employed in tourism decreased by a third (MBIE, n.d.). For the year ended March 2023, tourism was New Zealand's second-largest export earner (Tourism New Zealand, n.d.). As a result, for the year ended March 2023, the tourism-supported industry's indirect value added generated \$8.8 billion in additional income, or 2.5 per cent of GDP. And direct employment in the tourism industry was 189,432, or 6.7 per cent of total employment in New Zealand. In total, 317,514 people were directly or indirectly employed in the tourism industry, representing one-ninth of New Zealand's total population (Tourism New Zealand, n.d.).

Figure 1
Monthly overseas visitor arrivals, May 2014-2024



Note. This figure shows the trend in total visitor arrivals to New Zealand from May 2014 to 2024. Statistics New Zealand. All material Stats NZ produces is protected by Crown copyright.

Figure 1 shows the number of overseas visitors to New Zealand each month from May 2014 to 2024. It includes two lines: the blue line represents actual arrivals, and the yellow line shows the seasonally adjusted figures. The figure shows the trend from 2014 to 2019. The figure shows a clear seasonal pattern in New Zealand's travel industry, with peaks in December-January. The trough is reached during New Zealand's winter months from June to August. The seasonally adjusted line shows a gradual upward trend, suggesting steady growth in international tourism between 2014 and 2019. In the middle and latter parts of the figure, the blue line represents actual arrivals, and the yellow line shows the sharp seasonally adjusted decline. Overseas tourist arrivals fell sharply after February 2020, coinciding with the start of the COVID-19 pandemic and global travel restrictions. From May 2020 to December 2023, actual

arrivals fell to zero. Subsequently, actual arrivals were not recorded until 2023. Seasonal fluctuations reappear between 2023 and 2024, suggesting a partial return to standard travel patterns.

According to the International Visitor Arrivals Report New Zealand, released by Stats New Zealand, over the past ten years, New Zealand's tourism industry has experienced significant instabilities, primarily due to the impact of COVID-19 and the subsequent recovery phase. Pre-COVID Era (2014-2019), New Zealand's international tourist arrivals have steadily increased. Data shows a clear seasonal pattern in New Zealand's international visitor numbers, with peaks typically occurring in the summer months of December and January. By the end of 2019, visitor numbers were at their highest level. However, with the outbreak in early 2020, arrivals dropped precipitously to approach zero as global travel restrictions and border closures emerged (Gössling et al., 2020). This virus outbreak led to an unprecedented decline in international tourist arrivals. This sharp decline continued through 2020 and 2021, severely impacting New Zealand's tourism industry. In mid-2022, New Zealand's international borders became effective for all vaccinated international travellers, subject to a negative new crown test before arrival (Gauld, 2022). New Zealand's international visitor numbers recovered slowly but steadily as travel restrictions began to ease and borders gradually reopened. By mid-2023, data showed a marked rise in arrivals, although the recovery has been uneven. As of May 2024, visitor numbers are improving but have not yet returned to pre-2019 pandemic levels. Until now, New Zealand's tourism industry has been in a

recovery phase. While visitor numbers are slowly continuing to increase, the industry has not yet fully returned to its pre-pandemic performance. Therefore, appropriate digital innovation and progress are crucial for New Zealand's tourism industry (Munasinghe et al., 2022). Adequate understanding of tourist preferences and marketing are important strategies for recovering the tourism industry and continued development.

2.2 Digital transformation in tourism industry

The digital revolution is radically changing our world, and the tourism industry is actively participating in the digital transformation (Pencarelli, 2020). Kong et al. (2022) proposed that the evolution of artificial intelligence in the history of tourism development can be divided into three stages: the Initial stage (1991–2014), the Exploratory stage (2015–2018), and the Development stage (2019–2021). In the initial stage, with the advent of the Internet in the 1990s, physical travel suppliers such as hotels, airlines, and destinations developed their travel websites for marketing and distribution purposes (Leung, 2019). In the Exploratory stage, technological advancements, big data, social media, online communities, and the sharing economy became the driving forces for the development of the tourism industry (Bowen & Whalen, 2017). The efficacy of digital data in creating compelling customer targeting and service delivery in the tourism industry has been widely recognised (Stylos et al.,

2021). By understanding tourists' travel preferences and behaviours through digital data, travel agencies can develop timely and optimal strategies and travel packages (Li et al., 2020). This ability to customise services and products enables agencies to maintain a competitive advantage during challenging times (Perić & Vitezić, 2021). Meanwhile, Artificial intelligence systems and products were more widely adopted, including autonomous driving, intelligent information services, and robotics technology in travel companies and hotels (Ivanov & Webster, 2017; Kumar et al., 2021). In the Development stage (2019–2021), according to a literature review by Madzík et al. (2023), the tourism industry was severely affected by the COVID-19 outbreak, destabilising the market environment. As a result, a significant number of companies and organisations around the world have realised the importance of digital transformation (Madzík et al., 2023). Digital technologies were instrumental in implementing and monitoring health and safety protocols, enhancing public health responses to the pandemic (Chamola et al., 2020). For instance, AI-driven contactless services in hotels, airports, and tourist attractions minimised physical interactions, ensuring safer travel experiences (Afaq & Gaur, 2021). In the post-pandemic era, digital technology's needs, advantages, and disadvantages have attracted significant attention (Kong et al., 2022).

The industry in New Zealand has undergone a significant shift with the rapid development of digital technology. New Zealand businesses are increasingly adopting Information and Communications Technology (ICT) as part of their initiative. Since

2017, the total sales of published software and IT services increased by \$7.1 billion, or 96% (Stats NZ, 2024). In 2019, computer service firms contributed one-third of total corporate R&D expenditures (Stats NZ, 2020). With the development of ICT, it plays an increasingly important role in enhancing the competitiveness of tourism organisations and destinations (Navío-Marco et al., 2018). ICT became a key factor in the competitiveness of tourism organisations and destinations (Buhalis & O'Connor, 2005). Examples include digital marketing, search engine, and content optimisation; these strategies help to reach a wider audience and attract more potential customers, as well as use customer data to create personalised marketing messages and offers. As online marketing becomes an interactive staple, companies increasingly try to engage consumers in an online dialogue (Navío-Marco et al., 2018). As a result, traditional travel agents face the challenge of disintermediation, whereby suppliers such as airlines, hotels, and car rental companies sell their services directly to consumers via the Internet rather than relying on intermediary channels (Garkavenko, 2007). This shift has fundamentally changed the way tourism services are distributed and consumed.

From the consumer's perspective, the ICT economy means new opportunities (Gössling, 2020). For consumers, ICT provides convenience and accessibility. Consumers can easily search and book travel services online, including flights, accommodation, and tours (No & Kim, 2015). Consumers can also compare prices and reviews and make informed decisions based on real-time information (Gössling, 2020). The benefit for businesses is that ICT can be effective in increasing revenue. ICT tools

such as online booking systems, dynamic pricing, and digital marketing can help businesses attract more customers, increase bookings, and maximise revenue (Dyshkantiuk et al., 2020). As an online booking engine for SMEs, it is a tool to improve distribution and revenue management in the New Zealand tourism industry (Smith & Schott, 2004). The rise of online booking systems further exemplifies the impact of digital transformation on the tourism industry. Digital technologies have significantly impacted the New Zealand tourism industry in recent years. As of August 2024, 692 travel agents are cooperating with Tourism New Zealand (Tourism New Zealand, n.d.). Visitors can jump to the right travel agent page according to their needs. These include 570 general travel operators, 240 self-drive holiday specialists, 231 adventure travel, 203 group travel specialists, and ski specialists (28), golf specialists (49), fishing specialists (6), cruise holiday specialists (56), coach holiday specialists (100), and accommodation specialists (52). All the listed travel agents are from different regions and countries, but they all have official websites with product descriptions, online booking, and contact details. Some travel agencies provide real-time prices to visitors, while some customised travel agencies set prices based on customer needs, providing practical and convenient information. Currently, there are seven major systems on the market in New Zealand, most of which cover the entire process from information display to booking, confirmation, and payment (Smith & Schott, 2004). Reports show that New Zealand businesses that use the Internet more extensively are 6 per cent more productive than the industry average (MBIE, 2017).

Moreover, the tourism sector is increasingly characterised by the adoption of innovative technologies. Smart tourism refers to the application of advanced technologies—such as artificial intelligence (AI), the Internet of Things (IoT), big data, and robotics—to improve the efficiency, sustainability, and personalisation of tourism services and experiences (Pencarelli, 2020). It enhances service quality, supports data-driven decision-making, and enables more interactive and user-centric travel experiences.

For example, Christchurch Airport demonstrated a smart tourism initiative by introducing Pepper, a humanoid robot, in 2019 to help passengers navigate security screening procedures. This innovation not only improved passenger flow but also reduced health-related risks. Following its success, the airport expanded its fleet to four robots in subsequent years (Christchurch International Airport, n.d.). After the COVID-19 outbreak, the tourism and hospitality industry increasingly adopted contactless intelligent services to turn public health challenges into operational innovations (Li et al., 2021). In New Zealand, SkyCity Hotels in Auckland implemented robotic food delivery and code-swipe ordering at Andy's Burgers & Bar (SkyCity Auckland, n.d.). Similarly, Sudima Hotels have integrated service robots to enhance room service operations (NZ Herald, 2024). These developments illustrate how smart tourism technologies are not only improving operational efficiency but also elevating the overall visitor experience, making tourism more responsive to modern travellers' needs.

2.3 Corporate Digital Responsibility

The use and development of digital technology raise ethical concerns about data leaks, privacy, and unemployment (Dhirani et al., 2023; Zeng et al., 2020). Similarly, network disruptions can paralyse tourism value systems that rely on constant connectivity, and cybercrime seriously threatens tourism systems (Herden et al., 2021). While ICT technologies bring many advantages to business, they also raise consumer concerns about privacy breaches, extensive personal analyses, algorithmic bias and discrimination (Someh et al., 2019). As the complexities of the digital age, businesses must recognise the need to incorporate ethical considerations into their practices (Herden et al., 2021). Hence, the concept of CDR has been proposed, constituting applied ethics to guide actions, support judgments, and inform choices (Lobschat et al., 2021).

CDR is an applied ethical framework designed to guide businesses in making moral decisions related to digital transformation. It emphasises the need for organisations to consider the impact of their digital practices on various stakeholders, including consumers, employees, and society (Lobschat et al., 2021). The driving force behind CDR is an increased sense of responsibility for the impact of the digital transformation process and the opportunities and risks it presents for different interest groups (Pelters, 2021). As organisations become increasingly reliant on digital technologies, they must

ensure that their actions are guided by ethical principles that prioritise the well-being of all stakeholders. While CDR is increasingly recognised as an important component of corporate responsibility, it is still an emerging concept and varies between regions and industries.

CDR is crucial for maximising the benefits of digital transformation while effectively managing its associated risks. CDR is important in the tourism industry, where digital technologies play a role in delivering services and enhancing the customer experience. Tourism companies are responsible for ensuring ethical practices in managing users throughout the digital value chain, from data collection and storage to service delivery (Wirtz et al., 2023). By reducing adverse privacy breaches and consumer protection incidents, travel companies can build strong CDR frameworks and earn their customers and business partners' trust and loyalty (Herden et al., 2021). In this way, CDR becomes an extension of traditional corporate responsibility, reflecting the ethical imperatives of the digital age. By adopting a strong CDR framework to protect their stakeholders, travel companies can enhance their reputation and competitiveness in an increasingly digital world.

CDR is increasingly recognised as essential to modern business practices, especially as digital technologies become deeply ingrained in organisational operations (Wynn & Jones, 2023). With growing concerns about digital technologies, some countries have introduced legislation to control privacy and security. These laws apply to specific technologies, business operations, physical architectures,

cyberinfrastructure, and the entire information ecosystem. The development of CDR also reflects differences in domestic and international legislation and strategic autonomy, as well as current practices on how user data companies access and store data in different jurisdictions (Wynn & Jones, 2023). For instance, the General Data Protection Regulation (GDPR), effective 25th May 2018, is a data protection legislation that provides rules for processing, storing, and managing data for individuals in the European Union. It strengthens data protection in the European Union to address new privacy challenges posed by advances in digital technology (Li et al., 2019). In New Zealand, consumers are protected through the Consumer Guarantees Act, the Privacy Act, and the Harmful Digital Communications Act (HDCA) when purchasing goods from or sharing information with businesses in New Zealand (New Zealand Government, 2020). New Zealand's Privacy Act applies to any person, organisation, or business, whether in the public or private sector, that collects and holds personal information about others. Thirteen information privacy principles in the Privacy Act govern how businesses and organisations collect, process, and use personal information (Privacy Commissioner, n.d.).

The New Zealand Government has promoted a Privacy by Design (PbD) approach to protect private data in the operational and information ecosystem. PbD is a design methodology that includes privacy as an essential priority in any product, service, system, or process, to minimize the data protection concerns (Romanou, 2018). The principles of PbD ensure that the information privacy principles of privacy

laws are met. Furthermore, the PbD raises organisational awareness about privacy and personal information processing in projects, products, services, systems, or processes. Identifying and addressing potential privacy risks and problems as early as possible. Moreover, the success of the PbD principle relies not only on technical solutions but also on integrating privacy protection into the organisation's overall strategy. Therefore, companies are required to embed privacy protection into their core strategy, rather than making it the responsibility of a single department, and to engage in continuous communication and education with senior leaders, colleagues, and employees (Angermann, 2023; Herden et al., 2021; Lobschat et al., 2021).

To guide this approach, the New Zealand Government has outlined seven foundational principles of Privacy by Design:

1. Proactive not reactive, preventative not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality — positive-sum, not zero-sum
5. End-to-end security — lifecycle protection
6. Visibility and transparency
7. Respect for user privacy — keep it user-centric

(New Zealand Digital government, 2024)

Although governments and authorities in various countries have enacted laws to ensure online data security, the literature indicates that current CDR practices reflect a lack of comprehensive legislation, low awareness, inconsistent implementation, and reliance on autonomy (Angermann, 2023; Elliott et al., 2021). Many large organisations seek to transform all business areas by leveraging digital technologies. However, most are slow to publicly acknowledge and address the new responsibilities of introducing these technologies (Wynn & Jones, 2023). Therefore, different industries face different challenges when adopting CDR frameworks.

2.4 Key Elements for the Implementation of CDR

While the concept of Corporate Digital Responsibility (CDR) is gaining recognition, its practical implementation remains challenging for many organisations due to regulatory complexities, limited resources, and rigid organisational structures. Accenture, one of the world's largest IT consulting firms, first introduced the concept of CDR in 2015, identifying five key areas of application: digital stewardship, digital transparency, digital empowerment, digital equity, and digital inclusion (Brink et al., 2020; Cooper et al., 2015; Elliott et al., 2021). These principles emphasise responsible data use, fairness in digital participation, and the inclusive accessibility of digital technologies and information (Angermann, 2023a; Elliott et al., 2021).

Digital stewardship refers to managing customer data by developing and implementing effective policies, processes, and technologies (Angermann, 2023). Therefore, it ensures data's secure, compliant, and ethical use. In a data-driven economy, digital stewardship is fundamental to building customer trust and complying with laws and regulations. It requires organisations to focus not only on data security but also on ensuring that data is collected, stored, and used in an ethical and socially responsible manner (Herden et al., 2021). Similarly, digital transparency relates to how organisations communicate openly with customers regarding how their data is collected, used, and shared. Transparency is key to building customer trust, reducing concerns, and increasing confidence in data processing (Wynn & Jones, 2023). Without clear and open communication, customers may feel uncertain about data usage, which could negatively impact their trust in digital services (Chang et al., 2018). In addition to transparency, digital empowerment plays a crucial role in enabling customers to control their data by providing them with the necessary tools, resources, and information to protect their privacy where necessary (Angermann, 2023). By empowering customers, organisations demonstrate a commitment to ethical data use, which can further enhance trust and foster positive relationships with consumers. Digital equity ensures that companies distribute the profits from data usage fairly and commit to not misusing customer information (Angermann, 2023; Wirtz et al., 2023). Fair data use practices not only contribute to customer trust but also prevent social injustices that may arise from data exploitation. Additionally, digital inclusion emphasises the importance of

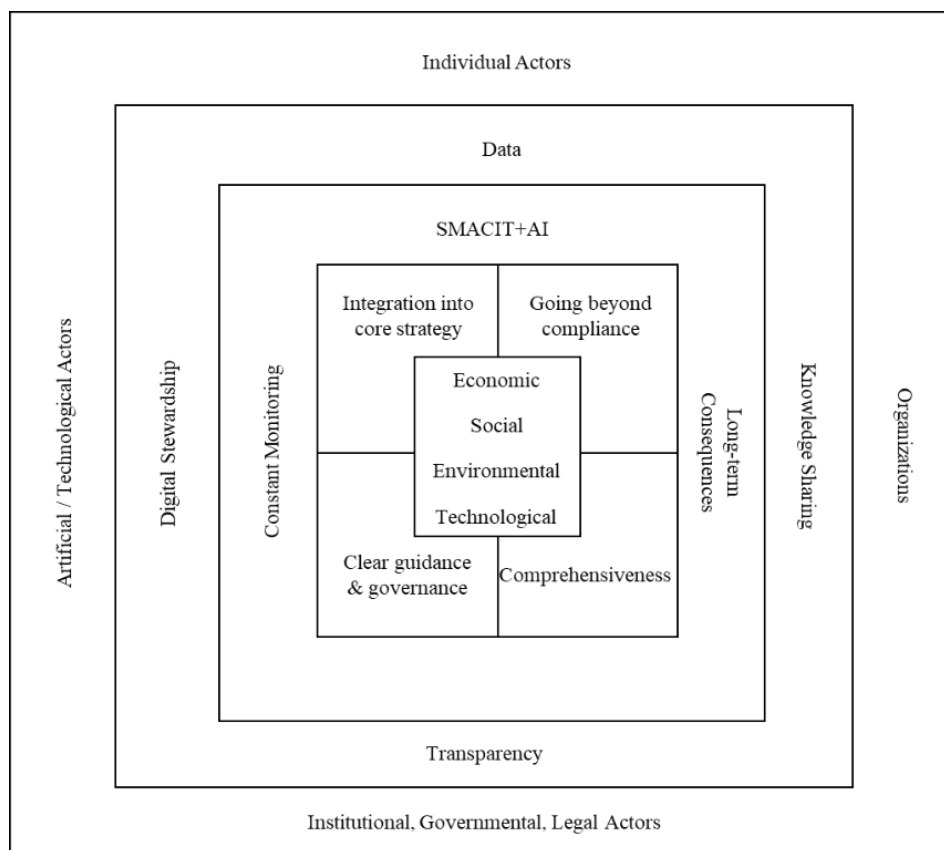
making digital technologies accessible and affordable to everyone, reducing barriers to digital participation and ensuring that all individuals, regardless of socioeconomic background, have equal opportunities to engage with digital services (Basu et al., 2024).

To effectively implement Corporate Digital Responsibility, Angermann (2023) outlines key elements for CDR adoption. These include embedding CDR at the organisation's core and integrating digital responsibility into corporate values, culture, and long-term vision. Organisations must go beyond regulatory compliance and view CDR as a legal obligation and a strategic commitment to ethical digital engagement. Additionally, establishing a clear direction and governance framework is essential, with leadership and accountability structures in place to support the CDR programme. Furthermore, effective implementation of CDR should involve all stakeholders, ensuring the education and empowerment of employees to understand and adhere to digital responsibility principles. This holistic approach enables organisations to embed ethical digital practices at all levels, fostering a culture of responsibility and transparency.

Despite the growing awareness of CDR, organisations continue to face several challenges in implementing its principles effectively. One of the primary challenges is regulatory complexity and compliance. Lobschat et al, (2021) and Martin & Murphy, (2017) states that inconsistent global regulations create additional difficulties, particularly for agencies and multinational corporations operating across multiple jurisdictions. Another significant challenge is resource constraints (Merwe & Achkar,

2022), especially for SMEs that may lack the financial and technical capacity to adopt data protection technologies. For SMEs, adopting or even understanding CDR can be a substantial challenge. Additionally, organisational awareness and culture play a critical role in CDR adoption. Many organisations still view digital responsibility as a legal obligation rather than an ethical commitment (Basu et al., 2024; K. V. Carl et al., 2022). This perspective can hinder proactive engagement with CDR principles and result in a compliance-driven rather than value-driven approach. These challenges emphasise the need for clear regulatory guidance and ongoing education to strengthen CDR adoption across industries.

Figure 2
CDR implementation



Note. The figure shows that several key elements have been identified to address the challenges of CDR. From “The Challenge of Corporate Digital Responsibility – An Analysis of Key Elements for CDR Implementation”, by P. Angermann, 2023, p.38. Copyright by Universidade Católica Portuguesa.

The figure highlights several key elements for implementing CDR, among which four are critical to its successful adoption. These elements include integrating CDR into the core strategy, going beyond regulatory compliance, establishing clear guidance and governance, and ensuring the comprehensiveness of CDR across all stakeholders.

However, continuously enhancing the CDR framework remains essential, given the rapid pace of technological change. Ongoing monitoring, adaptation, and a sustained commitment to digital stewardship and knowledge sharing are crucial to maintaining effective CDR practices. By understanding and applying these key elements, organisations can better manage risks, seize opportunities associated with digital transformation, and create value for both their organisation and society.

2.4.1 Privacy

Privacy has become a significant point of public concern in this digital age. The rapid development of information technology has led to profound changes in both the definition and scope of privacy (Kovanič & Spáč, 2022). Initially, privacy was understood as an individual's right to be free from intrusion. However, it has since evolved to encompass the security and autonomous control of personal information in the digital realm (Introna, 1997). Privacy fundamentally refers to an individual's right to control their personal information, which includes autonomy over the collection, disclosure, and use of personal data (Solove, 2002). The rise of the internet has transformed modern business, creating a new paradigm for business relationships and transactions (Wu et al., 2012). Digital platforms such as websites, apps, and social media frequently collect and store large amounts of users' data to better understand their needs and provide services more closely tailored to their preferences (Anshari et al.,

2019). From the consumers' perspective, personalised services benefit both parties somewhat. For example, e-commerce platforms analyse users' purchase histories and recommend products that match their preferences, saving users time and increasing merchants' sales efficiency (Akter & Wamba, 2016; Anshari et al., 2019). However, personalised services also pose privacy risks. If personal data is improperly disclosed, it seriously threatens an individual's privacy (Kaaniche et al., 2020).

Consumer concerns centre on the expansion of databases, the volume of personal data being collected, the potential for privacy invasions, and the loss of control over how personal information is accessed and used (Culnan, 1993). The tourism industry is a complex system covering a range of operations such as web search data, web access data, online booking data and other transactional data to understand tourist behaviour and improve tourism marketing (Li et al., 2018). However, the over-collection of such data has also sparked widespread social controversy. Research has shown that the potential for invasion of personal privacy triggers fear and mistrust in businesses (Wang et al., 1998). This distrust not only affects consumers' purchasing decisions but may also have far-reaching effects on the long-term reputation of the firm.

Privacy policies serve as a mechanism for individuals to trust that the company will act appropriately. Many online companies place privacy policies on their websites to reduce customer concerns about compromised personal information (Chang et al., 2018). In addition, customers value transparency in how data is handled. Chang et al. (2018) state that users find privacy policies more effective when organisations inform

them of their data practices and allow them to manage their personal information. Providing control over personal data reduces customer concerns about potential risks. The online shopping environment requires higher levels of consumer trust than physical stores (Grabner-Kräuter & Kaluscha, 2003; van der Heijden et al., 2003). In this context, a robust privacy policy is critical for building trust, protecting both the company and its customers, and ensuring responsible data management (Chang et al., 2018; Martin & Murphy, 2017). Research indicates that 65% of respondents are more willing to provide personal information online when they trust it will not be misused and will contribute to a higher-quality service (Wu et al., 2012).

In this respect, providing appropriate privacy policies and terms and conditions on websites is essential. One of the primary reasons for developing a privacy policy is to comply with legal requirements. Various countries and regions have introduced a series of laws and regulations on personal information protection, requiring companies to act by the law (Culnan & Bies, 2003). Additionally, for organisations, trust is the cornerstone of any successful business relationship (Elliott et al., 2021). However, many privacy statements are lengthy and challenging to read despite their importance, leading consumers to overlook them (Martin & Murphy, 2017). Poor comprehensibility may cause consumers to lose interest in privacy policies, preventing these policies from fulfilling their intended purpose (Van der Heijden et al., 2003). A clear and transparent privacy policy helps build and maintain customer trust (Wu et al., 2012).

The issue of privacy protection is particularly critical in the tourism industry. The industry highly depends on customers' personal information (Xiang et al., 2015). Smart tourism, while integrating various new technologies, poses additional security threats and challenges due to its cross-cutting, pervasive and comprehensive nature (Liu & Liu, 2016). Travel agencies, airlines, and online booking platforms typically collect large amounts of sensitive personal data, including passport information, payment information, and travel preferences (Yallop et al., 2021). While this data enables travel companies to offer personalised services such as tailored travel packages and a more convenient booking experience, there are significant risks (Xiang et al., 2015). Research has shown that web functionality, web content and information security are the three key factors influencing consumers' choice of online travel services (Liao & Shi, 2017). However, once these data are improperly managed, they can lead to serious security issues. Customers will face information security threats, including user data leakage, payment system vulnerability and business system failure (Larasetiati & Ali, 2019). Privacy violations not only lead to loss of customer trust and loyalty but may also cause irreparable damage to the organisation's reputation. Therefore, tourism organisations that clearly emphasise their ethical responsibilities and effectively address privacy concerns on their official websites significantly enhance consumers' authenticity, trust and loyalty to their brands and digital products (Kim & Kim, 2024).

2.4.2 Legislation

In the history of human rights development, the significance of privacy was established in the 1948 Universal Declaration of Human Rights and was recognised as a fundamental human right (Ziegeldorf et al., 2014). This concept has since been deeply integrated into the constitutional systems of most countries. In this digital transformation era, cybersecurity and privacy awareness have reshaped the business landscape, leading to significant changes in all aspects of organisations and becoming a key point of international attention (Saeed et al., 2023). Different countries and regions have developed privacy laws with distinct characteristics shaped by their political, economic, and cultural contexts, demonstrating their importance on cybersecurity (Bechara & Schuch, 2020; Bygrave, 2010).

The United States was among the first countries to prioritise privacy protection, enacting the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and the Children's Online Privacy Protection Act of 1998 (Fiero & Beier, 2022). These regulations reflect the United States' approach to privacy and security in the online environment, addressing concerns across multiple dimensions and demographics. The European Union's General Data Protection Regulation (GDPR) has had far-reaching global implications, granting consumers extensive control over their data. The GDPR ensures access, correction, and deletion rights, thereby strengthening individuals' control over their own data (Li et al., 2019). In New Zealand, the Privacy Act of 1993

defines national values and privacy rights for citizens and online consumers (Hooper & Vos, 2009). Furthermore, due to variations in culture, legislation, government structures, and business practices, different countries hold diverse perspectives on and approaches to information privacy (Chua et al., 2017). Given these legislative differences, establishing a CDR framework will also vary across legal and cultural contexts (Lobschat et al., 2021).

At the enterprise level, implementing CDR is inherently complex. The fundamental application of CDR consists of voluntarily developed policies and principles of self-governance, created, implemented, and monitored by companies themselves, extending beyond statutory requirements (Merwe & Achkar, 2022). This results in greater autonomy but also introduces uncertainty regarding how organisations disclose privacy-related information in practice. Therefore, CDR should go beyond legal compliance and incorporate self-regulation (Angermann, 2023). Government regulation is designed to address well-defined issues; however, laws can also have unintended consequences, such as increasing operational costs, particularly for small and medium-sized tourism enterprises (Culnan & Bies, 2003). Compliance with stringent local data protection regulations often demands significant financial resources, creating considerable operational challenges (Hwang & Lockwood, 2006). Although establishing a privacy department may be costly for organisations, it enhances consumer trust and fosters long-term sustainability.

Furthermore, with the rapid advancement of AI, many countries have yet to explore the safety and privacy implications of AI applications sufficiently. Research by Londoño-Cardozo and Paz (2021) indicates that concerns regarding AI regulation remain low globally, with only 4% of countries or regions actively discussing the issue (Londoño-Cardozo & Paz, 2021). Therefore, demonstrating a lack of emphasis on ethics and privacy leads to further challenges in understanding and implementing CDR. In the tourism industry, AI is widely employed in intelligent recommendations and itinerary planning (Shi et al., 2021). For instance, online travel agencies use AI algorithms to suggest destinations and hotels based on tourists' historical browsing and booking records (Borràs et al., 2014). However, insufficient regulation of data privacy in AI applications may lead to the inappropriate collection and misuse of tourists' personal preferences, consumption habits, and other private information (Yallop et al., 2021). In the data-driven economy, information serves as a critical asset. Therefore, organisations must prioritise security and privacy concerns, establish a robust CDR framework, and go beyond mere regulatory compliance to ensure ethical digital responsibility.

2.4.3 Guidance

Guidance is key in implementing digital responsibility (Angermann, 2023; Lobschat et al., 2021). Guidance refers to principles and norms guiding an

organisation's digital activities, such as data collection, storage, use, and sharing. It covers everything from internal data management processes to external data interactions with customers and all stakeholders (Le et al., 2024). Legal regulations vary significantly from country to country and region to region, making it difficult for companies to refer to existing CDR practices based on current regulations (Merwe & Achkar, 2022). In this context, companies must reach a consensus on their digital responsibilities and form practical guidance to regulate their digital behaviour. Organisational consensus on corporate digital responsibility is essential to providing clear guidance for its implementation (Carl et al., 2022).

In addition, companies of different sizes show significant differences in determining responsibility for the CDR programme. Angermann (2023) found that smaller companies often believe the management team should monitor CDR, whereas larger organisations tend to delegate this responsibility to their Corporate Social Responsibility (CSR) department. Unfortunately, many companies do not have a dedicated CDR department and often place responsibility on compliance or other departments, resulting in inconsistent implementation and oversight. To implement CDR effectively, consideration of the broader ecosystem within a company is necessary. The implementation involves multiple roles that interact with each other during the development and use of digital technologies (Herden et al., 2021; Lobschat et al., 2021). These roles may include project managers, business owners, privacy officers or teams, legal teams, requirements engineers, designers, programmers,

testers, and users. Therefore, for organisations, CDR should satisfy compliance and actively engage in self-regulation (Angermann, 2023). Organisations can better protect customer privacy and enhance their market competitiveness by establishing strict internal data management processes and monitoring mechanisms.

Ensuring each role understands, shares knowledge, and engages with digital stewardship and CDR will create a more integrated and practical approach to digital responsibility. There is currently no research linking CDR closely to management responsibilities within tourism organisations for the tourism industry. However, as the digital transformation of travel organisations accelerates, travel companies must adopt an agile approach to CDR. The tourism industry is unique in that customers provide a large amount of personal information on platforms, which, if compromised, can cause considerable losses to tourists and seriously damage the reputation of tourism organisations. Mazilescu (2019) points out that digital transformation is an inevitable trend, which, in turn, requires the tourism industry to be deeply involved in data management and security issues. Given the rapid pace of technological development, every company should adopt an agile approach to CDR and a strategy for regularly reviewing and updating their policies to ensure that they maintain optimal levels of digital responsibility (Herden et al., 2021).

2.5 Summary

As digital transformation continues and awareness of digital security grows, it has become critical for the New Zealand tourism industry to adopt a CDR approach. As Xiang et al. (2015) highlighted, the tourism industry relies heavily on personal customer data to provide services such as customised travel packages and bookings. This reliance underscores the importance of privacy protection and the need for a strong commitment to digital responsibility.

The CDR framework provides clear guidelines for organisations to manage their digital practices, ensuring compliance with privacy regulations while promoting ethical digital practices. According to Angermann (2023), reaching a consensus within an organisation on its digital responsibilities is essential for developing effective guidance. For CDR to be successful, it must be integrated into the organisation's core strategy, go beyond mere regulatory compliance, and establish a clear governance structure. In addition, it must ensure full accountability of all stakeholders, which helps organisations guide the management of their digital practices, including data collection, storage, use, and sharing (Angermann, 2023; Lobschat et al., 2021). By adopting the CDR framework, the New Zealand tourism industry can enhance privacy protections, build trust with customers, and ensure the ethical use of data, which will support sustainable business practices in the digital age.

Research Methodology

3.1 Research Paradigm

The ontological perspective chosen in this study is relativistic, which shapes how the problem is viewed and addressed. Relativism is subjective and posits that reality is not fixed or singular but is constructed and understood differently through various observations. Our understanding of the world is inherently limited to our interpretation of our experiences (Morgan, 2014). The relativism adopted in this study emphasises subjective experience, which is influenced by social, cultural, and personal factors, as qualitative research can delve into specific contexts and capture rich and nuanced insights into complex phenomena (Lim, 2024), relativism helps the study to understand the development of the local tourism industry in New Zealand more comprehensively, both at the cultural and social levels.

In this study, it is acknowledged that different tourism agencies have varying insights and practices regarding CDR. Therefore, there is no absolute right or wrong, only different positions or conditions influenced by their past contexts and cultures. The experiences of tourism organisations in implementing CDR are shaped by New Zealand's political constraints, values, and socio-economic environment. The diversity of their approaches to digital responsibility reflects their unique perspectives and responses to the challenges and opportunities presented by the digital transformation of the tourism industry. By recognising multiple realities, this study aims to understand in

greater detail the impact and role played by CDR in the tourism industry. The relativist ontological approach allows for considering different perspectives and practices of CDR within the New Zealand tourism industry. By acknowledging that different organisations construct their realities based on their unique experiences, this study can effectively provide insights into how New Zealand tourism organisations practice corporate digital responsibility.

In terms of epistemology, this study adopts a subjectivist approach. Subjectivism recognises that each individual's personal views and experiences play a key role in shaping their understanding of the world (Ratner, 2002). This approach acknowledges that different travel agencies' experiences, cultural backgrounds, and environments influence their interpretations and practices of corporate digital responsibility. It emphasises the importance of recognising the diversity of human experience and understanding that knowledge is not objective but shaped by subjective interpretation. This perspective is key to understanding how different travel agencies implement CDR practices.

Thus, the philosophical paradigm used in this study is interpretivism. Interpretivism holds that truth and knowledge are subjective, culturally and historically contextualised, and based on people's experiences and understanding (Ryan, 2018). Interpretative epistemology advocates understanding the world by studying people's experiences and viewpoints. Researchers should explore real-life contexts to explain and reconstruct these concepts and meanings.

The main aim of this study is to explore the gaps in corporate digital responsibility within the New Zealand tourism industry. Through an extensive literature review, this study analyses the challenges and key elements of CDR implementation, providing a theoretical foundation for further research on corporate digital responsibility in the tourism industry. The literature review offers an in-depth understanding of CDR's existing frameworks, challenges, and opportunities, forming a basis for exploring its application in the New Zealand tourism sector. Adopting interpretivism as the philosophical paradigm allows this research to delve into real-life understandings of CDR practices and explain and reconstruct the underlying concepts and meanings. Interpretivism emphasises documenting phenomena and understanding and explaining the cultural, social, and contextual factors behind the data (Lacity & Janson, 1994). The study interprets the secondary data through qualitative analysis and compares it with existing literature to explore possible consistencies, differences, or gaps. The interpretive approach highlights the importance of giving new meaning to observed behaviours and practices, enabling researchers to interpret and understand them in context. This deeper analysis helps explain the causes and meanings behind these behaviours, ultimately building a comprehensive understanding of the research questions. Thus, interpretivism helps to illuminate the unique challenges and future directions of implementing digital responsibility in the New Zealand tourism industry. By adopting this approach, the study aims to provide a nuanced and contextually rich

understanding of how CDR is practised and perceived within the sector, contributing to academic and practical advancements in the field.

3.2 Research Method

A qualitative research methodology was employed in this study. Qualitative research is a naturalistic form of inquiry that focuses on non-numerical data and explores processes, patterns, and meanings rather than solely outcomes (Nassaji, 2020). This approach is particularly valuable for gaining insights into the complexities and challenges associated with implementing Corporate Digital Responsibility (CDR) in the New Zealand tourism industry.

In this study, the data refers to publicly available website content from 30 New Zealand travel agencies that met the selection criteria. This includes their terms and conditions, privacy policies, contact information, presence of privacy officer details, and other elements relevant to CDR principles such as digital transparency, data governance, and ethical data handling. These online materials were collected and recorded in a Microsoft Excel spreadsheet.

The dataset was organised with columns dedicated to specific CDR-related variables, enabling structured coding. Coding involved categorising the qualitative data to identify patterns and recurring themes. Thematic analysis was then applied to

uncover key issues related to ethical practices, privacy protection, data management, and stakeholder inclusion (Guest et al., 2012). This method facilitated a deeper interpretation of the travel agencies' digital practices and their alignment with CDR principles.

By applying this approach, the study addresses two main research questions: (1) How do tourism agencies in New Zealand implement privacy practices and data management strategies to align with CDR principles? and (2) What are the key challenges faced by tourism organisations in New Zealand in achieving compliance with privacy legislation and integrating ethical digital practices into their operations?

3.3 Data collection

The secondary data were collected from Qualmark-accredited travel agents listed on the official Tourism New Zealand website. Qualmark®, Tourism New Zealand's official quality assurance organisation, awards certification to businesses that meet specific quality, environmental, and safety criteria. It serves as a trusted benchmark for travellers and industry stakeholders alike. The Qualmark logo, which includes the '100% Pure New Zealand' slogan and the silver fern, is widely recognised as a symbol of service excellence and reliable visitor experiences (Florek & Insch, 2008). As of August 2024, Tourism New Zealand has accredited 701 travel agents globally under the Qualmark standard. This certification signifies that these travel agents or organisations

have undergone specialised training by Tourism New Zealand and possess in-depth knowledge of the country.

This study excluded travel agents not based in New Zealand, narrowing the selection to 158 travel agents operating within the country, ensuring the accuracy of the data. Furthermore, only websites using the '.co.nz' or '.nz' domain names were selected from the 158 agents to guarantee that the data sources are directly linked to the New Zealand market. Using New Zealand-specific domain names was crucial in maintaining the credibility of the data. A domain name serves as an identifier for a computer system, replacing numerical Internet Protocol (IP) addresses with readable text (Liddicoat, 2019). The '.co.nz' domain is more representative of the New Zealand market, whereas a '.com' domain may indicate that a company is either not based in New Zealand or does not primarily target the New Zealand market.

Furthermore, all entities with domain names ending in '.nz' or '.co.nz' are regulated by InternetNZ (Liddicoat, 2019). These domain holders must comply with InternetNZ regulations. According to the Fifth Edition of the .nz Dispute Resolution Scheme Rules, which took effect on 1 October 2024, "domain name holders and their registrations will be governed by the laws of New Zealand, and they will comply with all obligations set out in these '.nz' Rules, their contracts with registrars, and any other relevant agreements" (InternetNZ, n.d.).

3.4 Sampling

For this study, data on travel agents with Qualmark accreditation were collected from the official Tourism New Zealand website for sampling purposes. The dataset was filtered to identify valid web pages, focusing on those using the ‘.co.nz’ domain. Following the sampling process, the selected travel agent websites were systematically reviewed to assess the presence of key elements, including terms and conditions, privacy policies, booking policies, legal restrictions, and privacy officer information.

Excel was utilised as the primary data analysis tool to conduct fundamental statistical analyses, such as calculating percentages and generating figures to visualise the data. The percentages and other numerical findings were examined to identify patterns, trends, and potential correlations. The primary objective of this analysis was to address the research questions effectively.

Table 1

Sample selected

TRAVEL AGENCIES	WEBSITE
34°SOUTH	https://www.34south.co.nz/
AMPED THE SKI ADVENTURE TRAVEL SPECIALISTS	https://www.amped4ski.co.nz/
ANZ SKY TOUR	https://www.anzskytours.co.nz/
CRUISE DEALS POWERED BY HOOT	https://www.cruisedeals.co.nz/
EXPERIENCE GOLF	https://www.experiencegolf.co.nz/
FINE TOURS NEW ZEALAND	https://www.finetoursnewzealand.co.nz/

GO2NEWZEALAND 2019 LTD	https://www.go2newzealand.nz/
GREAT DAYS NEW ZEALAND TOUR	https://greatdays.nz/
HOT EVENT	https://www.hotevents.co.nz/
HOUSE OF TRAVEL AUCKLAND CITY	https://www.houseoftravel.co.nz/
INTERNATIONAL STUDENT TOURS	https://studenttours.co.nz/
KATETRAVEL NEW ZEALAND	https://www.katetravel.co.nz/
LUXURY PRIVATE GUIDED TOURS NEW ZEALAND	https://www.arohatours.co.nz/
MATESRATES CAR HIRE	https://www.matesratescarhire.co.nz/
NEW ZEALAND FISHING LODGES	https://www.newzealandfishinglodges.co.nz/
NEW ZEALAND TOUR	https://nztour.co.nz/
NEW ZEALAND SELF DRIVE TOURS	https://www.newzealandselfdrivetours.co.nz/
NZ TRAVEL BROKERS LTD	https://nztravelbrokers.co.nz/
PAR NZ GOLFING HOLIDAYS	https://www.parnz.co.nz/
PLAYING AROUND NEW ZEALAND	https://playgolf.co.nz/
PUKEKOHE TRAVEL	https://www.pukekohetravel.co.nz/
RELAXING JOURNEYS	https://www.relaxingjourneys.co.nz/
SEASONZ TRAVEL	https://www.seasonz.co.nz/
SETTLERS TOURS	https://hello-newzealand.co.nz/
THRIFTY TOURS NEW ZEALAND	https://www.thriftytours.co.nz/
VYOM JOURNEYS	https://www.vyomjourneys.co.nz/
XPERIENZ	https://xperienz.nz/
YNZ HOLIDAY	https://www.oceaniacc.co.nz/
YOUNG PROFESSIONALS TRAVEL (YOPRO TRAVEL)	https://www.yoprotravel.co.nz/
ZEST4TRAVEL	https://www.zest4travel.co.nz/

Thirty New Zealand travel agencies that met the selection criteria were chosen. The data were recorded in a Microsoft Excel spreadsheet and systematically coded for specific variables, including relevant terms and conditions, privacy policies, contact details, privacy officer information, and other CDR-related factors. Coding involved systematically categorising qualitative data to identify patterns and themes, thereby facilitating the organisation and interpretation of the dataset.

The dataset consisted of 30 travel agencies, with columns dedicated to specific aspects of CDR practices. Once the data had been collated and summarised, the prevalence of CDR-related practices in the New Zealand tourism industry was quantified using percentage calculations. The results of the research objectives were analysed and compared with existing literature to identify consistencies, discrepancies, and research gaps. This study provided targeted insights and recommendations for enhancing CDR practices within New Zealand's tourism industry.

3.5 Data analysis techniques

Thematic analysis was employed in this study to capture the complex meanings of textual datasets (Guest et al., 2012) and to classify and analyse the collected data. The findings were categorised into themes based on the secondary qualitative data gathered, which enabled an organised understanding of key aspects of Corporate Digital Responsibility (CDR) in the New Zealand tourism industry. Each theme was supported

by data evidence. The identified themes included privacy, legislation, and CDR implementation.

Figure 3

Phases of thematic analysis

Phase	Description of the process
1. Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

Note. Braun & Clarke's six-phase framework for doing a thematic analysis. From "Using thematic analysis in psychology" by Braun, V., & Clarke, V, 2006, *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi-org.ezproxy.aut.ac.nz/10.1191/1478088706qp063oa>.

A According to Braun and Clarke's (2006) six-phase framework for thematic analysis, the first phase involves familiarising oneself with the data through repeated reading and active engagement. In this study, reviewing the secondary data collected from the websites of New Zealand travel agents allowed for an in-depth understanding of the content. This process supported the identification of initial observations and ideas about how various digital practices—such as privacy policies, data handling, and disclosure statements—might relate to broader Corporate Digital Responsibility (CDR) principles.

The second phase involved generating initial codes from the familiarised data. The information was entered into a Microsoft Excel spreadsheet and systematically coded for each relevant variable. These variables included, but were not limited to, the presence of a privacy policy, disclosures regarding third-party data sharing, and booking conditions. The resulting codes formed a list that highlighted key aspects of digital accountability practices among the sampled travel agents.

Figure 4

Table with coded examples

Term & Condition	Privacy condition	Booking Condition	Third Party Usage (Cookies)	Location	Privacy Officer
Yes	Yes	Yes	Yes	Auckland	None
Yes	Yes	Yes	Yes	Queenstown	Yes
Yes	No	Yes	Not Clear	Auckland	None
No	No	No	Not Clear	Auckland	None
No	No	No	Not Clear	Auckland	None
Yes	Yes	Yes	Yes	Wanaka Town	None
Yes	Yes	Yes	Yes	Wanaka Town	None
Yes	No	No	Not Clear	Tokoroa	None
No	No	No	No	Auckland	None
Yes	No	Yes	Yes	Wanaka Town	None
No	No	No	No	Auckland	None
No	No	No	No	Dunedin	None
No	Yes	No	Yes	Auckland	None
Yes	Yes	Yes	Yes	Taupo	None
Yes	Yes	Yes	Yes	Auckland	None
Yes	Yes	Yes		Auckland	Yes
No	No	No	No	Wellington	None
No	Yes	No	No	Tauranga	None
Yes	Yes	Yes	Yes	Palmerston North	None
No	No	No	No	Christchurch	None
Yes	Yes	Yes	Yes	Auckland	Yes
Yes	Yes	No	Yes	Nelson	None
Yes	No	Yes	No	Queenstown	None
No	No	Yes	No	Christchurch	None
No	No	No	No	Christchurch	None
Yes	Yes	Yes	No	Pukekohe	None
No	No	No	No	Auckland	None
Yes	No	Yes	No	Auckland	None
Yes	yes	No	No	Nelson	Yes
Yes	Yes	No	No	Auckland	None

Note. The table above demonstrated the process of coding. The study examined the websites of selected New Zealand tourism organisations to identify specific words that

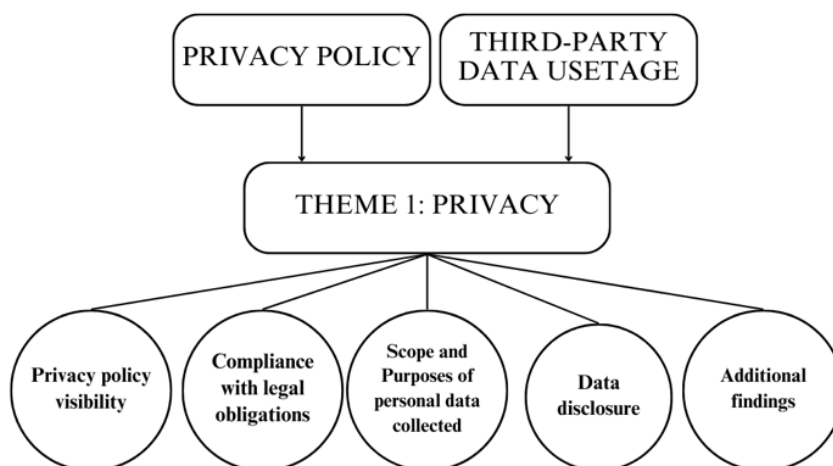
frequently appeared on tourism websites based on themes. These included privacy policies, terms treaties, booking terms, third-party use, and privacy officer information.

After the coding process, relevant codes were grouped into broader thematic categories. For instance, the privacy policy and third-party data sharing codes were classified under the privacy theme. The codes related to terms and conditions formed the regulation theme, and the privacy officer code was categorised under the guidance theme. The ‘searching for themes’ phase assisted in organising data corresponding to each potential theme.

During the ‘review of themes’ phase, the emerging themes were revisited to ensure they accurately represented the data. For example, it was examined whether the privacy policy was relevant to the privacy theme and whether the data was valuable and applicable. Additionally, sub-themes such as the scope and purpose of personal data collected by New Zealand travel agencies and data disclosure were explored in step 5, Define and Name the Themes. Once the viability of the themes was assessed, this study defined and named the themes. Each theme was described in detail, including its relevance to corporate digital responsibility practices and its relation to the research questions.

Figure 5

Example of coding definition and naming theme



Note. The coding tree visualised how the Corporate Digital Responsibility (CDR) principles were categorised in the research findings. The figure above illustrated Theme 1: Privacy. Privacy reflected how travel organisations handled user data based on privacy policies and third-party data usage found on travel agencies' websites. These categories were further divided into five sub-themes: privacy policy visibility, which assessed travel organisations' transparency; compliance with legal obligations, which evaluated whether organisations adhered to privacy laws such as the New Zealand Privacy Act 2020; the scope and purpose of personal data collected; data disclosure; and other relevant findings.

The final step involved producing a detailed analytical report based on the data and thematic narratives. This report included examples of data for each theme, such as specific quotes or excerpts from travel agency websites and percentages derived from the analysis. It also linked the analysis to the research questions and existing literature,

discussing gaps, trends, and challenges related to CDR practices in the New Zealand tourism industry.

3.6 Ethics Considerations

This research did not require AUTEK/ethical approval, as it relied solely on secondary data obtained from publicly available sources, such as tourism organisations' websites. Nevertheless, I acknowledged that ethical responsibilities remained paramount. I was committed to upholding the highest ethical standards by respecting the rights, privacy, and well-being of all individuals and organisations connected to the data. This included avoiding any misrepresentation of the information analysed. These ethical principles were diligently maintained throughout the entire research process.

Although the analysed data were publicly accessible, the privacy and reputational interests of the organisations involved were carefully considered. To preserve confidentiality and prevent direct identification, each travel agency was referred to by a numerical identifier (e.g., Agency 1, Agency 2) throughout the analysis. This approach ensured clarity and consistency while safeguarding organisational anonymity.

All data, including contact details and privacy policies, were collected from publicly accessible sources such as official travel agency websites. The contact information, including privacy officer details and complaint channels, was taken exactly as presented on these websites at the time of data collection. No private or non-

public information was accessed or used in this study. The inclusion of such details is intended solely to illustrate how travel agencies communicate privacy responsibilities and to analyse their compliance with Corporate Digital Responsibility principles.

It was acknowledged that the study included comparative observations and evaluative comments, particularly when highlighting examples of practice in Corporate Digital Responsibility (CDR). These comparisons were made strictly based on publicly available information and aimed to provide constructive insights into industry-wide patterns and opportunities for improvement. All evaluative statements were supported by transparent criteria aligned with CDR principles, and no negative assumptions were made about any organisation beyond what was explicitly evident in the reviewed data.

Findings

In the context of digital transformation reshaping global industries, the concept of CDR has emerged as an important framework for guiding responsible digital practices within organisations. The five application areas for CDR are digital stewardship, digital transparency, digital empowerment, digital equity, and digital inclusion.

This study evaluates the implementation of CDR principles by travel companies in New Zealand, using the five-point CDR application framework outlined by Accenture. Thirty travel organisations were analysed for privacy, data transparency, and customer empowerment practices. Digital stewardship refers to travel agents' responsible use of data, ensuring privacy and security. Digital transparency focuses on whether travel agents provide clear, transparent communication regarding the use of customer data. Digital empowerment involves enabling customers with digital tools and guidance to enhance their experience and control over personal data. Digital equity refers to the fair distribution of profits derived from customer data and includes the travel agent's commitment to never misuse this information. Lastly, digital inclusion ensures that the company's data is available for research while maintaining inclusive data practices.

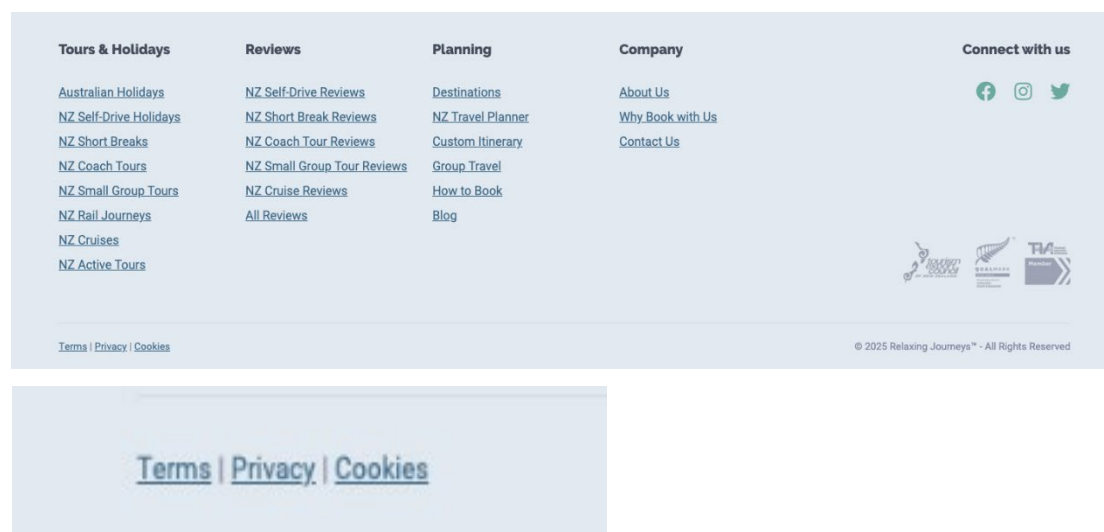
4.1 Privacy

4.1.1 Privacy policy visibility

Privacy policies regulate how internet service providers interact with their users while enabling users to monitor how companies handle their data. The sample for this research consisted of links to the official websites of 30 travel agencies. By reviewing the web pages of these travel companies, the study gathered information on whether the companies had listed a privacy policy on their sites. According to the findings, Theme 1 (Privacy): 50% of the companies have listed privacy conditions on their websites. In contrast, 50% of companies could not find privacy conditions on their websites.

Figure 6

Sample commercial website.



Note. The screenshot of the details provided above comes from the official website of a New Zealand travel agency, which offers background information about its services, destinations, and organisational structure. This example demonstrates how a commercial tourism website typically presents its privacy policy. Privacy policies are usually located at the website's bottom section, along with terms and conditions and

cookie information. Users must scroll to the bottom of the webpage to access the privacy policy.

The findings indicated a significant gap in privacy transparency among travel agencies. Fifty per cent of the companies did not have an easily identifiable privacy policy on their web pages. Privacy policies were essential as they informed users about how companies handle their personal data. As highlighted in existing literature, when users are unaware of a company's terms and conditions, they may unknowingly agree to use their personal information in ways they disapprove of (Steinfeld, 2016). A privacy policy outlines what information the company collects, how it is used, why it is necessary, and what rights users have regarding their data processing. Without a privacy policy, trust between the user and the company may be undermined, leading to a potential breach of privacy.

4.1.2 Compliance with legal obligations

Under the Privacy Act 2020, Information Privacy Principle 3 (IPP 3) on collecting information from subjects stipulates that if an organisation needs to collect personal information, it must take reasonable steps to ensure that the individual is aware. The organisation must disclose the fact that information is being collected, the purpose for which it is being collected, and who will use or collect the information—such as the

name and address of the agency collecting the information, the agency storing it, and the rights of individuals under IPP to access and correct the information they provide.

These regulations protect user privacy by ensuring transparency and accountability in data processing practices. Of the 50% (15) of travel agents that have a privacy policy on their webpage, all of them inform their customers/users of the purposes for which they collect information and what information they collect. Typically, travel agents collect information about their customers to market products and services, contact customers electronically, and improve the customer experience. In addition, the privacy policy usually indicates how travel agencies handle data disclosure, data protection, user rights, and other issues related to digital responsibility.

Figure 7

Example of travel agency privacy policy page.

INTRODUCTION

Seasonz Travel Limited (we, us, our) complies with the New Zealand Privacy Act 1993 (the Act) when dealing with personal information. Personal information is information about an identifiable individual (a natural person).

This policy sets out how we will collect, use, disclose and protect your personal information.

This policy does not limit or exclude any of your rights under the Act. If you wish to seek further information on the Act, see www.privacy.org.nz.

CHANGES TO THIS POLICY

We may change this policy by uploading a revised policy onto the website. The change will apply from the date that we upload the revised policy.

WHO DO WE COLLECT YOUR PERSONAL INFORMATION FROM

We collect personal information about you from:

You, when you provide that personal information to us, including via the website and any related service, through any registration or subscription process, through any contact with us (e.g. telephone call or email), or when you buy or use our services and products.

Third parties where you have authorised this or the information is publicly available.

If possible, we will collect personal information from you directly.

HOW WE USE YOUR PERSONAL INFORMATION

We will use your personal information:

To verify your identity.

To provide services and products to you.

To market our services and products to you, including contacting you electronically (e.g. by text or email for this purpose).

To improve the services and products that we provide to you.

To bill you and to collect money that you owe us, including authorising and processing credit card transactions.

To respond to communications from you, including a complaint.

To conduct research and statistical analysis (on an anonymised basis).

To protect and/or enforce our legal rights and interests, including defending any claim.

For any other purpose authorised by you or the Act.

DISCLOSING YOUR PERSONAL INFORMATION

We may disclose your personal information to:

Any business that supports our services and products, including any person that hosts or maintains any underlying IT system or data centre that we use to provide the website or other services and products.

Other third parties (for anonymised statistical information).

A person who can require us to supply your personal information (e.g. a regulatory authority).

Any other person authorised by the Act or another law (e.g. a law enforcement agency).

Any other person authorised by you.

A business that supports our services and products may be located outside New Zealand. This may mean your personal information is held and processed outside New Zealand.

PROTECTING YOUR PERSONAL INFORMATION

We will take reasonable steps to keep your personal information safe from loss, unauthorised activity, or other misuse.

ACCESSING AND CORRECTING YOUR PERSONAL INFORMATION

Subject to certain grounds for refusal set out in the Act, you have the right to access your readily retrievable personal information that we hold and to request a correction to your personal information. Before you exercise this right, we will need evidence to confirm that you are the individual to whom the personal information relates.

In respect of a request for correction, if we think the correction is reasonable and we are reasonably able to change the personal information, we will make the correction. If we do not make the correction, we will take reasonable steps to note on the personal information that you requested the correction.

If you want to exercise either of the above rights, email us at info@seasonz.co.nz. Your email should provide evidence of who you are and set out the details of your request (e.g. the personal information, or the correction, that you are requesting).

We may charge you our reasonable costs of providing to you copies of your personal information or correcting that information.

INTERNET USE

While we take reasonable steps to maintain secure internet connections, if you provide us with personal information over the internet, the provision of that information is at your own risk.

Note. The above screenshot shows the contents of a New Zealand travel agency's privacy policy, highlighting the significance of the policy, which outlines what personal information the company collects, what it is used for, and how it stores and protects user data. Key sections typically include data collection methods, the use of personal information, third-party sharing policies, and customer rights regarding data privacy.

4.1.3 Scope and Purposes of personal data collected

New Zealand travel agencies collect various types of personal information from customers to facilitate their services. This includes basic identifying details, contact information, payment details, health data, and other random information. The purpose of collecting such data varies between agencies, ranging from identity verification and service improvement to marketing and compliance with legal requirements.

Basic Identifying Information (Full name, Date of birth, etc.)

- ***Travel Agency 23*** “ *will collect client’s personal information to verify identity. To conduct research and statistical analysis (on an anonymised basis). To protect and/or enforce our legal rights and interests, including defending any claim. And for any other purpose authorised by you or the Act.* ”
- ***Travel Agency 22*** *collect client’s personal information “To facilitate the Services and business operations. To improve our website, Services, marketing, customer relationships and experiences (using data analytics etc.);*
- ***Travel Agency 10*** “ *collect your name, email address, user name, password, phone number, demographic information, date of birth, address, location and any other information we require or ask for to set you up with an account.* ”

Contact details (phone number, email address, and postal address);

- **Travel Agency 23** collect client's contact detail to provide services and products.
To market their services and products. To respond to communications from clients, including a complaint. And to improve the services and products.
- **Travel Agency 22** collect client's contact detail for "marketing and communication purposes, to notify you about changes or updates to the Services"
- **Travel Agency 25** will retain client contact details for communication and marketing purposes. "Any marketing emails we send will provide you with an unsubscribe option. You can view all the data we hold about you on request."

Payment Information (Billing address, Credit or debit card details);

- **Travel Agency 23** collects Financial Information "To bill you and to collect money that you owe us, including authorizing and processing credit card transactions."
- **Travel Agency 5** "use your payment information to process transactions securely."
- Credit card details are required to make an enquiry or booking with **Travel Agency 2** "However, **Travel Agency 2** does not store credit card numbers. Therefore, customers will need to provide us with their credit card number for each payment transaction."

Health Information (Medical conditions, Emergency contact details)

- **Travel Agency 11** “...so-called sensitive personal data is collected for any medical requirements...”

Other random information

- **Travel agency 10** “We also collect the following sensitive or special categories of personal information: personal data revealing racial or ethnic origin and religious or philosophical beliefs (Sensitive Information).”
- **Travel agency 19** collects “club affiliation and membership details”
- **Travel agency 11** collects browsing history such as “IP address (Internet Protocol address) of the computer from which the Studenttours-website is accessed; Internet address of the website from which the Studenttours-website was accessed (so-called origin or referrer URL); Name of the retrieved files or information; Date and time as well as duration of the call; transferred amount of data; Operating system and information about the internet browser of the computer accessing the Studenttours-website; http status code (e.g., “request succeeded” or “requested file not found”).”

New Zealand travel agents collect personal data for various purposes, typically aligned with service delivery, legal compliance, and business enhancement. However, the specific uses of data collection practices can vary between agencies.

A prevalent use is identity verification, which helps to ensure that customers are who they claim to be. Additionally, personal information is frequently utilised to improve services and business operations. For instance, Travel Agency 22 clearly outlines the various purposes of its data collection, linking it directly to service improvement and operational efficiency. This includes using data analysis to enhance service offerings and for marketing and communication purposes, which allows users to understand how their data contributes to an improved customer experience. Other common personal data uses include contact information for communication and marketing purposes and secure payment processing.

Some agencies, offer clients with greater control regarding the use of contact information, like Travel Agency 25, providing customers with an option to unsubscribe from marketing emails. This allows users to control their data and builds trust. Travel Agencies 2 and Travel Agencies 5 focus on securely handling payment transactions when collecting payment information. Travel Agency 5, for example, explicitly states that it does not store credit card numbers, providing users with clear insights into how payment information is managed and reducing the risks of data breaches.

In addition to service-related purposes, some agencies use personal information for research. Travel Agency 23 specifies that identifying information is used for

anonymised research and statistical analysis and emphasises compliance with New Zealand's Privacy Act, ensuring the protection of users' rights.

When collecting sensitive health information, Travel Agency 11 implements precise consent mechanisms and explains how the data will be processed and why it is necessary for safety and emergency preparedness. Travel Agencies 10 and 11 provide transparency about sensitive personal data, such as racial or ethnic origin and religious beliefs, and digital tracking data, helping users understand how their online activities are monitored.

Transparent data usage descriptions enhanced user trust, as seen in Travel Agencies 5 and 22, which explicitly linked data collection to service improvements. Second, user control was strengthened through opt-out options (e.g., Travel Agency 25).

4.1.4 Data disclosure

The study results revealed that 15 travel agencies clearly stated their data collection purposes in privacy policies. Additionally, 14 agencies disclosed whether personal data was shared with third parties, as shown in Table 2.

Table 2

Travel agencies with provide disclose

Agency	Disclosure Recipients
--------	-----------------------

<p>Travel agency 4 and Travel agency 10</p>	<ul style="list-style-type: none"> - <i>another company within our group in connection with any of the potential uses of your personal information identified above</i> - <i>any business that support our websites, products and services, including any person that hosts or maintains any underlying IT system or data centre that we use to provide our websites, products or services or that we use to process payments</i> - <i>a credit reference agency for the purpose of credit checking you</i> - <i>third parties (for anonymised statistical information)</i> - <i>professional advisers e.g. accountants, lawyers or auditors</i> - <i>a person who can require us to supply your personal information (e.g. a law enforcement agency or regulatory authority)</i> - <i>any other person with your consent</i> - <i>any other company in the case of a sale, merger, consolidation, liquidation, reorganisation or acquisition</i> - <i>any other person authorised by applicable law.</i>
<p>Travel agency 2</p>	<ul style="list-style-type: none"> - <i>provide statistical information about its sales, trading patterns, and information on navigation techniques to reputable third parties.</i>

Travel agency 5	<ul style="list-style-type: none"> - <i>Disclosure of Your Information for Third-Party Service Providers</i> - <i>Legal Requirements and Business Transfers.</i>
Travel agency 6	<ul style="list-style-type: none"> - <i>... with our suppliers</i>
Travel agency 8	<ul style="list-style-type: none"> - <i>Business transactions</i> - <i>Law enforcement</i> - <i>Other legal requirements.</i>
Travel agency 11	<ul style="list-style-type: none"> - <i>disclosure for the implementation of the services you have selected for partners of Study Nelson.</i>
Travel agency 14	<ul style="list-style-type: none"> - <i>We may disclose information when legally compelled to do so.</i>
Travel agency 15	<ul style="list-style-type: none"> - <i>- We keep your information safe by not sharing it with any third party and only using it to contact you directly with information relevant to your query.</i>
Travel agency 18	<ul style="list-style-type: none"> - <i>Share Your Personal Data to Authorised Third Parties.</i> - <i>Or with any legal obligations</i>
Travel agency 19	<ul style="list-style-type: none"> - <i>disclose your personal information in accordance with your authorisation and/or for the purposes.</i>
Travel agency 22	<ul style="list-style-type: none"> - <i>Your Personal Information will not be sold, traded, rented or otherwise provided to others without your consent.</i>

	<ul style="list-style-type: none"> - <i>third parties may submit requests to access information that has been generated from your use of our Services. This might include, for example, law enforcement or government agencies requesting information about you or Permitted Users.</i>
Travel agency 23	<ul style="list-style-type: none"> - <i>Any business that supports our services and products, including any person that hosts or maintains any underlying IT system or data centre that we use to provide the website or other services and products.</i> - <i>Other third parties (for anonymised statistical information).</i> - <i>A person who can require us to supply your personal information (e.g. a regulatory authority).</i> - <i>Any other person authorised by the Act or another law (e.g. a law enforcement agency).</i> - <i>Any other person authorised by you.</i> - <i>A business that supports our services and products may be located outside New Zealand</i>
Travel agency 25	<ul style="list-style-type: none"> - <i>we may be required to share limited information with our suppliers to enable reservations to be made (mostly names, country of origin and ages but in some cases, a contact</i>

	<p><i>number, address and email) to ensure that suitable and correct services are supplied.</i></p> <p><i>- We do not share email information or any other contact details with other parties.</i></p>
--	--

The recipients and uses of data disclosures vary across New Zealand's travel agencies, involving multiple parties in the collection and sharing process. Travel agencies collect personal data for various purposes, including booking, customer service, marketing, and legal compliance. Third-party service providers, such as accommodation providers, transport companies, and event organisers, also gather personal data to facilitate bookings, customer transactions, and other operational services. Additionally, law enforcement and government agencies may request access to personal data for legal or regulatory purposes. Business partners and statistical research entities often receive aggregated data to conduct analysis, gain transaction insights, and improve services.

Some travel agencies, such as Travel Agents 4, 10, and 23, offers more detailed disclosures, ensuring that customers are informed and in control of their data. For example, Travel Agent 23 adopts a comprehensive approach to data disclosure, clearly stating that it shares information with third parties supporting its services, including IT infrastructure providers and data centres. It also ensures transparency regarding sharing anonymised statistical data while limiting the disclosure of personal information to

legally authorised entities, such as regulators and law enforcement agencies. This level of clarity helps protect customer privacy and minimises the risk of misuse.

Travel Agencies 4 and 10 similarly emphasise that personal data may be shared within their corporate group, informing customers about the internal flow of their data. These agencies also specify data disclosures in the event of significant business changes, such as mergers, acquisitions, or reorganisations, allowing customers to anticipate potential data transfers. By listing authorised recipients, including credit reference agencies, legal professionals, and law enforcement agencies, these travel agents ensure that customers are fully aware of their data privacy rights and protections. In contrast, other travel agencies provide minimal disclosure or lack of clear transparency regarding the sharing of personal data.

4.1.5 Additional findings

Typically, privacy policies are located at the bottom of a website's homepage, and users can easily find them due to their consistent placement. However, while these policies are theoretically accessible, their readability remains a significant issue (Jensen & Potts, 2004). Many privacy policies, such as Travel Agency 11, use complex language, often with advanced vocabulary. This complexity can undermine the legal foundation of "informed consent" and make it difficult for users to understand their privacy rights fully. Furthermore, the study found that some travel agencies mention

potential changes to their privacy policies within the document. However, users are rarely notified of these updates directly, which may burden them more. To stay informed, users may need to frequently check individual websites for any changes to ensure their privacy rights are not compromised.

For example, in Travel agency 8: *“Changes to this Privacy Policy: We may update Our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.”* Travel agency 21 *“We may change this Privacy Policy from time to time, any change in the policy will be updated on our website and will apply from the date posted.”* and Travel agency 5: *“We may update this Privacy Policy from time to time. Any changes will be posted on this page with an updated revision date. Your continued use of our website following the posting of changes indicates your acceptance of those changes.”*

Requiring users to regularly review privacy policies and proactively check for updates imposes an unreasonable burden, especially for individuals who lack the time or inclination to review legal terms constantly. For instance, Travel Agency 5’s policy states that continued use of the site implies acceptance of any changes, placing the responsibility on users to remain informed and vigilant. Furthermore, most travel agencies in the sample did not provide clear or practical ways for users to easily identify

specific updates or changes, further hindering their ability to stay informed about their privacy rights.

However, there is a good practice of informed consent, with Travel agency 19: *“We may amend and update this Privacy Policy from time to time by posting a revised version on our website and/or App. Any changes will apply from the date we post the updated Privacy Policy on the website or App. If we make any significant changes, we will provide you with reasonable notice of such changes through the website or App, or via other means such as email.”* The best practices notify users of any changes to their privacy policies—such as via email—to ensure customers remain aware of how their personal information is handled and retain control over their data.

In conclusion, many of the privacy policies in this study fail to effectively serve users due to their complex language, lengthy content, and default user consent. These policies often contain advanced legal terminology that is difficult for the average user to understand, leading to confusion and undermining the principle of ‘informed consent’. As a result, users may unknowingly consent to compromising the security of their data. While this approach ensures broad legal coverage for companies, it does not adequately address users' needs, leaving them vulnerable to privacy risks.

4.2 Legal compliance

According to the findings, Theme 2 (Legal compliance) reveals that 60% of the companies listed terms and conditions on their websites, while 40% could not identify terms and conditions on their websites. Terms and conditions are a legal agreement between a company and its customers or potential customers, often found on websites and online services. These agreements usually include disclaimers to protect the business's interests. Clear and well-defined terms and conditions provide businesses with a structured framework to safeguard their interests and offer protection for consumers by clearly outlining their rights and defining how disputes will be handled.

The study found that 18 travel agencies (60%) in New Zealand included terms and conditions on their websites. These terms typically cover the booking process, currency and exchange rates, deposit or booking fees, payment and cancellation policies, and risk factors (such as natural disasters or man-made risks). Additionally, these terms usually address the company's liability for various services, such as package activities, transportation, accommodation, and customer support. Essentially, the terms and conditions act as a disclaimer, outlining the company's limited liability in certain situations, such as failure to perform or unforeseen circumstances.

However, a significant gap was observed in including consumer rights within these agreements. Only 13 travel agencies (43%) clearly stated in their terms and conditions or privacy policies that they comply with New Zealand law and are subject to the relevant national legislation. While most agencies include disclaimers about business responsibilities, customer rights and legal protections were often minimally addressed,

making it harder for consumers to fully understand how their rights are protected or enforced under New Zealand law or other applicable jurisdictions.

The companies listed below clearly state in their terms and conditions that they comply with the New Zealand law or offer customers the option to use either the New Zealand laws or the laws of other countries to protect their rights.

- **Travel Agency 23** *“(we, us, our) complies with the New Zealand Privacy Act 1993 (the Act) when dealing with personal information. Personal information is information about an identifiable individual (a natural person).”*
- **Travel Agency 22** *“processes personal information depending on the user's location. It always complies with applicable privacy laws and applicable anti-spam laws. If the user is in Australia, it complies with the the Privacy Act 1988 (Cth) (Australian Privacy Act), and the Spam Act 2003 (Cth); or if the user is in New Zealand, it complies with the Privacy Act 1993 and the Unsolicited Electronic Messages Act 2007; or if the user is in the United Kingdom, it complies with the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003.”*
- **Travel Agency 6, Travel Agency 25, Travel Agency 28** *“These terms and conditions should be read subject to and in conjunction with the provisions of the Consumer Guarantees Act and the Fair Trading Act (applicable in New Zealand) and do not affect your rights as expressed in these acts.”*

- **Travel Agency 8** *“These Terms are governed by the laws of New Zealand. Any disputes arising from these Terms or your use of our website will be subject to the exclusive jurisdiction of the courts of New Zealand.”*
- **Travel Agency 2** *“Any personal information that you disclose to us will be treated in accordance with the provisions of the Privacy Act 1993 and our Privacy Policy which appears on this Site, so far as we are in control of the same, except that it may be supplied to Providers. New Zealand law shall govern all information and Travel provided through the site.”*
- *“...Travel Agency 10 will be subject to New Zealand law and the jurisdiction of the New Zealand Courts. Suppliers and your contracts with them may be subject to different laws and jurisdictions.... Travel Agency 10 Limited and the entities within the Group, comply with the New Zealand Privacy Act 2020 when dealing with personal information.”*
- **Travel Agency 18:** *“This liability clause is subject to your rights under the Consumer Guarantees Act and nothing in these terms and conditions is intended to limit any rights you may have under the Consumer Guarantees Act or the Fair Trading Act.”*
- **Travel Agency 4** *“(we, us, our) comply with the New Zealand Privacy Act 2020 when dealing with personal information.”*
- **Travel Agency 15** *“This liability clause is subject to your rights under the Consumer Guarantees Act and nothing in these terms and conditions is intended to*

limit any rights you may have under the Consumer Guarantees Act or the Fair Trading Act.”

- **Travel Agency 21:** *Your rights. “Nothing in these Terms is intended to limit any rights you may have under the Consumer Guarantees Act 1993 or the Fair Trading Act 1986. Privacy. We understand and respect the importance of your privacy and we are committed to protecting your privacy in accordance with the Privacy Act 2020. ”*
- **Travel Agency 14** *maintain the information you send via e-mail in accordance with applicable New Zealand law. In compliance with the New Zealand Unsolicited Electronic Messages Act 2007 Act. These Terms and Conditions are governed by and construed in accordance with the laws of New Zealand. Any disputes arising under or in connection with these Terms shall be subject to the exclusive jurisdiction of the courts of New Zealand.”*

The findings of the study suggest that New Zealand travel agencies lack effective Corporate Digital Responsibility (CDR) practices, particularly in disclosing legal responsibilities and empowering consumers. Only 13 out of the 30 travel agencies sampled provided clear statements that they were subject to New Zealand law or any specific legal framework, which raises concerns about the level of transparency provided to customers regarding their rights and protections.

For example, Travel Agency 23 stands out by explicitly stating its compliance with the New Zealand Privacy Act 1993, ensuring that customers are aware of their rights to data protection under the New Zealand law. This disclosure provides clarity and helps build consumer trust, as customers are reassured that their data is managed according to established legal standards. In contrast, several other agencies, such as Travel Agency 6, Travel Agency 25, and Travel Agency 28, mention their compliance with the Consumer Guarantees Act 1993 and the Fair-Trading Act 1986 but fail to explain how these laws directly protect consumers. This lack of detail could confuse customers about their rights and legal recourse. The absence of clear communication on consumer protection under these laws diminishes the level of digital empowerment, which is a core component of CDR.

Moreover, although the terms and conditions section often contain disclaimers protecting business interests, they rarely address consumer rights in a clear and accessible way. This imbalance—focusing on business protection while neglecting to empower consumers—highlights a significant gap in CDR practices. If consumers are unaware of the legal protections available to them, they cannot make informed decisions or take the necessary actions to safeguard their interests. The failure to adequately empower customers in this regard weakens their confidence in travel agencies and undermines trust in their ability to handle personal data and provide fair treatment.

4.3 Guidance

Organisational consensus on CDR is essential to ensure clear guidance on its implementation (K. V. Carl et al., 2022), and in particular, a department should be established to manage the CDR programme. Under New Zealand's privacy laws (Privacy Act 2020, Ministry of Justice), organisations must appoint one or more individuals to act as the organisation's Privacy Officer, whose responsibilities include encouraging the agency to comply with the IPPs, dealing with requests made to the agency under this Act; working with the Commissioner in relation to complaints, investigations, and proceedings; and ensuring that the agency complies with the provisions of the Act.

Travel agency 22 provides clients with three different privacy officer's contact details in the contact information section.

- *“We take your concerns very seriously. If you have any questions or comments about this Policy, or wish to make a complaint or exercise your privacy rights, please contact our Privacy Officer using the details below:*

Country Contact Details

Australia Phone: +61 7 5556 5556

Post: ANZCRO

Attn: Privacy Officer

Address: Level 1, 6 Short Street, Southport QLD 4215

Email: privacy@anzcro.com.au

New Zealand Phone: +61 7 5556 5556

Post: ANZCRO

Attn: Privacy Officer

Address: Level 1, 6 Short Street, Southport QLD 4215

Email: privacy@anzcro.com.au

UK Phone: +61 7 5556 5556

Post: ANZCRO

Attn: Privacy Officer

Address: Level 1, 6 Short Street, Southport QLD 4215

Email: privacy@anzcro.com.au”

In addition, if clients are not satisfied with the response from Travel agency 22, they also provide clients with alternative complaints organisations.

“Country Office

The Office of the Australian Information Commissioner (OAIC) via the OAIC

Australia website:

www.oaic.gov.au.

The New Zealand Privacy Commissioner via the website:

New Zealand *https://www.privacy.org.nz/your-rights/making-a-complaint/*

United Kingdom *The Information Commissioner's Office (ICO) via the website*

https://ico.org.uk/global/contact-us."

"We would, however, appreciate the chance to deal with your concerns before you approach one of these entities, so please do get in touch using the details above in this section."

Travel Agency 4, Travel Agency 10, and Travel Agency 11 have mentioned the privacy officer position. Only 4 (13%) of the 30 New Zealand travel agents indicated a privacy officer in their privacy policy or terms and conditions, highlighting a significant gap in digital stewardship. The lack of a designated privacy officer at most travel agencies may undermine their ability to manage data responsibly and communicate effectively with customers. The absence of a privacy officer role also hinders the development of consistent policies to address privacy issues. Furthermore, the lack of a Privacy Officer at most travel agencies indicates that most travel agents in New Zealand fail to maintain good digital empowerment practices and digital equity in implementing CDR. Customers may not have a clear channel to address privacy concerns without a dedicated role such as a Privacy Officer.

Travel Agent 22 is an example of best practice in this area. It has a Privacy Officer listed on its business website and clear and easy-to-understand contact details for customers across multiple locations (Australia, New Zealand, and the UK). The agency demonstrates excellent digital transparency by proactively making it easy for customers to contact the appropriate person with privacy-related questions. It also exemplifies digital empowerment, as customers are given the option to resolve concerns, enabling them to take action where necessary.

4.4 Data Management

The more personal data travel agencies collect, and their data increases, the more consumers' concern over privacy violations and a lack of control over their private information also rises (Culnan, 1993). Therefore, data management is a crucial part of validating CDR practices. Similarly, the New Zealand Privacy Act has enacted specific regulations to protect information security (Ministry of Justice, 2020). Under the Information Privacy Principle 5, "Storage and security of personal information," an agency that holds personal information must ensure that the information is protected by reasonable security safeguards against loss and unauthorised access, use, modification, or disclosure, as well as other misuse. If personal information needs to be shared with another person or organisation to provide a service on behalf of the agency, the agency is required to take all reasonable steps to prevent any unauthorised use or disclosure of

that information. The table below shows the different approaches taken by travel agencies in New Zealand regarding data management and protection.

Table 3

Data management and security practices of selected New Zealand travel agencies

Travel Agency	Data Management and Security Practices
Travel agency 4	<i>"We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks inherent in processing personal information. You play an important role in keeping your personal information secure by maintaining the confidentiality of any password and accounts used in relation to our products and services. Notify us immediately if there is any unauthorised use of your account or any other breach of security."</i>
Travel agency 5	<i>"We implement appropriate security measures to protect your personal information from unauthorized access, alteration, disclosure, or destruction. However, no method of transmission over the Internet or electronic storage is 100% secure, so we cannot guarantee absolute security."</i>
Travel agency 8	<i>"The security of your personal data is important to us, but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security."</i>
Travel agency 10	<i>"We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks inherent in processing personal information. You play an</i>

	<p><i>important role in keeping your personal information secure by maintaining the confidentiality of any password and accounts used in relation to our products and services. Notify us immediately if there is any unauthorised use of your account or any other breach of security."</i></p>
Travel agency 14	<p><i>"We request that you do not send private information to us by email. However, doing so is allowed, but at your own risk. Some of the information you may enter on our website may be transmitted securely via Secure Sockets Layer (SSL). Credit card information and other sensitive information are never transmitted via email. We use software programs to monitor network traffic for unauthorized attempts to change or damage information."</i></p>
Travel agency 15	<p><i>"We keep your information safe by not sharing it with any third party and only using it to contact you directly with information relevant to your query. However, we cannot be held responsible for any cyber-attack or other breach of security. Financial information is only gathered through personal phone calls and stored securely on our server."</i></p>
Travel agency 21	<p><i>"We will not sell, rent, or lease your personal information to third parties. In accordance with the Privacy Act 1993, you may access and change your personal information at any time. We will take all reasonable steps to keep your information secure."</i></p>
Travel agency 22	<p><i>"We implement a variety of security measures to protect the loss, misuse, and alteration of your Personal Information when you enter, submit, or access your Personal Information. While we endeavour to protect the privacy of your account and</i></p>

	<i>Personal Information we hold, we cannot always guarantee complete security. There are a number of measures you need to take to keep your information secure, such as choosing a strong password."</i>
Travel agency 23	<i>"We will take reasonable steps to keep your personal information safe from loss, unauthorised activity, or other misuse."</i>

Effective data management and security practices are fundamental to ensuring the protection of personal information and demonstrating a travel agency's commitment to Corporate Digital Responsibility (CDR). While many agencies acknowledge the importance of safeguarding client data, the depth and clarity of their policies vary considerably.

Travel agency 11 (The best practice)

- *In principle, you can visit our internet pages or use the online services without having to provide any personal information. Only anonymous access data is stored, e.g. the name of your Internet Service Provider (ISP), the website from which you are visiting us, or the name of the requested file. This data is collected and evaluated exclusively for the purpose of improving our online offer; they are at least temporarily stored by us and deleted after a purely statistical evaluation; they do not allow any conclusion on your person.*
- *Personal data is individual information about personal or factual circumstances of a person. Personal data will only be collected if you provide such in the context of*

contacting us via our booking or contact form. Personal data includes, for example, name, address, telephone number and e-mail address. We use the personal data in accordance with the applicable statutory provisions, in with the data protection provisions of the German Telemedia Act (TMG) and the German BDSG.

- *All data from the enrollment will be transferred to the database and processed there for the execution of the enrollment process and participation on our tour.*
- *Study Nelson, in accordance with the state of the art, undertakes all necessary technical and organizational efforts to safeguard your personal data from loss, falsification or knowledge of unauthorized persons.*
- *Erasure concept: The user has the right to revoke a given consent with effect for the future at any time.*
- *The deletion of the stored personal data takes place when the user revokes the consent to the storage, when your knowledge is no longer necessary to fulfill the purpose of the storage, the contractual relationship is terminated or if your storage for other legal reasons is inadmissible. Data for billing purposes and accounting purposes are not affected by a request for cancellation.*
- *Personal data of participants and their parents will be kept until the end of the 7th year after the regular end of the tour due to New Zealand statutory retention periods. Study Nelson affiliates retain data submitted to them by Study Nelson in accordance with their respective national regulations.*

Data management practices are crucial in protecting personal information and compliance with privacy regulations such as New Zealand's Privacy Act 2020. Only 10 agencies mentioned data security in their privacy policies to safeguard client information from loss, misuse, and unauthorised access. While some agencies emphasise general security measures, others take more detailed approaches to data protection. For example, Travel Agencies 5 and 23 mention implementing "reasonable security measures" but fail to outline specific methodologies, ambiguous policies weaken trust.

In contrast, Travel Agencies 10 and 22, and others provide more robust details on their data security practices. These agencies acknowledge the inherent limitations of online security and outline specific measures, such as encryption and strong password strategies, to protect client data. These practices demonstrate a higher level of digital transparency and empowerment, as clients are made aware of the specific measures taken to secure their personal information, empowering them to take appropriate actions to safeguard their privacy.

Travel Agencies 14 and 29 also adopt security practices such as using secure servers and external platforms for data storage and advising clients not to send sensitive data via unsecured email. These practices help mitigate the risks of data breaches and unauthorised access, reflecting a commitment to digital stewardship by ensuring that clients are informed about how to protect their data. The sample's best example of data management practices comes from Travel Agency 11. This agency implements a

comprehensive approach that includes limiting data collection, establishing regular data deletion policies, and adhering to legal retention periods. It ensures that data is only retained when necessary and that clients' personal information is not kept longer than required. Travel Agency 11's proactive approach to data minimisation and retention policies ensures that client data is handled responsibly, minimising the risks associated with unnecessary data storage.

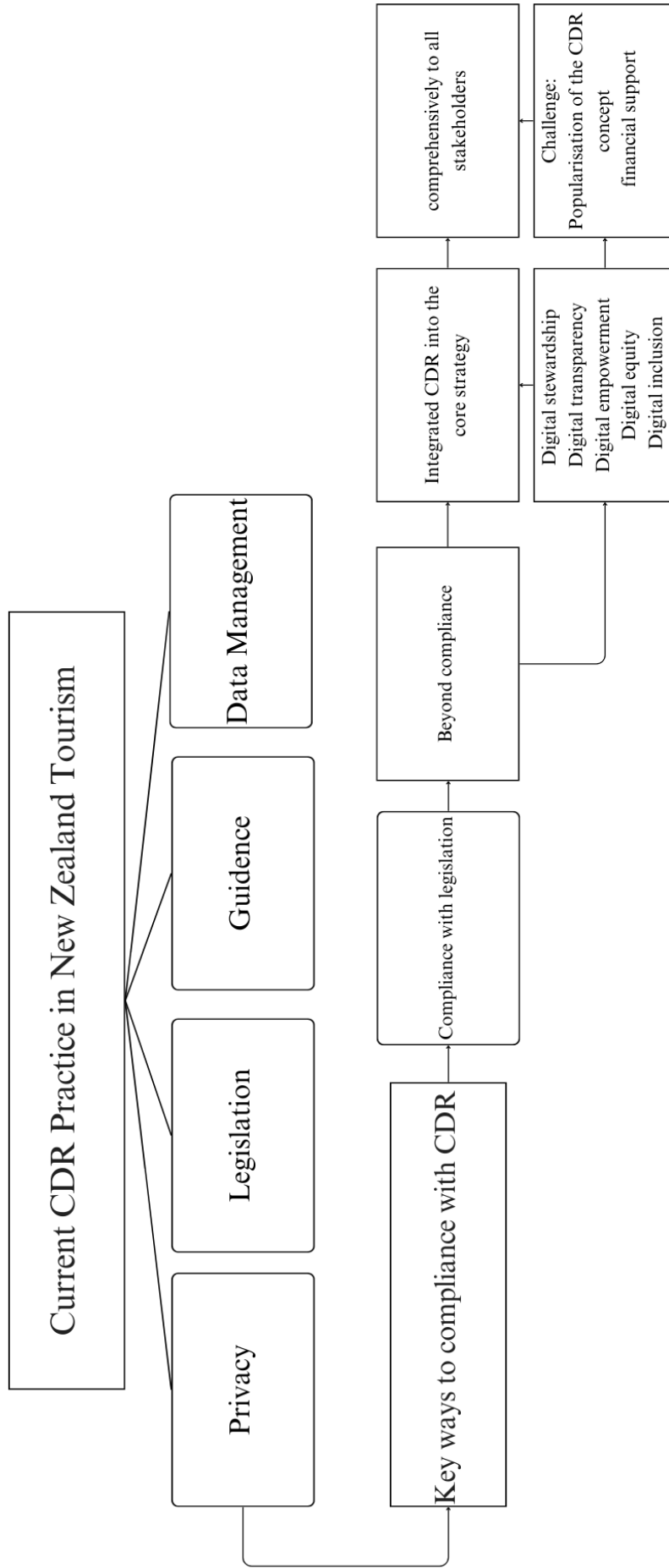
While some New Zealand travel agents have demonstrated strong data management practices by adopting encryption, strong passwords, and secure storage methods, most travel agents do not specify how they address the risks inherent in data security on their privacy policy pages. The lack of well-practised data management reflects the challenges in digital stewardship and digital equity in the implementation of CDR.

4.5 Summary

Based on the findings, this research illustration (figure 8) presents a structured framework outlining the current CDR practices among tourism agencies in New Zealand. It also provides basic steps for effectively implementing Corporate Digital Responsibility (CDR) in New Zealand travel agencies. The framework emphasises an incremental approach, starting with essential legal compliance and progressing to the full integration of CDR into business strategies.

Figure 8

CDR practice in New Zealand tourism



Firstly, from the findings, the CDR practices of New Zealand tourism organisations centred around privacy policies, identifying four key areas: privacy, legislation, guidance, and data management. Travel organisations showed variations in their privacy policies. Some travel agents provided clear and detailed information about data collection and protection, while others offered vague or no information. In terms of privacy transparency, the performance of each travel agent varied.

Secondly, compliance with the New Zealand Privacy Act 2020 remains inconsistent. The findings indicate that most organisations have not appointed a privacy officer, leading to poor data protection and security practices, disclosure, and consumer rights safeguarding. This highlights the need for more vigorous enforcement and industry-wide awareness. Furthermore, the lack of a designated privacy officer underscores the absence of proper guidance within the tourism industry. Travel agents largely follow the most basic legal requirements, but no standardised framework guides CDR implementation, resulting in a gap in digital practices across New Zealand's tourism sector.

The industry exhibits varying levels of maturity when it comes to data management. Some agencies have policies for secure data storage, encryption, and anonymisation, while others have not mentioned any data management practices, possibly due to resource constraints. Digital responsibility efforts are further complicated by unclear stewardship, insufficient consumer control over personal data, and inadequate cybersecurity measures.

An incremental approach to CDR implementation is proposed to address these challenges. First, agencies must ensure full compliance with the Privacy Act 2020 by improving privacy policies and data management practices. Second, they should go beyond legal compliance to enhance customer trust through five key CDR principles. Digital Stewardship requires establishing internal policies and appointing a Privacy Officer to oversee data management, ensuring compliance with legal and ethical standards. Digital Transparency involves disclosing data collection, usage, and sharing practices on official websites to enhance customer trust. Digital Empowerment encourages organisations to provide customers with tools to manage their data, granting them greater control over their personal information. Digital Equality can be achieved through data minimisation and advanced security measures to prevent misuse and unauthorised access. Lastly, Digital Inclusion calls for community collaboration to promote inclusive data practices, ensuring that all stakeholders benefit from digital advancements.

Finally, embedding CDR into core business strategies is crucial for long-term sustainability. The government, industry, and regulators should collaborate to promote best practices, provide training, and increase public awareness of CDR to drive digital responsibility across the tourism sector.

Discussion

5.1 Discussion of Finding

Based on the five application areas of CDR (Angermann, 2023) — this study evaluates the practices of 30 travel companies in New Zealand in terms of privacy, regulations, and guidance. The study finds that New Zealand travel agencies perform differently in implementing CDR principles, with significant gaps overall.

In terms of digital stewardship, some travel agencies demonstrated good practices in responsible data use and security measures. For example, Travel Agency 11 showed a commitment to data minimisation by limiting data collection, establishing regular deletion policies, and complying with statutory retention periods. However, most travel agencies lacked a clear privacy officer role, resulting in inconsistent data stewardship policies and weakening customer trust. Only 13% of travel agencies explicitly mentioned a privacy officer in their privacy policies, highlighting the industry's shortcomings in digital stewardship.

Regarding digital transparency, 50 per cent of the travel agents in the sample had a privacy policy indicated on their web pages. Some travel agencies improved transparency by providing precise data collection purposes and detailed security measures. For instance, Travel Agencies 10 and 23 clearly stated the purpose and use of data collection, while Travel Agencies 11 and 22 provided information on security practices such as encryption and strong password policies. However, the privacy

policies of many agencies are complex and lengthy, lacking clear explanations of data usage and risks. This complexity makes it difficult for users to understand, undermining the basic principle of "informed consent".

In terms of digital empowerment, some travel agencies enhanced customer capabilities by offering user control and clear communication channels. For example, Travel Agency 25 provides marketing email unsubscribing options and data viewing methods, while Travel Agency 22 has established a privacy officer and provided multi-regional contact information, reflecting its high attention to customer privacy issues. However, most travel agencies fail to empower customers effectively with adequate privacy protection options. There is a lack of clear explanations about user rights and legal remedies.

The study found that travel agencies performed poorly in fairly distributing data usage profits and preventing information abuse in digital equality. Although some agencies, such as Travel Agencies 4 and 10, performed well by mentioning information sharing within the group and disclosure during business changes in their privacy policies, New Zealand travel agencies lack a clear commitment to the fair distribution of data usage profits and do not fully explain how to prevent the abuse of customer information. In digital inclusion, only a few New Zealand travel agents referenced in their privacy policies whether their datasets are used for research and how they ensure inclusive data practices. New Zealand travel agencies should actively improve digital

inclusion and openly and mutually learn from each other's best practices. Therefore, it helps in improving CDR practices.

In addition to the practice of travel agents in New Zealand, another finding is a disconnect between legal compliance requirements and CDR's practical application. Organisations often have privacy policies or terms and conditions on their websites that align with legal requirements. However, because privacy acts are generic and not tailored to an organisation's needs, policies may lack the detail needed to address each organisation's unique situation. Policies are vital tools that communicate how an organisation collects, stores, uses and shares customer data. However, the Privacy Act does not regulate how privacy clauses should be written. As a result, most travel agents refer to the most common privacy policies rather than incorporating their business model. The result is that policies often lack comprehensibility in many New Zealand travel agencies. Many privacy policies are written in complex legal language that may be difficult for the average consumer to understand. Poor comprehensibility of complex privacy policies, consistent with legal language, is especially common for individuals without a law or privacy regulations background. This lack of readability can undermine the effectiveness of privacy policies and prevent customers from making informed decisions about their data. Additionally, some travel agents provide lengthy, dense privacy policies that prevent customers from having the time or inclination to read all the details. As a result, many customers may skip reading the policy and agree to the terms, unknowingly accepting terms that expose their data to risk.

In conclusion, there are significant gaps in the implementation of CDR principles by New Zealand travel agencies, particularly in terms of digital equity and digital inclusion. While some agencies have demonstrated good practices in digital stewardship and digital transparency, the entire industry needs to simplify the language of privacy policies, enhance user rights to know, establish privacy officer roles, and clarify the distribution of profits from data use. These improvements are essential to comprehensively enhancing customer trust and industry compliance.

5.2 Research questions

Research questions 1: How are privacy practices and data management strategies implemented by tourism agencies in New Zealand to align with CDR principles?

This research question seeks to understand how the New Zealand tourism industry is developing its digital practices to meet modern expectations of privacy and responsibility. To achieve sustainable development and digital transformation within the New Zealand tourism industry, it is crucial to incorporate CDR principles such as transparency, fairness, customer empowerment, and legal compliance.

The research findings indicate that privacy practices among New Zealand tourism agencies lack consistency and standardisation. While 50% of the sampled agencies provide a privacy policy on their websites, the quality of these policies varies significantly. For example, Agency 23 demonstrates good practice with a simple and

clear privacy policy, while Agency 22 categorises the content of its privacy policy, enabling users to quickly access relevant sections. However, many privacy policies are lengthy and complex, making it difficult for customers to fully comprehend their rights and how their data is handled. This lack of readability contradicts the CDR principle of transparency, as merely having a privacy policy does not guarantee that users are adequately informed. Furthermore, informed consent practices are weak, as many agencies do not explicitly seek user permission before collecting and processing their data. Instead, consent is often assumed through passive acceptance, such as continued website use. This undermines the CDR principles of digital empowerment and equity, as users may not be aware of the extent of data collection and its implications. These limitations in transparency and empowerment indicate a failure to translate legal compliance into meaningful consumer empowerment. As a result, privacy policies often function as one-way legal statements rather than interactive tools. Privacy policies should facilitate user understanding through clear explanations and interactive elements; however, most agencies in this study fail to implement these practices.

The lack of data governance is evident in the fact that only 13% of the sampled agencies have designated a privacy officer, highlighting a significant gap in accountability. The absence of a privacy officer often results in inconsistent data management practices, as there is no dedicated individual responsible for overseeing compliance, risk management, and ethical data handling. Additionally, only 10 agencies mention data management practices in their privacy policies, with a focus on

protecting personal information from loss, misuse, and unauthorised access. Another critical issue is the lack of emphasis on fairness and inclusivity in data management strategies. Very few tourism agencies actively consider how customer data is used to promote digital fairness or prevent algorithmic bias. For example, agencies rarely disclose how the financial benefits derived from customer data are distributed, which may raise concerns about the ethical use of personal information.

These findings highlight the significant challenges faced by the New Zealand tourism industry in complying with CDR principles. While there are some good practices, many organisations fail to give customers control over their data through accessible policies and consent processes. Closing these gaps is critical to fostering customer trust and achieving sustainable digital transformation.

Research questions 2: What are the key challenges faced by tourism organisations in New Zealand in achieving compliance with privacy legislation and integrating ethical digital practices into their operations?

Tourism organisations in New Zealand exhibit varying levels of compliance with the Privacy Act 2020, which requires transparent and accountable management of personal data. A lack of legal awareness and expertise has prevented many organisations from developing comprehensive data management strategies that meet legal standards, as evidenced by the fact that very few have appointed dedicated privacy officers to oversee compliance. The absence of a consistent framework for digital

practices in the New Zealand tourism industry further complicates matters, as organisations must interpret and apply privacy laws independently, leading to inconsistencies across the sector (Lobschat et al., 2021). A key issue is digital transparency, demonstrated by the differences in how organisations disclose the collection, use, sharing, and storage of data.

Implementing advanced security measures to protect personal data from disclosure or misuse is another critical area for improvement, especially for small and medium-sized enterprises (SMEs), which may face resource constraints (Merwe & Achkar, 2022). Limited budgets and the high cost of legal advice and staff training make it difficult for SMEs to implement effective CDR practices. Additionally, obtaining informed customer consent remains challenging, as consent processes are often buried in terms and conditions or complex privacy policies. These policies are lengthy, complex, and difficult for users to understand (Jensen & Potts, 2004). Furthermore, few organisations provide customers with the tools to manage their personal data, limiting user control and authorisation.

These challenges reflect resource constraints, technological gaps, and a lack of awareness of legal and ethical obligations within New Zealand tourism organisations. Addressing these issues will require government support, industry cooperation, and investment in education and technology to ensure compliance with privacy legislation and adherence to CDR principles.

5.3 Theoretical implications

This study analyses the implementation of CDR in the New Zealand tourism industry, focusing on its practical execution. Previous studies have explored CDR from both a conceptual and cross-industry perspective (Angermann, 2023; Lobschat et al., 2021), but this study provides insights into how travel agents are responding to digital responsibility, particularly regarding privacy, transparency, and governance. From a theoretical standpoint, Angermann (2023) outlines four key elements for effective CDR implementation: integrating CDR into the core strategy, exceeding regulatory compliance, providing clear guidance and governance, and engaging all stakeholders. However, New Zealand tourism organisations demonstrate inconsistency in applying these principles.

Among these travel agencies, the integration of CDR into business strategy remains limited. As Lobschat et al. (2021) argue, adopting CDR requires organisations to align digital responsibility with their long-term business vision, embedding ethical digital practices across all levels. While some agencies comply with the New Zealand Privacy Act 2020 by maintaining basic privacy practices, few have incorporated CDR as a central component of their digital transformation strategies.

The principle of exceeding compliance stresses that CDR should surpass minimum regulatory standards (Merwe & Achkar, 2022). Agencies should proactively ensure ethical data practices, promote digital equity, and strengthen cybersecurity measures. However, the findings suggest that many New Zealand travel agents view CDR as an

external obligation rather than an internal strategic priority. Most of the agents in the sample only meet the minimum legal requirements. This passive approach to integrating CDR into business strategy undermines the potential benefits of CDR, such as the ability to respond to emerging threats and capitalise on opportunities presented by digital technologies (Wynn & Jones, 2023).

The absence of a dedicated CDR governance structure further exacerbates the challenges facing the tourism industry. Effective CDR implementation requires a clear governance model (Lobschat et al., 2021), which should include the appointment of a privacy officer or a dedicated digital management department. The study revealed that while the New Zealand Privacy Act 2020 mandates organisations to appoint a privacy officer, only 13% of travel agents explicitly reported having a privacy officer or a designated CDR team. This highlights a significant gap between regulatory requirements and actual implementation. Additionally, while the New Zealand government promotes principles such as Privacy by Design (PbD), the adoption of this principle remains inconsistent within the New Zealand tourism sector, indicating a need for greater awareness of PbD practices.

Moreover, the scope of CDR remains limited in its comprehensiveness across all stakeholders. The study found little evidence of New Zealand travel agents cooperating with key stakeholders, such as employees, business partners, and regulators. This impacts broader ethical responsibilities, such as promoting employee awareness of digital responsibility, ensuring fair digital practices, responsibly sharing data, and

adhering to broader industry regulations (Basu et al., 2024). Although the study relied on secondary data, which limits deeper insights into internal operational practices, reviewing the privacy policies and terms and conditions of New Zealand travel agents reveals that the existing CDR framework has not been fully adopted. Travel agencies must incorporate CDR into their digital practices to gain a distinct advantage in terms of brand reputation and stakeholder trust and loyalty (Basu et al., 2024).e

5.4 Practical implications

This study provides several practical implications for travel agencies, public administrations, and policymakers to address the challenges of digital transformation. The study found that New Zealand tourism organisations exhibit varying levels of engagement across the five key areas of CDR: digital stewardship, digital transparency, digital empowerment, digital equity, and digital inclusion. Addressing these areas requires action from various stakeholders to ensure that business practices align with the theoretical framework.

Recommendations for New Zealand Travel Agencies

As shown in figure 8, New Zealand travel agents can refer to the CDR framework presented in this paper to implement corporate digital responsibility step by step. First, New Zealand travel agents must prioritise compliance with the Privacy Act 2020. In particular, organisations without a privacy policy listed on their website should address

this as an urgent matter. Furthermore, they should establish the position of privacy officer to ensure that privacy policies and data management practices comply with the law. To achieve this, travel agents should develop and implement an internal digital policy to integrate data management and privacy protection into their daily operations. Appointing a privacy officer can further support the effective implementation and monitoring of these policies.

To ensure long-term sustainability, travel agents must integrate CDR into their core business strategy. Enhance transparency by implementing CDR, and travel agents should clearly communicate how customer data is collected, used, and shared. This can be achieved by updating privacy policies and terms and conditions on their websites, ensuring that these policies are comprehensive, accessible, and easy to understand. In addition, travel agents should enhance digital empowerment by providing customers with the tools and resources needed to manage their data effectively. This includes policy update alerts, options to correct personal information, data deletion requests, and explicit consent mechanisms, enabling clients to have better control over their personal information. Digital equity should also be a priority, and travel organisations can adopt the principle of data minimisation, collecting only the necessary information. They should also adopt data security technologies (e.g., encryption, anonymisation) to protect customer data from misuse or leakage. Moreover, collaborating with industry partners to promote digital inclusion will ensure that all stakeholders, including smaller travel agencies, benefit from digital advancements. Larger organisations should

consider knowledge-sharing programmes to help smaller businesses improve their digital responsibility practices.

Although the implementation of CDR still faces challenges, such as limited awareness and support for CDR, travel agents can work closely with government agencies and other organisations to gain knowledge or technical support. Finally, and most importantly, travel agents should conduct internal training to increase staff understanding and acceptance of CDR. By incorporating best CDR practices within the organisation and stating them clearly in terms and conditions or privacy policies, travel agents can increase customer trust and encourage active participation from all stakeholders in the implementation of CDR. This will help strengthen the digital responsibility of the entire travel industry.

Recommendations to the New Zealand Government

The government should strengthen the regulatory framework by introducing more detailed regulations to enhance user privacy protection. The government could implement standardised privacy policies and mandatory transparency measures across the travel industry to ensure consistency. Additionally, the government could provide targeted support to small travel agencies and others that lack resources. For example, many travel agencies lack the financial and technical resources to fully implement CDR. Such support could include funding opportunities, training programmes, and organising digital inclusion exchanges to help small businesses comply with CDR standards.

Furthermore, the government can adopt best practices from the travel industry to develop guidelines for implementing CDR standards. By establishing clear standards, a unified approach to digital responsibility can be adopted across the travel industry. Recognising and rewarding businesses that demonstrate strong CDR practices will further motivate organisations to engage actively in responsible digital management.

Recommendations for Consumers

Consumers also have a key role to play in promoting ethical digital practices in the tourism industry. However, this requires additional effort, complexity, and inconvenience on the part of the consumer. Consumers can minimise digital interactions by providing less personal information, such as the use of pseudonyms, dates of birth, and profile pictures, thereby limiting activities that may disclose personal information. Consumers can manage their digital activity by verifying a company's privacy policy. They can also limit access to information by adjusting privacy settings, such as changing cookie settings. By raising awareness of digital security and privacy rights, customers can make better choices and hold travel agents accountable for their digital practices. Supporting businesses that prioritise ethical data management and transparency will encourage wider adoption of CDR principles across the industry. By making informed decisions, consumers can create a more responsible and sustainable digital environment within the travel industry.

5.5 Limitations and recommendations for future research

This study has made significant progress in exploring the CDR practices of travel agents in New Zealand; however, several limitations should be acknowledged. The primary limitation is the reliance on secondary data. This study utilised information obtained from travel organisation websites. However, the data presented on these websites may not fully reflect the actual digital responsibility practices within the organisations. For example, some travel organisations may have more detailed internal policies that are not publicly available, such as security and protection measures for data storage. Additionally, secondary data may be outdated, as updates are often delayed, meaning that the research findings could be time-sensitive and may not reflect the latest practices of tourism organisations. Future research could address these limitations by incorporating primary data collection methods, such as interviews or surveys with key stakeholders, to obtain deeper and more comprehensive insights.

Secondly, the limited sample size impacts the generalisability of the study's findings. This study only covered 30 travel agents in New Zealand, which is a relatively small sample compared to the size of the country's extensive tourism market. CDR practices may vary significantly between travel agencies of different sizes, business models, and market positions. For instance, a small travel agency may have limited resources and may be under-invested or understaffed in data protection technologies, while a larger agency may have a more sophisticated CDR system in place. Therefore, the sample may not fully represent the CDR practices of the entire New Zealand travel

industry. In future research, the sample size should be expanded to include a broader range of travel agencies with different characteristics. Additionally, expanding the scope of the study to include tourism organisations from other countries and regions could facilitate a comparative analysis of CDR practices.

Furthermore, CDR is still an emerging concept, with insufficient literature and mature frameworks available in both academic and practical fields. While the importance of digital responsibility is increasingly recognised, significant gaps remain in standardised practices and guidelines for CDR across industries. The relative newness of CDR means there are few comprehensive models or definitions to guide cross-industry implementation. As a result, many organisations may adopt temporary or inconsistent approaches to digital responsibility, leading to gaps in CDR implementation. To address these gaps, future research should focus on developing comprehensive theoretical frameworks for CDR that can be applied across various industries.

5.6 Conclusion

As society evolves, the tourism industry is increasingly embracing digitalisation. However, with the rise of cybersecurity challenges and other associated risks, the concept of CDR has emerged and is gradually gaining significance. This study highlights the varying levels of engagement with CDR principles among New Zealand

tourism organisations. While these organisations are generally compliant with the New Zealand Privacy Act 2020 and have made progress in areas such as digital stewardship and transparency, significant gaps remain. Many organisations fail to adopt a proactive and comprehensive approach to CDR, resulting in inconsistencies in the implementation of digital empowerment, equity, and inclusion.

Key challenges include limited transparency in privacy practices, a lack of customer empowerment, and resource constraints that hinder New Zealand travel agents from developing comprehensive and inclusive digital strategies. A major issue is the absence of clear industry standards, which leads to organisations interpreting and implementing CDR principles in varied ways. To address these gaps, a collaborative approach is essential. Governments should introduce stricter regulations and procedures while providing targeted support to smaller operators. Larger travel organisations should integrate CDR into their core strategies, striving to go beyond mere compliance by promoting data-inclusive practices. Customers can also play a role by advocating for greater awareness of data security and supporting organisations that adhere to stringent ethical standards.

References

- Afaq, A., & Gaur, L. (2021). The Rise of Robots to Help Combat Covid-19. *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 69–74. <https://doi.org/10.1109/ICTAI53825.2021.9673256>
- Akter, S., & Wamba, S. F. (2016). Big data analytics in E-commerce: A systematic review and agenda for future research. *Electronic Markets*, 26(2), 173–194. <https://doi.org/10.1007/s12525-016-0219-0>
- Angermann. (2023). *The Challenge of Corporate Digital Responsibility – An Analysis of Key Elements for CDR Implementation*.
- Anshari, M., Almunawar, M. N., Lim, S. A., & Al-Mudimigh, A. (2019). Customer relationship management and big data enabled: Personalization & customization of services. *Applied Computing and Informatics*, 15(2), 94–101. <https://doi.org/10.1016/j.aci.2018.05.004>
- Basu, S., Jha, S., Ooi, K.-B., & Cham, T.-H. (2024). Unveiling the Potential of Corporate Digital Responsibility (CDR). *Journal of Computer Information Systems*, 0(0), 1–33. <https://doi.org/10.1080/08874417.2024.2445745>
- Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(2), 359–374. <https://doi.org/10.1108/JFC-07-2020-0149>
- Bell, C. (2008). 100% PURE New Zealand: Branding for back-packers. *Journal of Vacation Marketing*, 14(4), 345–355. <https://doi.org/10.1177/1356766708094755>
- Borràs, J., Moreno, A., & Valls, A. (2014). Intelligent tourism recommender systems: A survey. *Expert Systems with Applications*, 41(16), 7370–7389. <https://doi.org/10.1016/j.eswa.2014.06.007>
- Bowen, J., & Whalen, E. (2017). Trends that are changing travel and tourism. *Worldwide Hospitality and Tourism Themes*, 9(6), 592–602. <https://doi.org/10.1108/WHATT-09-2017-0045>
- Buhalis, D., & O'Connor, P. (2005). Information Communication Technology Revolutionizing Tourism. *Tourism Recreation Research*, 30(3), 7–16. <https://doi.org/10.1080/02508281.2005.11081482>
- Bygrave, L. A. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian Studies In Law*.
- Campbell, H., Malahoff, A., Browne, G., Graham, I., & Sutherland, R. (2012). New Zealand Geology. *Episodes*, 35(1), Article 1.
- Carl, K. V., Zilcher, T. M. C., & Hinz, O. (2022). *Corporate Digital Responsibility and the current Corporate Social Responsibility standard: An analysis of applicability*. 75–86. <https://dl.gi.de/handle/20.500.12116/38706>
- Cater, C. (2006). *World Adventure Capital*.

- Chambers, E. (2009). From authenticity to significance: Tourism on the frontier of culture and place. *Futures*, *41*(6), 353–359.
<https://doi.org/10.1016/j.futures.2008.11.003>
- Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access*, *8*, 90225–90265.
 IEEE Access. <https://doi.org/10.1109/ACCESS.2020.2992341>
- Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445–459. <https://doi.org/10.1016/j.giq.2018.04.002>
- Christchurch International Airport. (n.d.). *Artificial Intelligence—Christchurch Airport*. Retrieved 8 August 2024, from <https://www.christchurchairport.co.nz/about-us/innovation/artificial-intelligence/>
- Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157–170.
<https://doi.org/10.1016/j.tele.2017.01.008>
- Cloke, P., & Perkins, H. C. (2002). Commodification and Adventure in New Zealand Tourism. *Current Issues in Tourism*, *5*(6), 521–549.
<https://doi.org/10.1080/13683500208667939>
- Culnan, M. J. (1993). 'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, *17*(3), 341–363. <https://doi.org/10.2307/249775>
- Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*(2), 323–342.
<https://doi.org/10.1111/1540-4560.00067>
- Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, *23*(3), Article 3. <https://doi.org/10.3390/s23031151>
- Dyshkantiuk, O., Salamatina, S., Polishchuk, L., Komarnytskyi, I., Tserklevych, V., & Nedobiichuk, T. (2020). *Modern Hotel Business Management Tools* (SSRN Scholarly Paper 3645056). <https://papers.ssrn.com/abstract=3645056>
- Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K., & van Moorsel, A. (2021). Towards an Equitable Digital Society: Artificial Intelligence (AI) and Corporate Digital Responsibility (CDR). *Society*, *58*(3), 179–188.
<https://doi.org/10.1007/s12115-021-00594-8>
- Fiero, A. W., & Beier, E. (2022). New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation. *Stanford Journal of International Law*, *58*(2), 151–192.

- Florek, M., & Insch, A. (2008). The trademark protection of country brands: Insights from New Zealand. *Journal of Place Management and Development*, 1(3), 292–306. <https://doi.org/10.1108/17538330810911271>
- Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business & Society*, 58(1), 3–19. <https://doi.org/10.1177/0007650317727540>
- Foroudi, P., Gupta, S., Sivarajah, U., & Broderick, A. (2018). Investigating the effects of smart technology on customer dynamics and customer experience. *Computers in Human Behavior*, 80, 271–282. <https://doi.org/10.1016/j.chb.2017.11.014>
- Garkavenko, V. (2007). *New Zealand travel agents in the internet era: Impacts, responses, and relationships* [Auckland University of Technology]. <https://hdl.handle.net/10292/328>
- Gauld, R. (2022). A review of public policies on Covid-19: The New Zealand experience. *Public Administration and Policy*, 26(1), 10–20. <https://doi.org/10.1108/PAP-04-2022-0028>
- Gössling, S. (2020). Technology, ICT and tourism: From big data to the big picture. *Journal of Sustainable Tourism*, 29(5), 849–858. <https://doi.org/10.1080/09669582.2020.1865387>
- Gössling, S., Scott, D., & Hall, C. M. (2020). Pandemics, tourism and global change: A rapid assessment of COVID-19. *Journal of Sustainable Tourism*, 29(1), 1–20. <https://doi.org/10.1080/09669582.2020.1758708>
- Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783–812. [https://doi.org/10.1016/S1071-5819\(03\)00043-0](https://doi.org/10.1016/S1071-5819(03)00043-0)
- Guest, G., M. MacQueen, K., & E. Namey, E. (2012). *Applied Thematic Analysis*. SAGE Publications, Inc. <https://doi.org/10.4135/9781483384436>
- Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., Griffiths, C., Gupta, S., Kamani, S. R., Kiratli, Y.-S., Kispataki, M., Lange, G., Moles de Matos, L., Tripero Moreno, L., Betancourt Nunez, H. A., Pilla, V., Raj, B., Roe, J., Skoda, M., ... Edinger-Schons, L. M. (2021). “Corporate Digital Responsibility”. *Sustainability Management Forum | NachhaltigkeitsManagementForum*, 29(1), 13–29. <https://doi.org/10.1007/s00550-020-00509-x>
- Hooper, T., & Vos, M. (2009). Establishing business integrity in an online environment. *Online Information Review*, 33(2), 343–361. <https://doi.org/10.1108/14684520910951258>
- InternetNZ. (n.d.). *Nz Rules*. Retrieved 3 October 2024, from <https://internetnz.nz/nz-domains/nz-policies/nz-rules-2023/>

- Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy*, 28(3), 259–275.
<https://doi.org/10.1111/1467-9973.00055>
- Ivanov S. H., & Webster C. (2017). *Adoption of Robots, Artificial Intelligence and Service Automation by Travel, Tourism and Hospitality Companies – A Cost-Benefit Analysis* (SSRN Scholarly Paper 3007577).
<https://papers.ssrn.com/abstract=3007577>
- Jaforullah, M. (2015). International Tourism and Economic Growth in New Zealand. *Tourism Analysis*, 20(4), 413–418.
<https://doi.org/10.3727/108354215X14400815080523>
- Jensen, C., & Potts, C. (2004). *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*. 6(1).
- Jessica Hwang, L., & Lockwood, A. (2006). Understanding the challenges of implementing best practices in hospitality and tourism SMEs. *Benchmarking: An International Journal*, 13(3), 337–354.
<https://doi.org/10.1108/14635770610668820>
- Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications*, 171, 102807.
<https://doi.org/10.1016/j.jnca.2020.102807>
- Kim, D. J., Kim, W. G., & Han, J. S. (2007). A perceptual mapping of online travel agencies and preference attributes. *Tourism Management*, 28(2), 591–603.
<https://doi.org/10.1016/j.tourman.2006.04.022>
- Kim, J., & Kim, M. (2024). Influences of Ethical Values of e-Travel Agents on Authenticity and Trust Formations: The Moderating Role of Privacy Concerns. *International Journal of Human-Computer Interaction*, 40(20), 6442–6457.
<https://doi.org/10.1080/10447318.2023.2254638>
- Kong, H., Wang, K., Qiu, X., Cheung, C., & 卜乃鹏. (2022). 30 years of artificial intelligence (AI) research relating to the hospitality and tourism industry. *International Journal of Contemporary Hospitality Management*, 35(6), 2157–2177. <https://doi.org/10.1108/IJCHM-03-2022-0354>
- Kovanič, M., & Spáč, S. (2022). Conceptions of Privacy in the Digital Era: Perceptions of Slovak Citizens. *Surveillance & Society*, 20(2), 186–201.
<https://doi.org/10.24908/ss.v20i2.14099>
- Kumar, S., Kumar, V., & Attri, K. (2021). IMPACT OF ARTIFICIAL INTELLIGENCE AND SERVICE ROBOTS IN TOURISM AND HOSPITALITY SECTOR: CURRENT USE & FUTURE TRENDS. *Administrative Development 'A Journal of HIPA, Shimla'*, 8(SI-1), 59–83.
<https://doi.org/10.53338/ADHIPA2021.V08.Si01.04>
- Lacity, M. C., & Janson, M. A. (1994). Understanding Qualitative Data: A Framework of Text Analysis Methods. *Journal of Management Information Systems*, 11(2), 137–155. <https://doi.org/10.1080/07421222.1994.11518043>

- Larasetiati, M., & Ali, H. (2019). *Model of Consumer Trust: Analysis of Perceived Usefulness and Security toward Repurchase Intention in Online Travel Agent*.
- Le, T. N. N., Sylvester, A., & Campbell-Meier, J. (2024). *Towards a Conceptualisation of Corporate Digital Responsibility: Assessing the current literature*.
- Leung, X. Y. (2019). Technology-enabled service evolution in tourism: A perspective article. *Tourism Review*, 75(1), 279–282. <https://doi.org/10.1108/TR-06-2019-0229>
- Li, H., Hu, M., & Li, G. (2020). Forecasting tourism demand with multisource big data. *Annals of Tourism Research*, 83, 102912. <https://doi.org/10.1016/j.annals.2020.102912>
- Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), 1–6. <https://doi.org/10.1080/1097198X.2019.1569186>
- Li, J., Xu, L., Tang, L., Wang, S., & Li, L. (2018). Big data in tourism research: A literature review. *Tourism Management*, 68, 301–323. <https://doi.org/10.1016/j.tourman.2018.03.009>
- Li, K., Jin, M., & Shi, W. (2018). Tourism as an important impetus to promoting economic growth: A critical review. *Tourism Management Perspectives*, 26, 135–142. <https://doi.org/10.1016/j.tmp.2017.10.002>
- Li, M., Yin, D., Qiu, H., & Bai, B. (2021). A systematic review of AI technology-based service encounters: Implications for hospitality and tourism operations. *International Journal of Hospitality Management*, 95, 102930. <https://doi.org/10.1016/j.ijhm.2021.102930>
- Liao, Z., & Shi, X. (2017). Web functionality, web content, information security, and online tourism service continuance. *Journal of Retailing and Consumer Services*, 39, 258–263. <https://doi.org/10.1016/j.jretconser.2017.06.003>
- Liddicoat, J. (2019). A country road: Domain name disputes in .nz—is private dispute resolution working? *International Journal of Law and Information Technology*, 27(4), 409–436. <https://doi.org/10.1093/ijlit/eaz013>
- Lim, W. M. (2024). What Is Qualitative Research? An Overview and Guidelines. *Australasian Marketing Journal*, 14413582241264619. <https://doi.org/10.1177/14413582241264619>
- Liu, P., & Liu, Y. (2016). *Smart Tourism via Smart Phone*. 129–132. <https://doi.org/10.2991/cimns-16.2016.33>
- Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875–888. <https://doi.org/10.1016/j.jbusres.2019.10.006>
- Londoño-Cardozo, J., & Paz, M. P. D. (2021). CORPORATE DIGITAL RESPONSIBILITY: FOUNDATIONS AND CONSIDERATIONS FOR ITS DEVELOPMENT. *RAM. Revista de Administração Mackenzie*, 22, eRAMD210088. <https://doi.org/10.1590/1678-6971/eRAMD210088>

- Madzík, P., Falát, L., Copuš, L., & Valeri, M. (2023). Digital transformation in tourism: Bibliometric literature review based on machine learning approach. *European Journal of Innovation Management*, 26(7), 177–205. <https://doi.org/10.1108/EJIM-09-2022-0531>
- Martin, K., & Murphy, P. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>
- MBIE. (n.d.). *The outlook for New Zealand-Aotearoa tourism*. Retrieved 22 January 2025, from <https://www.mbie.govt.nz/immigration-and-tourism/tourism/tourism-projects/governments-tourism-snapshot/the-outlook-for-new-zealand-aotearoa-tourism>.
- MBIE. (2017). *Business Information and Communication Technology (ICT) use and productivity growth in New Zealand*.
- McIntosh, A. J. (2004). Tourists' appreciation of Maori culture in New Zealand. *Tourism Management*, 25(1), 1–15. [https://doi.org/10.1016/S0261-5177\(03\)00058-X](https://doi.org/10.1016/S0261-5177(03)00058-X)
- Merwe, J. van der, & Achkar, Z. A. (2022). Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data & Policy*, 4, e12. <https://doi.org/10.1017/dap.2022.2>
- Morgan, D. L. (2014). Pragmatism as a Paradigm for Social Research. *Qualitative Inquiry*, 20(8), 1045–1053. <https://doi.org/10.1177/1077800413513733>
- Munasinghe, S., Powell, L., Herath, H. M., & Frey, R. A. (2022). Lessons for resilience building in tourism and hospitality: The case of New Zealand. *Worldwide Hospitality and Tourism Themes*, 14(6), 604–609. <https://doi.org/10.1108/WHATT-05-2022-0055>
- Nassaji, H. (2020). Good qualitative research. *Language Teaching Research*, 24(4), 427–431. <https://doi.org/10.1177/1362168820941288>
- Navío-Marco, J., Ruiz-Gómez, L. M., & Sevilla-Sevilla, C. (2018). Progress in information technology and tourism management: 30 years on and 20 years after the internet - Revisiting Buhalis & Law's landmark study about eTourism. *Tourism Management*, 69, 460–470. <https://doi.org/10.1016/j.tourman.2018.06.002>
- New Zealand Digital government. (2024, August 14). *Privacy by Design (PbD)*. New Zealand Digital Government. <https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/>
- New Zealand Government. (2020, August 26). *Consumer laws*. New Zealand Government. <https://www.govt.nz/browse/consumer-rights-and-complaints/consumer-laws/>
- No, E., & Kim, J. K. (2015). Comparing the attributes of online tourism information sources. *Computers in Human Behavior*, 50, 564–575. <https://doi.org/10.1016/j.chb.2015.02.063>

- NZ Herald. (2024, April 11). *Room service robots: Why Sudima Hotels wants to expand its fleet*. <https://www.nzherald.co.nz/business/room-service-robots-why-sudima-hotels-wants-to-expand-its-fleet/LFTQA5D4DRBTJAG5YLTBGHTLH4/>
- Pelters, E. (2021). Corporate Digital Responsibility—Understanding and Applying. In T. A. Herberger & J. J. Dötsch (Eds.), *Digitalization, Digital Transformation and Sustainability in the Global Economy* (pp. 71–84). Springer International Publishing. https://doi.org/10.1007/978-3-030-77340-3_6
- Pencarelli, T. (2020). The digital revolution in the travel and tourism industry. *Information Technology & Tourism*, 22(3), 455–476. <https://doi.org/10.1007/s40558-019-00160-3>
- Perić, M., & Vitezić, V. (2021). Tourism Getting Back to Life after COVID-19: Can Artificial Intelligence Help? *Societies*, 11(4), Article 4. <https://doi.org/10.3390/soc11040115>
- Privacy Act 2020. (Ministry of Justice). *Privacy Act 2020*. <https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html>
- Privacy Commissioner. (n.d.). *Office of the Privacy Commissioner | Your privacy responsibilities*. Retrieved 22 August 2024, from <https://www.privacy.org.nz/responsibilities/your-obligations/>
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>
- Ratner, C. (2002). Subjectivity and Objectivity in Qualitative Methodology. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 3(3), Article 3. <https://doi.org/10.17169/fqs-3.3.829>
- Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer law & security review*, 34(1), 99-110.
- Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, 25(4), Article 4.
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, 23(15), Article 15. <https://doi.org/10.3390/s23156666>
- Shi, S., Gong, Y., & Gursoy, D. (2021). Antecedents of Trust and Adoption Intention toward Artificially Intelligent Recommendation Systems in Travel Planning: A Heuristic–Systematic Model. *Journal of Travel Research*, 60(8), 1714–1734. <https://doi.org/10.1177/0047287520966395>
- Simmons, D. G. (2013). *Tourism and ecosystem services in New Zealand*. Manaaki Whenua Press. <https://hdl.handle.net/10182/6848>

- SkyCity Auckland. (n.d.). *Andy's Burgers & Bar*. SkyCity Auckland. Retrieved 8 August 2024, from <https://skycityauckland.co.nz/restaurants/andys-burgers-bar/>
- Smith, K., & Schott, C. (2004). *2004 New Zealand Tourism and Hospitality Research Conference Proceedings 2004 - Tourism Research: Advances and Applications*.
- Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1156.
- Someh, I., Davern, M., Breidbach, C., & Shanks, G. (2019). Ethical Issues in Big Data Analytics: A Stakeholder Perspective. *Communications of the Association for Information Systems*, *44*(1). <https://doi.org/10.17705/1CAIS.04434>
- Stanford, D. (2008). 'Exceptional Visitors': Dimensions of Tourist Responsibility in the Context of New Zealand. *Journal of Sustainable Tourism*, *16*(3), 258–275. <https://doi.org/10.1080/09669580802154082>
- Stats NZ. (2019). *Tourism satellite account: 2019*.
- Stats NZ. (2020, April 17). *Business R&D expenditure doubles between 2012 and 2019*. <https://secure.livechatinc.com/>
- Stats NZ. (2024, May 24). *Information and communication technology supply survey: 2023*. <https://secure.livechatinc.com/>
- Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, *55*, 992–1000. <https://doi.org/10.1016/j.chb.2015.09.038>
- Stylos, N., Zwiendelaar, J., & Buhalis, D. (2021). Big data empowered agility for dynamic, volatile, and time-sensitive service industries: The case of tourism sector. *International Journal of Contemporary Hospitality Management*, *33*(3), 1015–1036. <https://doi.org/10.1108/IJCHM-07-2020-0644>
- Tourism New Zealand. (n.d.). *Tourism New Zealand is responsible for promoting New Zealand in key markets as a visitor destination*. What We Do. Retrieved 21 August 2024, from <https://www.tourismnewzealand.com/about-us/what-we-do/>
- Tourism New Zealand. (n.d.). *Find Travel agencies | 100% Pure New Zealand*. Retrieved 21 August 2024, from <https://www.newzealand.com/nz/products/travel-agency/>
- Tourism New Zealand. (2024). *Markets overview*. <https://www.tourismnewzealand.com/about-us/markets-overview/>
- van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems*, *12*(1), 41–48. <https://doi.org/10.1057/palgrave.ejis.3000445>
- Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), 63–70. <https://doi.org/10.1145/272287.272299>
- Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. <https://doi.org/10.1016/j.lrp.2018.12.001>

- Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate Digital Responsibility in Service Firms and Their Ecosystems. *Journal of Service Research*, 26(2), 173–190. <https://doi.org/10.1177/10946705221130467>
- Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889–897. <https://doi.org/10.1016/j.chb.2011.12.008>
- Wynn, M., & Jones, P. (2023). Corporate Responsibility in the Digital Era. *Information*, 14(6), Article 6. <https://doi.org/10.3390/info14060324>
- Xiang, Z., Magnini, V. P., & Fesenmaier, D. R. (2015). Information technology and consumer behavior in travel and tourism: Insights from travel planning using the internet. *Journal of Retailing and Consumer Services*, 22, 244–249. <https://doi.org/10.1016/j.jretconser.2014.08.005>
- Yallop, A. C., Gică, O. A., Moisescu, O. I., Coroş, M. M., & Séraphin, H. (2021). The digital traveller: Implications for data ethics and data governance in tourism and hospitality. *Journal of Consumer Marketing*, 40(2), 155–170. <https://doi.org/10.1108/JCM-12-2020-4278>
- Zeng, Z., Chen, P.-J., & Lew, A. A. (2020). From high-touch to high-tech: COVID-19 drives robotics adoption. *Tourism Geographies*, 22(3), 724–734. <https://doi.org/10.1080/14616688.2020.1762118>
- Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742. <https://doi.org/10.1002/sec.795>