Data Privacy as a Business Opportunity: Leveraging Privacy Maximizing Features to Address Client Privacy Concerns

Luis Fastje

Dissertation written under the supervision of Professor Peter V. Rajsingh Ph. D

Dissertation submitted in partial fulfilment of requirements for the MSc in Master of Science in Management with Specialization in Strategy, Entrepreneurship & Impact, at the Universidade Católica Portuguesa, 2023.

Abstract

Data privacy is a critical concern in the era of data-driven businesses. Users are becoming increasingly sensitive about the collection and processing of their personal data. This Master's thesis examines whether a firm's data privacy policy can provide an edge over competitors.

Primary research was conducted to ascertain user preferences and behavior regarding data privacy in the context of identified business drivers for prioritizing data privacy as well as for mitigating associated risks and benefits. This data supplemented secondary material from the literature review. PESTEL analysis indicated that key drivers for data privacy are legal, ethical, financial, and technical. Moreover, expert interviews and the survey revealed that businesses cannot avoid data privacy and proved the above-mentioned key drivers. Furthermore, the drivers can be structured for transparency, trust, capabilities, and holistic processes. Data privacy must be approached holistically as data governance to ensure efficient and responsible data management within an organization. Hence, a concept was developed which proactively leverages user concerns and minimizes the consequences of data breaches and non-compliance with the GDPR.

Based on the foregoing, privacy policies can lead to unique positioning and consequently provide a competitive advantage (CA) with the following measures: (1) explicit opt-in choices on a consent management platform, (2) efficient Data Lifecycle Management, (3) are in the context of privacy by design, and (4) represent technical best practices, such as differential privacy. These criteria, properly executed with consideration to company-specific use cases and the internal resources and capabilities, leverage privacy maximizing features for CA.

Key Words: Competitive Advantage**,** Data Privacy, GDPR, Data Governance, Data Governance Maturity Model, Data Lifecycle Management, User Trust.

Title: Data Privacy as a Business Opportunity: Leveraging Privacy Maximizing Features to Address Client Privacy Concerns

Author: Luis Fastje

Resumo

A privacidade dos dados é uma preocupação crítica na era das empresas orientadas pelos dados. Os utilizadores estão a tornar-se cada vez mais sensíveis quanto à recolha dos seus dados pessoais. Esta tese de mestrado examina se a política de privacidade de dados de uma empresa pode proporcionar uma vantagem sobre a concorrência.

Foi realizada uma pesquisa primária para determinar as preferências e o comportamento dos utilizadores relativamente à privacidade dos dados no contexto dos impulsionadores empresariais identificados para dar prioridade à privacidade dos dados. Estes dados complementaram o material secundário da revisão bibliográfica. A análise PESTEL indicou que os principais motores da privacidade de dados são legais, éticos, financeiros, e técnicos, comprovados por entrevistas e inquéritos. Além disso, os condutores podem ser estruturados para transparência, confiança, capacidades, e processos holísticos. A privacidade dos dados deve ser abordada holisticamente como governação dos dados para assegurar uma gestão eficiente dos dados dentro de uma organização. Foi desenvolvido um conceito que mostra que as políticas de privacidade podem conduzir a um posicionamento único e, consequentemente, proporcionar uma vantagem competitiva com as seguintes medidas:(1) escolhas explícitas de opt-in sobre uma plataforma de gestão de consentimento, (2) gestão eficiente do ciclo de vida dos dados, (3) estão no contexto da privacidade por conceção, e (4) representam as melhores práticas técnicas, tais como a privacidade diferencial. Estes critérios, devidamente executados tendo em consideração os casos de utilização específicos da empresa e os recursos e capacidades internas, potenciam as características de privacidade para uma vantagem competitiva.

Palavras-chave: Vantagem Competitiva, Privacidade de Dados, GDPR, Governação de Dados, Modelo de Maturidade de Governação de Dados, Gestão do Ciclo de Vida dos Dados, Confiança do Utilizador.

Título: Privacidade de dados como uma oportunidade de negócio: Alavancar a Privacidade Maximizando as Características para Abordar as Preocupações de Privacidade do Cliente

Autor: Luis Fastje

Acknowledgments

The dissertation completes my academic journey at the Católica Lisbon School of Business & Economics. Thanks to supportive, wonderful, and encouraging people I met on this journey, I was able to overcome the academic and personal challenges.

I would like to express my sincere gratitude to my supervisor, Professor Peter V. Rajsingh, for his invaluable guidance, support, and encouragement throughout the course of the competitive advantage seminar. His expertise, feedback, and network helped me to stay focused on the essentials and reach the goal of successfully finishing this thesis.

Moreover, I am grateful for the experts who shared their insights and opened various perspectives on the topic of data privacy as well as every individual who contributed to the survey and shared the link.

Ultimately, I want to thank my family, friends, and partner for their unconditional support. Their encouragement has been a constant source of motivation and inspiration during this time.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ATT	Apple Tracking Transparency
CA	Competitive Advantage
DPO	Data Privacy Officer
DLM	Data Lifecycle Management
GDPR	General Data Protection Regulation
IDFA	Identifier for Advertisers
MBV	Market-based View
PESTEL	Political, Economic, Social, Technological, Ethical, Legal
PET	Privacy-enhanced Technology
PII	Personally Identifiable Information
Privacy UX	Privacy User Experience
RBV	Resource-based view

1. Introduction

The European Union's General Data Protection Regulation (*GDPR*) was introduced in May 2018 to create a uniform data security law for all EU members. Its data protection principles not only promote transparency and consistency across the entire EU, but also data minimization, storage limitation, integrity, and confidentiality as well as accountability of the data controller (Wolford, 2020). Increased demand for privacy regulations has led to various regulations to promote privacy including the California Consumer Privacy Act and the Brazilian General Data Protection Law requiring compliance from organizations (iapp, 2021). The construct of data privacy in society is illustrated in Figure 1 and indicates that data privacy concerns influence purchase intention, which ultimately impacts firms' performances. Firms adjusting through privacy-enhancing factors can improve organizational trust. As a corollary, privacy failures such as data breaches influence both consumer behavior and organizational performance (Martin & Murphy, 2017).

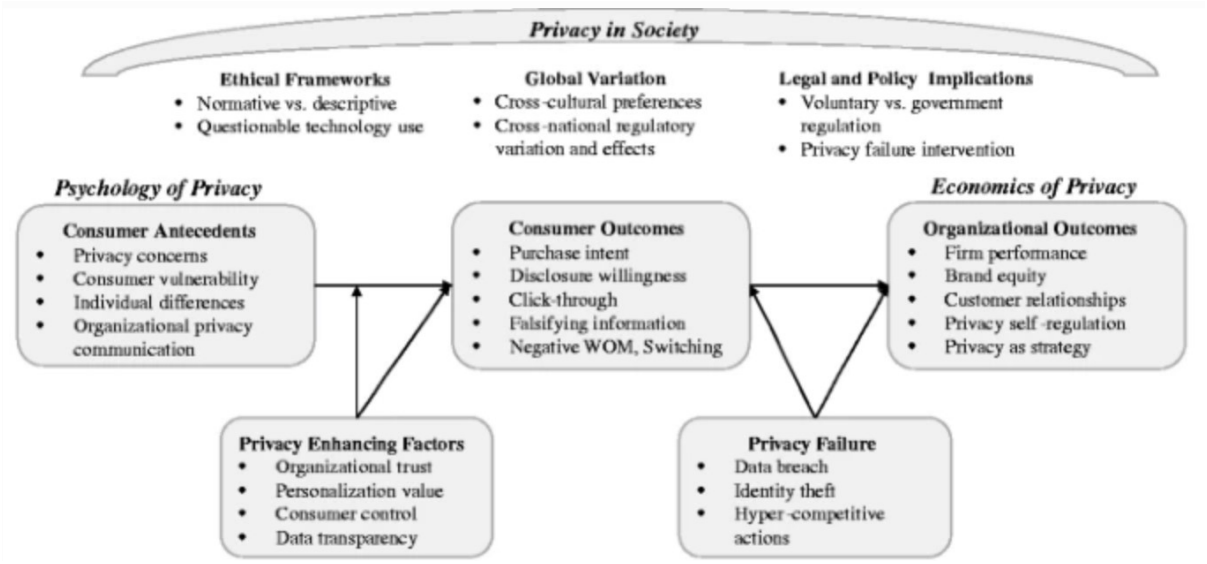

Figure 1: Privacy in Society (Martin & Murphy, 2017)

The introduction of privacy laws has led to an emerging privacy tech sector focused on this growing area. Across the Venture Capital and investment landscape, there has been an increase of approx. 588% in investments in the sector, from $1.7 billion in 2010 to $10 billion in 2019 (iapp, 2021). Data breaches are an increasing threat to companies. Firms seen as leaking sensitive information engender consumer distrust along with the perception of lacking adequate data protection. Due to non-compliance with general data-processing principles or legal parameters for data processing under the GDPR, major companies with well-known

reputations, *inter alia* Amazon, Meta, WhatsApp, and Alphabet, have received fines and penalties in the past ranging from $90 million up to $746 million (CMS Legal, 2022).

Data has become inevitable in almost all sectors – production, sales, marketing, R&D, supply chain, etc. Digital technology is central to society and accessible to most people which implicates firms. Processing and analyzing customer data enables companies to forecast consumer behavior, improving consumer engagement and usability of products. Moreover, personal information offers the opportunity to individualize products for customer needs as well as create targeted advertisements, build more precise customer profiles, and understand consumers' pain points along the customer journey (Acquisti et al., 2016). Consumers are making increasingly conscious decisions about what types of data they share with companies and are significantly more inclined to share technically relevant personal data only. Healthcare and financial services providers are perceived as the most trustworthy for handling consumer personal data (Anant et al., 2020). Security breaches have also spurred increased use of tools that give people more control over their data. Companies are considered to have fiduciary duties for responsible handling and collection of data. As awareness of the importance of data security grows, the way companies deal with consumer data and privacy can become a differentiator and even a source of competitive advantage (CA) (Anant et al., 2020).

> *"We believe privacy is a fundamental human right, and the best technology is one that people can trust. At Apple, we're constantly innovating to give our users more control over how their data is used and the choice with whom to share it."* – Tim Cook, CEO of Apple Inc., Twitter

With over $2.37 trillion in market capitalization, Apple is the most valuable company in the world. It embeds data privacy as a strategic differentiating factor while other companies are reliant on collecting data (Cinar & Ateş, 2022). Apple has thus limited the ability of apps to monitor user behavior without first getting explicit consent. It has further decreased the personalization of third-party cookies and made targeted advertising, as well as exchanging individual data with data brokers, more difficult (Apple, 2021). Thus, a major player within Big Tech is increasingly committed to protecting customers. In fact, Apple's new data privacy policy is estimated to be costing Facebook about $12 billion a year (O'Flaherty, 2022). Simultaneously, Apple has expanded its capabilities to collect first-party data and thus has more granular and real-time data (Kraus, 2021).

IT infrastructure for data storage and privacy is becoming more flexible but also more complex through technological advancements such as cloud services. With greater flexibility comes

higher risks and vulnerabilities in terms of cyber security and privacy-compliant procedures. Companies are being forced to implement data privacy on the operational level to gain strategic advantages (Acquisti et al., 2016, 2020). Given the growing demand for data privacy, this thesis aims to discuss the added value when firms provide elevated levels of data privacy in terms of enhanced customer loyalty, consumer perception of the brand, etc. We will explore the impact of Data Privacy Policies on business models. What are the implications of renewing Privacy Policies? How do companies benefit from these, what is the added value, and how do these measures provide a strategic competitive advantage?

The Research Question arising from the above-mentioned challenges and being examined in the paper is: Can a Firm's Data Privacy Policy Provide an Edge Over Competitors?

2. Literature Review

This literature review consists of four sections. These encompass the data privacy environment and related concerns as well as the techniques of deriving data. Moreover, the literature concerning motives of firms for enhancing data privacy policy and the impact of these moves on CA will be explored, along with different strategies and expected benefits.

2.1. Data Privacy and Regulations

What is data privacy?

To further examine the role of data privacy within a business context, it is essential to shed some light on the term data privacy and its interpretation in literature. The Cambridge Dictionary (n.d.) describes *privacy* as *"the right that someone has to keep their personal life or information secret […]".* The *GDPR* defines the term *personal data* in Article 4 as

> *"… any information relating to an identified or identifiable natural person ('data subject'); […], in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (GDPR, 2016).

Hence, data privacy is the right that *personal data* shall be kept secret, which aligns with the second chapter of the *EU Charter of fundamental rights*. This states that EU citizens have the right to the protection of their data (European Union, 2012). However, this definition should not be taken to be exhaustive since unambiguous interpretation is difficult due to many different factors concerning privacy. Individuals tend to have their own particular conceptions of privacy. Therefore, this thesis accepts that there are ambiguities and nuances to the notion of data privacy. However, in light of discussing the impact on CA, data privacy shall be considered a valuable asset for businesses and individuals (Renaud & Gálvez-Cruz, 2010).

Value of Customer Privacy

Consumers' personal information gained from data represents a valuable economic resource for businesses. Firms acquire user data, process it for business purposes, and frequently sell it to third parties. In this environment, data practices, including the collecting, processing, and marketing of huge amounts of personal data, are frequently perceived negatively by users. This leads to growing concerns about the preservation of privacy and the dangers of malpractice (Acquisti et al., 2016). Furthermore, people are becoming more conscious of the worth of their data, at least in theory, and some are even demanding monetary compensation for personal data

being sold. Businesses profit from significant data-driven knowledge and users gain benefits from data-driven services and products (Schomakers et al., 2020).

The multi-layered nature of data privacy and user behavior can be illustrated in the relation between the *privacy paradox* and the *privacy calculus*. The *privacy paradox* describes the tension between individuals' privacy concerns and their willingness to share personal information. On one hand, individuals are increasingly aware of the risks to their privacy and the potential for personal data to be mishandled. Alternatively, people continue to share personal information freely, often without understanding the implications. The behavior is exemplified by a cost-benefit trade-off within the *privacy calculus model* in which a set of factors are weighed by individuals when deciding whether to share personal information. These include perceived benefits and risks of sharing, the trustworthiness of the party receiving the information, and the overall comfort level with sharing personal information (Chen, 2018). If users decide not to divulge specific personal information, those benefits become opportunity costs (Acquisti et al., 2016).

The value of personal data is context-dependent and idiosyncratic for each user. Privacy trade-offs are intertemporal and entail intangible and tangible benefits. Costs are uncertain and often occur in the future including loss of autonomy due to the disclosure of data. Even though privacy captures subjective preferences, it can be characterized as an intermediate good. Valuing privacy is not trivial as the reference points vary: costs a user would accept, the expected cost that the user would experience through disclosure or breaches, or expected profit that the data holder can derive through the personal information. Although personal data is traded by businesses, the market structure and lack of an open and recognized market do not allow users to participate in these trades (Acquisti et al., 2016). Consumer privacy and protection concerns vary according to the type of digital data. A recent study by Anant et al. (2020) indicates that the content of emails, downloaded files, location data, and chatrooms are perceived as very sensitive data by North American users. But the importance of data privacy decreases with time of internet usage, searches performed, and websites visited. Moreover, businesses that take adequate measurements to prevent data breaches, limit the use of personal data, and transparently report hacks and breaches, are perceived as reliable and trusted brands by consumers. However, as already discussed in the preceding chapter in the context of the privacy paradox, consumers themselves do not take adequate measures to prevent data malpractice despite increasing concerns (Anant et al., 2020).

In order to preempt this issue, regulations such as the GDPR provide a framework for protecting data privacy, which will be highlighted in-depth in the following section.

GDPR

The *GDPR* introduced in 2018 supersedes the 1995 EU Data Protection Directive and provides a framework for businesses to protect consumers' *personal data*. Processing personal data of EU citizens must comply with six key principles described in the GDPR. Being an important component of EU privacy and human rights law, it requires businesses to receive explicit consent from individuals before collecting, analyzing, or sharing personal data.

Article 5 of the *GDPR* describes six principles relating to the processing of personal data (European Parliament & Council of the European Union, 2016):

a. *Lawfulness, fairness, and transparency:* Businesses must process personal data lawfully, fairly, and transparently;
b. *Purpose limitation*: Businesses can only process personal data for specified, explicit, and legitimate purposes;
c. *Data minimization*: Businesses must only collect relevant personal data in accordance with the compliance of the defined purpose;
d. *Accuracy*: Personal data must be accurate and up to date and erased in case of inaccuracy;
e. *Storage limitation*: Personal data must solely be stored until the purpose of the collection has been reached;
f. *Integrity and confidentiality*: Best practice technologies must be implemented to protect personal data from unauthorized access, disclosure, damage, or destruction.

The GDPR governs any business that processes personal data of EU citizens, irrespective of the location of the business, and defines a precise framework. Particularly, Chapter 3 and Chapter 8 are crucial within the context of this thesis. Initially, Chapter 3 discusses the right to access personal data, the right to rectify inaccurate or incomplete data, the right to erase data (*right to be forgotten*), the right to restrict processing, the right to object to processing, and the right to data portability. Chapter 8 stipulates that businesses that infringe on the GDPR will be fined the greater of either €20 million or 4% of their annual turnover (European Parliament & Council of the European Union, 2016).

The role of data privacy policies

While businesses are assiduous in accessing customer data, the privacy factor remains the most important issue that must be resolved by organizations. Concerns about collecting, processing, and utilizing consumer data and the rising number of information leaks demand firm strategies concerning comprehensive data handling. Businesses must be aware of risks and have policies in place to handle leaks, as these can have long-term damaging effects on businesses and cause economic losses (Chang et al., 2018). Firms' data privacy policies are generally structured to protect the confidentiality of customer information. This includes provisions for how information is collected, used, and protected. Additionally, policies should also disclose if data may be sold or shared with third parties and the purpose behind it (Laird, 2022). Fouad et al. (2020) state that 87.5% of 20,218 analyzed cookies do not provide a cookie policy explaining their data processing purpose.

It remains to be seen which types of data usage are permissible and which are not, and it is necessary to determine to what extent data protection properly implemented can be used to gain CA.

2.2. Data Gathering

Data capturing principles

Personal data has been framed as the *"new oil of the internet"* or the new currency of the digital world (Humby, n.d.). Nevertheless, one commonality is that oil and data are only valuable when they are processed. To gain insights for customer retention, new revenue/business models, advertising, etc. data must be managed considering four principles: *Data privacy* demands that data analysis complies with data regulations such as the GDPR. Therefore, adequate *data protection* must prevent data breaches and the loss of valuable data. Lastly, *data preparation* describes the process of consistently and repetitively scrubbing data to improve the quality of insights (Talagala, 2022).

Regarding business strategy drivers for acquiring CA, it is crucial to define not only the market but also the business model and processes surrounding monetizing data. In the literature, there are various definitions of CA and hence associated ambiguities (Lieberman, 2021). Porter (1985) argues that CA may be achieved by particular factors including lower costs, product differentiation, and creating distinctive value for customers. According to Porter, CA may occur in conjunction with economies of scale due to a company's market positioning, business models,

or processes and competencies. Dagnino et al. (2021) suggest that CA is derived from managing factors that uniquely apply to a business under constantly changing conditions. Successful competitive strategies are predicated on understanding the competition, as well as the drivers that underlie accruing advantage (Christensen, 2001).

Individuals' data is derived by participation in daily transactions involving their information in exchange for a provided service. The retrieved information consists of vestiges of users' digital activities. A search engine query, for example, indirectly sells information about the user's interests in return for relevant results. Members of an online social network sell information about their personal lives, demographics, and networks of friends and acquaintances in exchange for a new way to communicate with each other (Acquisti et al., 2016). Data privacy addresses the issues of acquisition, storage, purposing, and analysis of data as well as disclosure to third parties of personal information. When users create, share, and consume digital content through online platforms, content is personalized by first- and third-party cookies, web beacons, tracking pixels, and fingerprinting. This leads to personally identifiable information (PII) associated with user identities and behavior being collected and applied for business purposes. First-party and third-party trackers are the two crucial components of online tracking (Cinar & Ateş, 2022).

Cookies are textual data stored on servers either temporarily for authentication reasons or permanently and set via HTTP requests. Both types of trackers are intended to enhance the online experience. However, first-party cookies are directly stored on the computer by the domain or website and seek to improve functionalities on the visited website – tracking user analytics data to customize services/products of the provider. The user is exposed to an improved user experience by saving, among other things, language preferences, the cart, and login data (Demir et al., 2022). Third-party cookies enable tracking of users for fraud prevention, law enforcement and anti-money laundering (Cinar & Ateş, 2022). On a technical level, they are similar as they can perform the same function. The difference is in the purpose – first-party trackers are crucial for website performance and are always activated. In contrast, third-party cookies are non-domain created. Ad-tech companies place advertisements across sites to increase interactions with products and motivate customers to buy (Demir et al., 2022). Advanced digital technologies optimize, automate, and simplify the process of monitoring, tracking, aggregating, and analyzing personal data. Digital advertising is reliant on third-party data for comprehensive information about consumers (Cinar & Ateş, 2022).

Digital Marketing

In 2022, ad spending on digital advertising is expected to reach $616 billion (Statista, 2022). Digital Marketing is an activity deployed by most every business (Bala & Verma, 2018). The term describes the use of digital channels to reach, acquire, and retain customers by promoting the brand as well as products and services (Barone, 2022). Kannan & Li (2017) suggest that digital marketing and the process of value creation through new customer experiences are enabled by digital technologies and are *"an adaptive, technology-enabled process by which firms collaborate with customers and partners to jointly create, communicate, deliver, and sustain value for all stakeholders"*. The shift from third-party data to first-party data has intensified, stemming from growing consumer concerns and comprehensive data protection regulation. Alternative approaches and technologies are crucial for ensuring that the customer experience will not suffer due to the shift and that transparency expectations concerning data collection practices will still be met (Cinar & Ateş, 2022). Advertisers and publishers rely more heavily on direct engagement with the consumer. Hence, approaches need to create a user experience promoting connections with consumers (Brodherson et al., 2021). Key success factors for an effective marketing strategy to achieve CA include promoting privacy characteristics associated with the brand to customers (Kannan & Li, 2017). Such strategies and approaches will be further explained in Chapter 2.4.

2.3. Key Drivers

> *"The added value of privacy is intrinsic no matter where your company sits in the digital economy. From consumer goods manufacturers to healthcare services entities, any business will benefit from proactively tackling privacy issues in one of three primary ways: protecting your brand, offering a competitive advantage from integrating privacy and security features into products and services, and creating new products and services designed to protect personal data"* (Hoffman, 2014).

As discussed in Chapter 2.2, CA is derived from a combination of a series of conditions that prevail (Porter, 1985). Obtaining a market position requires the firm to take certain actions along with appropriate exploitation of internal or relational resources. There are different approaches to achieving CA including: the market-based view (MBV), the resource-based view (RBV), and the relational view (Wang, 2014).

The Market-based view (MBV)

The MBV of strategy relates firm performance to industry factors and the firm's orientation towards the external market. The strategic positioning of a product distinguishes it from

competitors due to its differentiated qualities in a competitive landscape. Porter's Five Forces theory traces a firm's performance to the structure and competitive dynamics of the industry in which it operates. But industries are both dynamic and complex with multiple interdependencies, i.e., decreasing the applicability of the Five Forces Model. Strategic management studies since the 1980s propose that key determinants of profitability are firm-specific rather than market-specific and sustainable CA is based on resources and capabilities instead of solely on products and market positioning (Wang, 2014).

The Resource-based view (RBV)

Achieving CA can be explained by the external context and firm positioning within the MBV or the internal possession or access to certain resources and knowledge, which is emphasized by the RBV (Dagnino et al., 2021). Core resources focusing on the capabilities of a firm are its primary source of CA (Christensen, 2001). Resources can be distinguished in various ways, including the distinction between intangible and tangible resources. A potential competitive edge can be achieved by distinctive, rare, valuable resources that cannot be imitated or replaced by competitors. The VRIO (Valuable, Rarity, Imitability, Organization) framework has been applied to analyze a firm's internal resources and capabilities (Wang, 2014). Wang (2014) suggests that knowledge and capabilities can be ascribed to the RBV and elaborates that these two factors have idiosyncratic characteristics and hence can be seen as individual factors associated with a firm for achieving sustainable CA. Thus, the reasoning is that *"capabilities are the source of competitive advantage while resources are the sources of capabilities"* (Wang, 2014). But as Lieberman (2021) points out, there is definitional ambiguity and a lack of predictive ability in claiming a true causal relationship between resources and capabilities and CA.

The Relational View

The relational view critiques assumptions of the RBV and MBV. It suggests that CA is achieved through the combining assets, knowledge or capabilities in a mutually beneficial approach. Relation-specific assets such as shared knowledge, complementary resources, decreased transaction costs, and scarcity of partners, and not the MBV's notion of barriers to entry through positioning or the RBV's set of unique resources and capabilities, are key for business success (Wang, 2014).

PESTEL

Privacy-enhancing measures offer a business opportunity to attain CA (Hoffman, 2014). To gauge the effectiveness of data privacy-enhancing measures and understand external influence factors (E.g., regulatory and technical challenges for data privacy), drivers of data privacy-enhancing measures must be identified. The PESTEL Framework considers political, economic, social, technological, environmental, and legal factors. It is a strategic management tool that frames and analyses key drivers of transformation in a particular industry or market (Issa et al., 2010). PESTEL analysis aims to help organizations identify macro factors of the external business environment to develop strategic plans to capitalize on opportunities and minimize risks (Helbig et al., 2021).

Political

Political factors concern the influence and risks a business or industry must navigate associated with its political environment, the source of policies and regulations (Issa et al., 2010). Governments and institutions must protect the rights of their citizens (Brunnee & Toope, 2006). This includes individual rights to data privacy and demands for stricter data regulations due to proliferating data breaches (Anant et al., 2020). The GDPR represents a key political influence factor because institutions need to comply e.g., with the right to rectify or erase data (Wolford, 2020). Furthermore, data privacy and protection are a geopolitical phenomenon since businesses need to comply with data regulations of the jurisdictions in which they operate to avoid fines or sanctions. Data protection regulations change with various geographies (Gregory, 2022).

Economic

The economic factor considers the financial aspects of the business (Issa et al., 2010). From an economic perspective, data privacy has managerial importance since malpractice results in fines as described in Chapter 8 of the GDPR (Wolford, 2020). For instance, Amazon incurred roughly €746 million in punitive sanctions because of a lack of transparency to opt-in consent mechanisms associated with the company placing cookies on consumers' devices. In another example, WhatsApp was fined €225 million because it failed to explain data processing practices in its privacy notice. The third highest fine of €90 million was issued to Alphabet because of their cookie consent procedures on YouTube where cookies were easy to accept but disproportionally hard to refuse (CMS Legal, 2022). However, data privacy does not solely

represent a negative economic impact on the firm through fines. Marota et al. (2019) estimated that Fortune's Global 500 will invest approximately $7.8 billion in technical and organizational measures to be compliant with the GDPR. Moreover, by not setting cookies, as well as not collecting and analyzing personal-related data, revenue from personalized and targeted ads is foreclosed (Marotta et al., 2019). Hence, there are significant costs associated with data privacy-enhancing measures.

Social

Emerging new technologies are increasingly integrated into our daily lives. Artificial intelligence or machine learning increases the complexity of how these bear upon society (Hijmans & Raab, 2018). The social factor is closely linked to ethics. Data collected does not only consist of non-sensitive data but also encompasses sensitive personal data i.e., ethnic origin, political opinion, medical data, financial information, etc., which requires explicit consent (Issa et al., 2010; van Ooijen & Vrabec, 2019). Legal and regulatory adjustments do not encompass the full scope of ethical considerations regarding data handling, data protection, and data privacy. Therefore, Corporate Digital Responsibility (CDR) could offer an approach to mitigate ethical concerns in instances of data breaches (Lobschat et al., 2021).

Technological

Advances in technology enable more precise analyses of data, which offers advantages for data-driven business models, targeted marketing, deploying behavioral science insights, etc. (Grewal et al., 2020). Taking associated risks into consideration, Onik et al. (2019) suggest that data breaches originate less from technological disorder but rather from the lack of regulations, monitoring, and accountability. Consequently, data protection regulations should be developed to vigorously protect personal information.

Environmental

Data privacy does not directly influence the environment. Nonetheless, increasing amounts of data collection raise the electricity consumption of data centers. The large amount of personal data stored, processed, and analyzed is associated with higher carbon footprints. Greater energy efficiency, as well as renewable energy, are reasonable approaches for reducing the carbon footprints of data centers since limiting technology is not a feasible alternative (Jones, 2018; Oró et al., 2015).

Legal

The GDPR provides a legal framework for businesses, prioritizing individual protection by regulating the collection, storage, and processing of personal data. However, defining a workable and substantive privacy policy is onerous due to the trade-offs needed and the tension between profit maximization through data use and the imperative to protect consumer privacy (Lobschat et al., 2021). From a data privacy point of view, data breaches and unauthorized access to personal information have legal consequences and lead to loss of trust, diminished brand loyalty, loss of stock price value, higher audit fees, etc. (Schlackl et al., 2022). Legal and economic external factors regarding data privacy are closely linked, e.g., non-compliance with the GDPR results in legal consequences and fines (Gruschka et al., 2019).

To summarize the PESTEL analysis, it becomes clear that drivers of data privacy are legal, ethical, financial, and technical.

2.4. Strategic approach

Lessig (2007) discusses how data privacy can be achieved without restraining the systematic exploitation of data. He proposes introducing the principles *regulating traceability* and *regulating use*. He came up with the architecture of the *"nym"*, which is an arbitrary complex token de-linking data to an individual. It cannot be used outside the technology system or is encrypted and changes accordingly to the environment. The second principle is to regulate use and hence traceability. This limits access to data that can be linked to an individual and also reduces the data's value. Additionally, businesses that have access to the *nym* and the individual's data, must be heavily regulated (Lessig, 2007).

Apple, for instance, embeds data privacy as a part of its privacy-focused strategy. This turns rising user privacy awareness into a differentiation factor for business advantage (Cinar & Ateş, 2022). Apple limited tracking of user behavior without permission by offering an opt-in or opt-out feature within its App Tracking Transparency (ATT). And it restricted the sharing of Apple devices' unique identifiers for advertisers (IDFA). As a result, personalized and targeted advertising decreased, making exchanging individual data with data brokers more difficult (Apple, 2021). Apple's new data privacy policy is estimated to be costing Facebook about $12 billion a year (O'Flaherty, 2022). Data privacy and consumer data can represent a barrier to entry since, hypothetically, incumbents could leverage a Big Data-related advantage to defend

themselves against an emerging firm or to favor their products in new markets through exclusionary behavior. Possessing consumer data by an incumbent may be a barrier to entry (Mehrat, 2020).

Organizational privacy self-regulation

The GDPR and other drivers that enhance data privacy highlight individual control in the data economy (van Ooijen & Vrabec, 2019). Emerging digital challenges such as data privacy should be proactively tackled by a comprehensive CDR, given that legal and regulatory guidelines do not reflect the fast-paced digital environment (Lobschat et al., 2021). Ownership in the data environment governs who possesses and is responsible for data. The principle of regulating use described by Lessig (2007) can be achieved by adapting consent forms in clear and easy-to-understand language. This increases awareness about the collection, purpose, use, and protection of personal information (Belani et al., 2021). Martin & Murphy (2017) argue that firms self-regulating based upon well-constructed privacy policies, in combination with opt-in provisions, offer adequate mechanisms for protecting consumer privacy. There is evidence of firms moving more strongly towards protecting data privacy. Providing consumers with transparency and control is linked to performance and better consumer perception. Moreover, a comprehensive data privacy policy can protect a company from potential spillover effects caused by a competitor's data privacy breach. Recognizing the sophistication of consumers and addressing data management through transparent practices, instead of sourcing and using data in secret, appears to be a prerequisite for privacy as a differentiation strategy (Martin & Murphy, 2017). The notion of core competency refers to the coordination of the unique capabilities that an organization possesses. Thus, competitive advantage can be achieved through various capabilities an organization inhibits, such as processes, services, know-how, or other areas of expertise (Javidan, 1998). Creating value for stakeholders is crucial as highlighted by the stakeholder theory (Parmar et al., 2010). Shifting focus from privacy being an obstacle to serving as an opportunity requires holistic stakeholder management. Pursuing a data privacy-focused strategy and establishing concise guidelines for data handling, improve customer loyalty and retention. Additionally, customers are more likely to reveal their personal data (Martin & Murphy, 2017). Hence, this data can be leveraged for successful marketing and product development resulting in CA. Moreover, enhancing data privacy through transparency offers a way to minimize the risks identified in the PESTEL analysis. Simultaneously, properly designed regulation can partially or fully offset the cost of compliance and initiate innovations according to Porter’s hypothesis (Bleier et al., 2020).

Operational and Dynamical Capabilities

There is a tendency for organizations to think in silos which can lead to a lack of strategic clarity. The consensus concerning understanding data privacy and the requirements of various stakeholders, proposed by legal departments and system engineers, tends to be limited. Firms need to promote cross-functional knowledge and increase cognizance of organizational capabilities about the diverse requirements for data privacy (Petroff & Fauser, 2022). Key factors for attaining CA are internal resources, knowledge, and capabilities according to the RBV (Wang, 2014). *"Beyond Apple, a limited number of firms is emerging that appears to be competing on strong consumer privacy protections"* (Wang, 2014). Being a first mover by building and allocating internal resources and capabilities to data protection may be advantageous (Martin & Murphy, 2017). Lessig's (2007) principle of regulating traceability leads us to the concept of Privacy Enhancing Technology (PET). PETs offer noteworthy individual and societal benefits of data protection while maintaining data analytics (Acquisti et al., 2020). Encryption enables data analytics on encrypted data that matches the result of operational data once decrypted. In general, cryptographic algorithms enable data analysis while maintaining data privacy with encrypted data. Data masking techniques adopt the concept of Lessig's (2007) nym by protecting personal information through the minimization or pseudonymization of data sets. Generating synthetic data sets by applying machine learning algorithms offers an additional opportunity for randomizing (Scheibner et al., 2021). Nonetheless, PETs are inherently individualistic solutions that also highlight the systematic problem of privacy. They tend only to work in specific circumstances or applications (Acquisti et al., 2020). Enabling first-party data is crucial regarding discontinuing third-party data to realize the potential of data analysis. Concretely, first-party data must be obtained via as many company-owned channels as possible and compiled in a digital ecosystem considering every touch point along the customer journey (Cinar & Ateş, 2022). First-party data could lead to restructuring internet commerce by creating incentives for first-party favorable strategic alliances with a perspective of the relational view of CA (Hoofnagle et al., 2019).

3. Methodology

3.1. Research Design

This chapter examines the research findings. The outcomes of the qualitative research and the quantitative research were triangulated to validate the identified findings. The purpose of triangulation within this master thesis is to obtain validation of results through the analogy of varying perspectives following the three rationales: **completeness** to reduce flaws, **contingency** to understand which strategy is suitable, and lastly **confirmation** in order Vanquishing the biases imposed by a single technique (Jack & Raturi, 2006). The research considers the perspective of experts and the consumer perspective on privacy enhancement. Complementing qualitative methods with quantitative methods ensures an improved data analysis and consequently a more precise conclusion (Kaplan, 2015).

3.2. Qualitative Data Collection

While secondary research involves applying results and findings of previously completed studies to the research question, primary research provides first-hand specific results to the problem (Hox & Boeije, 2004). Semi-structured interviews offered an opportunity to generate insights and understandings of experts within the data privacy sphere. Flexibility within the process of conducting the interviews allowed out-of-scope responses and expanded upon the experts' assessments and expertise (Rowley, 2012). The catalog of questions within the semi-structured interviews served as a guide for discussing the findings and subjects under investigation. This allowed for more flexible and versatile communication to elaborate perceptions of the problems and issues (Kallio et al., 2016). Accordingly, depending on the dynamics of the interview, the focus of the interview could be adjusted. The biggest advantage of semi-structured interviews was the situational influence in contrast to standard interview techniques (Adams, 2015).

The interview guide was developed to elaborate on the motivations and drivers for employing data privacy measures. Firstly, general data of the experts were gathered such as the occupation and the employer. The second part involved discussing motivations to enhance data privacy measures, including disadvantages and advantages. This step was important for understanding the expert's backgrounds and views on data privacy. The last part dealt with implications and drivers of capabilities and the strategy regarding data privacy-enhancing features. The interviewee was given room for feedback at the end of the interview. The list of experts can be found in Appendix A. The interviews were conducted with experts in the subject areas of data

privacy and/or protection, individuals who occupy a position regarding data privacy and cyber security within a business, or individuals who published articles regarding data privacy in a business context. However, it needs to be highlighted that experts' views are personal and have biases. The interviewee selection process sought out individuals making decisions about data privacy within an organization and subjects who research data privacy from an external point of view. Focusing not only on high-level experts granted insights (von Soest, 2022).

Chapter	**Questions**
Introduction	What is your age, your country of origin, and your current occupation?
Motivation to enhance data privacy measurements	What are the motives for businesses to protect consumers data?
	Is there an advantage for data privacy enhancing measurements? What is that advantage/disadvantage? Why?
	How can data privacy be a differentiation factor?
Implications on capabilities and strategy	What know-how and capabilities do companies have to build to enhance data privacy?
	What are the key variables/capabilities associated with data privacy? E.g., technical, regulatory
	How do you think will data privacy impact data-driven businesses? How will businesses suffer from data privacy-enhancing measurements?
	Do you expect positive spillovers on the brand if businesses decide to implement data privacy measures?

Table 1: Guide semi-structured interviews

3.3. Qualitative Data Analysis

The interviews were recorded and summarized. The corresponding summaries can be found in Appendices B to I. According to Rowley (2012) data analysis is an iterative process and consists of four key components: *"(1) organizing the data set; (2) getting acquainted with the data; (3) classifying, coding, and interpreting the data; (4) presenting and writing up the data".* Moreover, the statements can be analyzed in qualitative content analysis and illustrated by quotes or numerous statements that support the findings (Devi Prasad, 2019; Rowley, 2012)

3.4. Quantitative Data Collection

The primary research was enhanced by complementing quantitative data analysis with qualitative data analysis which leads to a comprehensive understanding of both the customer

perspective and the experts' perspective. Conclusions were drawn by triangulating the primary data with the secondary research (Kaplan, 2015). Online surveys allow the researcher to monitor customer attitudes toward the research topic. Data privacy can be considered a sensitive topic. An online survey is efficient, with higher response rates, and anonymity. It addressed the research topic to a group affected by data privacy concerns simply due to their use of the internet (van Selm & Jankowski, 2006). The 7-point Likert scale was used to measure attitudes, opinions, and perceptions on an ordinal scale (Joshi et al., 2015). The survey was conducted in December 2022 and administered in English. Before launching the survey, it was tested for biases and flaws with ten voluntary students, whose answers were not considered in the final analysis. Firstly, general information about the attendees was gathered. Eventually, to test the findings of the literature review, information was gathered about how data privacy is perceived and assigned importance. The following questions were designed to understand sharing of data and the use of services. The research concluded with a use-case in which a company followed a privacy-focused strategy and protected the data privacy rights of users with an enhanced data privacy policy. This was used to understand the effect on the brand as well as on its products and services.

Category	**Question**	**Answer**
Demographics	What is your gender?	
	How old are you?	Open Question
Personal Preference	Data privacy is important to me.	1-7
	I do not want businesses to collect personal information.	1-7
	I would like to have more data privacy rights.	1-7
Perception	I feel like my data is well protected on the internet.	1-7
	I know how and for what my personal data is used for and if it is transacted/sold to third parties.	1-7
Behavior	I accept every cookie.	1-7
	I am concerned when a business whose service/product I frequently use or of which I am a customer is affected by data breaches.	1-7

Now imagine a business introduced a new data privacy policy in which you can decide to opt-out of sharing data with advertisers.		
Reaction	I would prefer this business over the competition.	1-7
	I think the business has improved its image and cares for its customers.	1-7
	I would be willing to buy this product even though it is more expensive than the competitors' one.	1-7
	Please indicate how much more you would be willing to pay for this service/product over the competition.	0-100%

Table 2: Questions survey

3.5. Quantitative Data Analysis

Quantitative data analysis helps describe, explore, and examine the relationship in the data set using statistical tools. After entering and checking the data set for flaws, statistical analysis tools were applied (Saunders, M, Lewis, P & Thornhill, 2016). Firstly, descriptive statistics, such as the mean, median, standard deviation, and allocation of votes, were analyzed and described. Next, correlations between variables were plotted to assess their dependence.

Secondly, three regression analyses were conducted to find relationships between a dependent variable and one (in the case of linear regressions), or two, (in the case of multiple regressions), independent variables. The goal of performing a regression analysis is to determine which, if any, of the independent variables are significantly related to the dependent variable, and to quantify the strength of this relationship. This information can be useful for making predictions, understanding underlying factors that influence a certain outcome, and testing hypotheses about cause-and-effect relationships (Saunders, M, Lewis, P & Thornhill, 2016). Additionally, two null hypotheses were established, and t-tests were conducted to determine whether there is a significant difference between the means of the two groups. By conducting a t-test one determines whether the difference between the means of the two groups is statistically significant, and therefore whether the observed difference is likely due to chance or to a real causal effect (de Winter & Dodou, 2010).

4. Results

4.1. Analysis of Interview

As described in the methodology Chapter 3.3, the semi-structured interviews were analyzed according to Rowley (2012) by *"(1) organizing the data set; (2) getting acquainted with the data; (3) classifying, coding, and interpreting the data; (4) presenting and writing up the data"*.

The eight interviewees were experts in data privacy-related occupations with diverse backgrounds to enrich data collection and ensure that data privacy is assessed from different perspectives. The list of interviewees can be found in Appendix A. The key insights of the interviews were classified into 5 categories, namely *drivers for data privacy, trust, trade-off, capabilities, and holistic processes* which can be seen in Figure 2 and will be outlined in this chapter. In general, all experts mentioned that users are becoming increasingly sensitive when their personal data is concerned. The second interviewee, a director in a consulting company who leads the GDPR area of competence also noted that as soon as data protection moves into focus, further *"stray effects"* follow across a variety of operational processes. Interviewee 3 confirmed this by highlighting how data privacy is already considered in the early stage of product development when programming a new website. Businesses are increasingly facing data privacy challenges and need to identify their particular needs to assess relevant strategies.

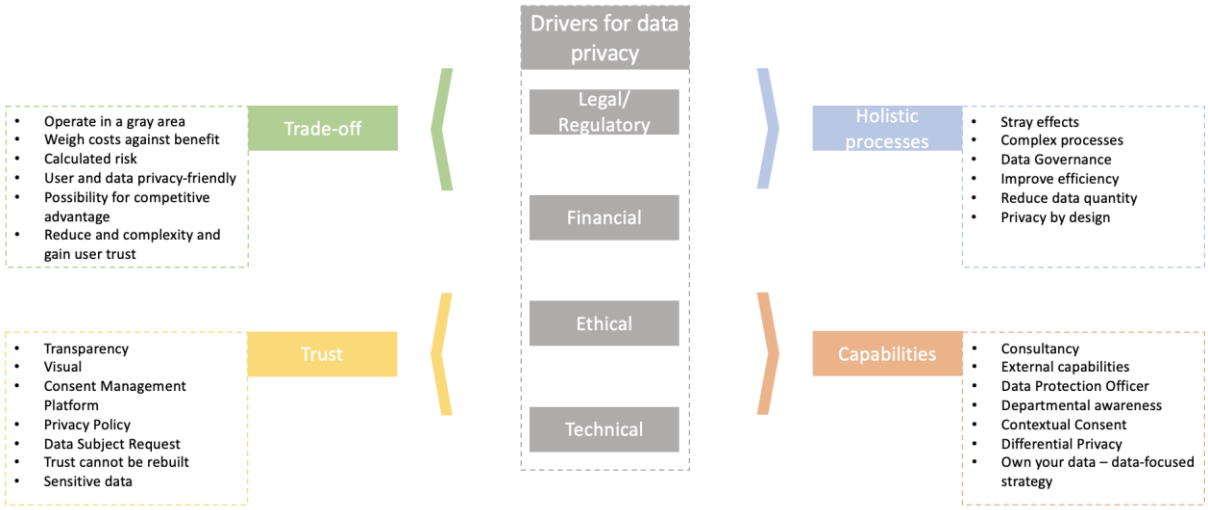

Figure 2: Overview of Content Analysis

Drivers for data privacy

Legal & Regulatory

All eight interviewees cited legal/regulatory reasons as the main driver for businesses to adopt data privacy measures. Data privacy is a legal concern due to the fundamental right of individuals to have control over their personal information and how it is collected, processed, and shared as defined in the GDPR. Interviewee 4 confirmed that by saying that *"data privacy is simply a legal requirement for businesses that fall under the scope of the GDPR".* The implementation of data privacy laws, such as the GDPR, has established the framework for the protection of personal data and grants individuals the right to know how their data is being utilized and have some control over its distribution, as mentioned by interviewee 1. These laws mandate that organizations be transparent about their data collection practices, obtain individuals' consent before collecting their data, and take measures to safeguard the security of that data. Nevertheless, interviewee 3 emphasized that the regulations and jurisdiction are running behind the business. Accordingly, the technologies and measures to circumvent the regulations are developing fast, which creates "*gray areas"* as room for maneuvering.

Financial

Data privacy is also a financial matter because it is closely linked to the concept of data security. According to interviewee 1, an organization has the responsibility to protect the collected, processed, and stored personal information from unauthorized access, use, or disclosure. If the organization adequately protects the personal data it collects, it could prevent financial consequences such as legal fees and reputational damage which was confirmed by all interviewees.

Interviewee 4 added that if the organization is perceived as not taking data privacy seriously, it could lose the trust of its customers, which could lead to negative financial consequences. Organizations need to safeguard the personal data they collect to avoid financial risks and protect their reputations. Moreover, interviewees said that following regulations have costs associated arising from consultancy services, legal support, and employing the required data privacy officer (DPO). Additionally, interviewee 2 mentioned the impact of data privacy on marketing spending. Retargeting is more complicated now with more impersonalized data and consequently *"reducing the Return on Advertising Spend".* Interviewee 8 provided a different perspective on data privacy, as he discussed that as soon as customers can participate in the monetization and trading of data, a whole new market will emerge.

Ethical

The ethical aspect of data privacy was covered by two of the interviewees as it is closely tied to the concept of personal autonomy. When an organization collects, uses, or shares personal information, it controls how data will be deployed, potentially impacting the individual. Organizations need to respect individuals' personal data. Interviewee 3 said that *"businesses may pursue data privacy for moral reasons, but this cannot be seen as a business driver"*. Additionally, data privacy is closely linked to the concept of trust, which is described separately due to the importance that the interviewees attached to it. Despite trust, interviewee 2 reasoned that insurance companies could analyze purchasing behavior and, for example, increase premiums when cigarettes are purchased.

Technical

Interviewee 3 said that from a software developer perspective a business would also need to have the necessary technology and infrastructure in place to support data privacy-enhancing measures and identify possible risks of a breach. Interviewee 1 introduced differential privacy as a technical capability and interviewee 2 consentless tracking. The best practices are for instance differential data privacy, where data is obscured by adding mathematical noise, and contextual consent, where consent should be drawn depending on the context and the purpose for collection should be transparently shown. Nonetheless, they also highlighted that there is no state-of-the-art technical capability a firm needs to prohibit and that it depends on businesses' circumstances.

Trust

Data privacy can strengthen consumer trust in a company by demonstrating that the firm takes responsibility for protecting personal data. Interviewee 2 explained that

> *"At the end of the day, data privacy is important because of course you want to protect customer data and as long as you are sensitive and respectful of the data, we will continue to receive data from customers and can therefore continue to develop."*

Hence, when a company has strong data privacy practices in place, it shows that it is committed to respecting individuals' autonomy and protecting their personal information. According to interviewee 1, trust can be clustered in either quality or emotions. Three of the eight interviewees identified a visual and transparent privacy framework as key to building trust. Interviewee 1 introduced the concept of a Privacy User Experience (Privacy UX) in which

special focus should be put on *"(1) Consent Management Platform, (2) Privacy Policy and (3) Data Subject Request"*. According to interviewee 5 data privacy must be both *"pragmatic and easy to understand"*.

Trade-off

Coming to the current status quo and how businesses evaluate the added value associated with data privacy, all interviewees explained it as a trade-off. The assessment of whether data privacy is beneficial was not unanimous among the interviewees and they viewed it as greatly dependent on the circumstances. According to some experts, implementing data privacy features and being stringent on regulations depends on an individual brand's appearance and user perception. As asserted by interviewee 3:

> *"It's very difficult to regain this authenticity. For example, WhatsApp with its end-to-end encryption. Well, if that had been said by another company, it might be more likely to be believed than it is now with WhatsApp."*

Some interviewees argued that it would be cost-efficient to comply with the regulations and not receive fines. However, it was also mentioned that the comfort of implementing the necessary measures is higher than the risks. Interviewee 2 provided insight into the practice that even prominent automotive manufacturers are weighing the trade-off between the risks of receiving fines and the benefits of potentially increased sales. Three interviewees mentioned that to have a positive effect on a brand measure must not be like *"greenwashing"*, meaning promoting misleading claims about data privacy. Interviewee 4 concluded that

> *"Of course, your repetition improves because it shows that you sort of care about your customer, care about their personal data [...]. But again, I don't know if that's something that the average consumer values."*

Thus, the general perception of the experts was that data privacy-sensitive users respond to data privacy enhancements and regular users only focus on the subject after data breaches have occurred

Capabilities

To comply with data protection regulations certain capabilities are needed and interviewee 4 said that *"it's a big investment and I can see why smaller businesses might find it harder to be compliant with"* and that big corporations have an advantage as they have more traffic on their websites to generate first-party data. According to interviewee 2, companies are required to follow the strategy *"own your data"* in which a data structure must be built to have efficient

data lifecycle management. Interviewees also mentioned capabilities such as regulatory expertise, security measures to protect personal data, and trained staff. Thus, it is essential to train employees on data privacy best practices and ensure that they understand their responsibilities for protecting personal data. *"Data privacy by Design"* was mentioned by some interviewees but interviewee 6 said that it is crucial to embed data privacy in the first steps of a process or product development. Excluding data privacy from the beginning and *"just asking for acknowledgment from the data protection officers in the end"* will necessitate inclusion in a later stage. Moreover, interviewees 6 and 7 highlighted the importance of a competent DPO. In this respect, decoupling these tasks from normal operations and the creation of a superior body, similar to the quality function, should ensure that the DPO can carry out activities independently.

Organizational processes

Data is perceived as a key driver for innovation in today's world. Nonetheless, the experts did not agree on whether data privacy inhibits innovation. Firstly, it can create constraints on how companies and organizations can use and collect personal data. Additionally, the introduction of coherent data privacy management is considered to *"increase effort at every level within a company"* as the cookie banner would not exist without the GDPR, according to interviewee 3. Contrasting preferences regarding data privacy are also evident within a business. Interviewee 2 illustrated this by saying that *"marketing always shouts no, no, no when it comes to data privacy and legal yes, yes, yes"*. Nonetheless, efficient, and automated data life cycle management (DLM) also decrease costs and complexity in case of a request to delete personal information. Besides, a positive *"stray effect"* is that once you start doing certifications *"data flows can be measured, and duplicate points reduced"*. Interviewee 7 elaborated on that point and said that businesses that have not understood the benefits data protection and privacy bring only do it because of regulatory fees and reputational damages. Instead, it was said that

> *"In contrast businesses who have understood that data protection is basically data governance, and that data transparency will and not can be an efficiency gain. Thus, reducing uncertainties and saving money because of transparent data flows."*

In the end, many experts confirmed that data privacy is a balancing act of working with competing imperatives and that measures that precede jurisdiction, such as consent-less tracking, offer an opportunity to operate in the *"gray area"*.

4.2. Analysis of Survey

The survey conducted resulted in 143 observations. The first step of the survey was to provide an overview of participants' general information. Among the 143 observations were 51.05% male (73 observations), 48.25% female (69 observations) and 0.7% (1 observation) has not disclosed their gender. The age group 18 to 24 is the most represented with 46.85%, followed by the age group 25 to 34 at 38.46% and the age group 35 to 44 at 9.09%. The remaining 5.6% of respondents are represented in some outliers in the age groups younger than 18 and older than 44.

The questions were designed to understand the behavior of the attendees regarding sharing of data and utilizing services. The survey sought to examine consumers' personal preferences towards data privacy by applying Likert scales to measure attitudes, perceptions, and behaviors. A value of 1 described that the participant *strongly disagree*s and 7 meant to *strongly agree* with the statement/question. To start analyzing the questions for the upcoming steps, the function *stargazer* produced a clearly arranged table of statistics such as the mean, standard deviation, median, the max. and min. for every chosen variable of our data set as shown in Table 3. Moreover, the correlations between each variable can be seen in Appendix J and K.

Statistic	N	Mean	St. Dev.	Min	Median	Max
Q1	143	5.769	1.214	2	6	7
Q2	143	5.329	1.418	1	6	7
Q3	143	5.713	1.254	2	6	7
Q4	143	2.636	1.412	1	2	7
Q5	143	2.406	1.606	1	2	7
Q6	143	4.727	1.553	1	5	7
Q7	143	5.322	1.292	2	6	7
Q8	143	4.273	1.725	1	5	7
Q9	143	5.483	1.560	1	6	7
Q10	143	5.895	1.155	1	6	7
Q11	143	5.902	1.064	2	6	7
Q12	143	3.336	1.869	1	3	7
Q13	143	10.741	17.790	0	2	81

Legend

Q1	Data privacy is important to me.
Q2	I do not want businesses to collect personal information.
Q3	I would like to have more data privacy rights.
Q4	I feel like my data is well protected on the internet.
Q5	I know how and for what my personal data is used for and if it is transacted/sold to third parties.
Q6	I accept every cookie.
Q7	I am concerned when a business whose service/product I frequently use or of which I am a customer is affected by data breaches.
Q8	I want to receive personal advertising based on websites I visited and my digital profile
Q9	I use services/products of businesses that do not promote data privacy. e.g., TikTok
Q10	I would prefer this business over the competition.
Q11	I think the business has improved its image and cares for its customers.
Q12	I would be willing to buy this product even though it is more expensive than the competitors' one.
Q13	Please indicate how much more you would be willing to pay for this service/product over the competition.

Table 3: Descriptive Statistics

The personal importance of data privacy was assessed by the statement *"Data privacy is important to me"* and the mean value was 5.77 with a standard deviation of 1.21. This indicates data privacy was a relevant factor for the participants. This finding can be confirmed as 87.41% of participants selected data privacy in the categories 5 to 7, only one participant disagreed, and none strongly disagreed. The descriptive statistics for the second question *"I do not want businesses to collect my personal information"* had a mean of 5.33 and a standard deviation of

1.41 and question 3 *"I would like to have more data privacy rights"* had a mean of 5.71 and a standard deviation of 1.25. The median answer was 6 in both cases, indicating the high importance of data privacy rights.

The two questions concerning the perception of data handling showed a similar distribution and effect. Nonetheless, the distribution was rather inverted as most participants rather disagreed with the questions *"I feel like my data is well protected"* and *"I know how and for what my personal data is used for and if it is transacted/sold to third parties".* The graphs are right-skewed and 77.62% somehow disagreed with the statement that they felt like their data was well protected. Moreover, the majority with 36.36% strongly disagreed with the second statement and both questions had 2 as the median.

After assessing the personal preferences about data privacy and the perception, of how their data is handled, the actual behavior was assessed. Firstly, participants were questioned rather they accept every cookie, whose values yielded a mean of 4.73 and a standard deviation of 1.55. However, the graph shifted more to the center compared to the distribution of the first part of the survey and only 5.59% strongly agreed. This showed that the customers still accept most of the cookies even though, they highly value data privacy has a high value for them. A mean of 5.43 for the questions *"I use services/products of businesses that do not promote data privacy. e.g., Instagram, Facebook, TikTok"* and 77.42% of the answers being from 5 to 7 indicated that participants used services in which they transacted their data to access the service. *"I am concerned when a business whose service/product I frequently use or of which I am a customer is affected by data breaches"* was strongly left-skewed represented by a mean of 5.32 whereas the span ranged from 2 to 7. Hence, consumers were indeed concerned if a business were affected by data breaches and as a consequence, this had negative implications for the brand. The answers to the question *"I want to receive personalized advertising based on websites I visited and my digital profile"* with an average value of 4.27 indicated a rather more even distribution compared to the previous questions. Hence, there was variance in individual preferences for receiving personalized advertising

Lastly, the use case *"Now imagine a business introduced a new data privacy policy in which you can decide to opt-out of sharing data with advertisers"* was incorporated in to understand the perception and implications of an enhanced data privacy policy on a business. The mean value for *"I would prefer this business over the competition"* and *"I think the business has improved its image and cares for its customers"* were both 5.90 with a standard deviation of

1.15 and 1.09 respectively. Accordingly, enhancing data privacy has positive implications for the business as it is preferred by consumers and improved a firm's image. Nonetheless, the monetization of this enhancement was not clear as the answers were distributed randomly. This can be also confirmed since the majority (53.85%) disagreed with *"I would be willing to buy this product even though it is more expensive than the competitors' one"*. The participants' answers to *"Please indicate how much more you would be willing to pay for this service/product over the competition"* ranged from 0% to 81% with a mean of 10.74. The median was 2, which showed that outliers influenced the mean, and the majority was not willing to pay a surplus for data privacy.

Interrelation

To explore the relationship between two continuous variables and explain how variables influence each other linear regressions were executed. Within the scope of this master thesis and considering the goal to identify whether privacy maximizing features leverage businesses CA the influence of the data privacy preference on selected variables shall be examined.

The relation between each dependent variable of the willingness to pay an extra amount (Q13) and the dependent variable whether the business has improved its image (Q11) was examined as the independent variable regarding data privacy preferences (Q1) and can be described by the following equations:

$$\textit{Willingness to spend an Extra Amount} = \beta_0 + \beta_1 * \textit{Data Privacy Preference} + \mu \quad (1)$$

$$\textit{Influence on Businesses Image} = \beta_0 + \beta_1 * \textit{Data Privacy Preference} + \mu \quad (2)$$

Additionally, a multiple regression was conducted to understand how selected variables are related to each other and how they jointly affect the dependent variables of whether the participants perceive the taken measure as an image improvement (Q11).

$$\textit{Influence on Businesses Image} = \beta_0 + \beta_1 * \textit{Data Privacy Preference} + \beta_2 * \textit{Concernedness of Data Breaches} + \beta_3 * \textit{Usage of Social Media Services} + \mu \quad (3)$$

	Dependent variable:		
	Q13	Q11	
	(1)	(2)	(3)
Q1	3.102**	0.276***	0.208***
	(1.206)	(0.070)	(0.075)
Q7			0.134*
			(0.073)
Q9			0.070
			(0.056)
Constant	-7.154	4.310***	3.601***
	(7.108)	(0.413)	(0.499)
Observations	143	143	143
R2	0.045	0.099	0.139
Adjusted R2	0.038	0.093	0.121
Residual Std. Error	17.448 (df = 141)	1.013 (df = 141)	0.997 (df = 139)
F Statistic	6.617** (df = 1; 141)	15.532*** (df = 1; 141)	7.488*** (df = 3; 139)
Note:			*p<0.1; **p<0.05; ***p<0.01

Figure 3: Regression Analysis

β_0 is the %- extra amount someone was willing to pay and was not statistically relevant. It would represent that consumer willingness to pay an extra amount for a product is 7% less when the importance of data privacy was ranked at 1. For each additional engagement unit in the importance of data privacy (Likert-scale), on average, the % - extra amount of the original price increased by 3.102%, *ceteris paribus*. The variable explained only 4.5% of the variation in the variable Q13 around its mean as indicated by the R^2.

Thereafter, the influence on the perceived image was explored. On average, for each additional engagement unit in the importance of data privacy, the perceived image increased by 0.276, *ceteris paribus*. This indicated that individuals who ranked data privacy higher perceived businesses that protect consumer data more positively.

The multiple regression (3) included next to the variable Q1 *("Data privacy is important to me"*) and the variables Q7 (*"I am concerned when a business whose service/product I frequently use or of which I am a customer is affected by data breaches"*) and Q9 (*"I use services/products of businesses that do not promote data privacy. e.g., Instagram, Facebook, TikTok"*). On average, for each additional engagement unit in the importance of data privacy, the perceived image increased by 0.208, *ceteris paribus*. For each additional engagement unit of the concern about data breaches (Likert-scale), on average, the perceived image increased by 0.134, *ceteris paribus*. On average, for each additional unit usage of certain services/products, the perceived image increased by 0.070, *ceteris paribus*. However, it was non-significant at the 1%, 5%, or 10% level, indicated by the missing stars next to this coefficient. The perceived image of businesses that promote data privacy was positively influenced by the individual preference for the importance of data privacy and the concern of data breaches used of services/products.

Hypothesis Testing

Finally, two hypotheses were tested by carrying out two-sample tests. Firstly, we examined how the sensitivity toward data privacy influences the perceived image improvement in the illustrated use case. The null hypothesis is the following:

Null-Hypothesis 1: *There is no difference in the perceived image improvement for businesses focusing on data privacy for sensitive and non-sensitive data privacy users.*

As the p-value (0.0321) was smaller than the significance level at 0.05, the null hypothesis was rejected. Therefore, we are 95% confident that the sensitivity towards data privacy does influence the perceived image improvement. The test indicated that data privacy-sensitive users perceived the business better as shown by the mean (5.99) in Table 4. Nonetheless, as already indicated in the previous analysis, the perceived image improvement is in general very high.

	n	Mean	95% conf. interval
Data Privacy ranked <= 3	14	5.29	-1.3441
Data Privacy ranked >= 5	125	5.99	-0.0684
	t = -2.3482	df = 15.948	p-value =0.0321

Table 4: Results of t-test Null-Hypothesis 1

The second two-sample test included the relationship between the sensitivity towards data privacy and the usage of services that do not promote data privacy. The null hypothesis was the following:

Null-Hypothesis 2: *There is no difference in the usage of services that do not promote data privacy for privacy-sensitive and non-privacy-sensitive users*

Given that the p-value (0.1093) was higher than the significance level at 0.05, the null hypothesis cannot be rejected. Therefore, we were 95% confident that the sensitivity towards data privacy does not influence the usage of such services/products.

	n	Mean	95% conf. interval
Data Privacy ranked <= 3	14	4.79	-1.7426
Data Privacy ranked >= 5	125	5.56	0.1940
	t = -1.697	df = 15.793	p-value =0.1093

Table 5: Results of t-test Null-Hypothesis 2

5. Discussion

Triangulating the key insights of the literature review with the semi-structured interviews and the survey allows one to validate insights from varying perspectives. The Research Question being examined is if a firm's data privacy policy provides an edge over competitors and how data privacy measures can be leveraged to gain CA. In general, the quantitative and qualitative analysis confirmed the fact that data is valuable for both consumers and businesses. Acquisti et al. (2016) discussed whether privacy equilibria exist in which the individual and the business benefit and questioned if data should be treated as a fundamental right or solely as an economic good. In the following section, the conducted primary and secondary research will be triangulated to answer the research question.

The survey indicated that data privacy is very important to consumers and that they are concerned about their personal data. The first three questions regarding personal preference for data privacy received a very high level of agreement, as described in the analysis above. Theoretically, consumers are sensitive toward data privacy, but their own preference or data privacy value assessment did not correspond to their behavior assessed in questions 6 to 9. Interviewee 3 said that users are increasingly sensitive in the realm of data and, in particular, their personal data. However, the survey showed that 78.26% do not know how their data is handled and processed which also aligns with the experts` perception. Thus, these findings contribute to the *privacy paradox.*

According to Christensen (2001), successful competitive strategies are predicated on understanding the drivers that underlie each advantage (Christensen, 2001). The drivers identified in the PESTEL analysis, namely legal, financial, ethical, and technical, were also confirmed by the interviews with experts. In this context, the legal and financial drivers were fairly closely interrelated. The interviews provided a clear picture of data privacy being a legal requirement that must be complied with. The focus here is on penalties due in the event of non-compliance. Nonetheless, undertaking measures to protect data was initially linked with investments and additional effort. The literature review clearly showed that data privacy provides added value. Hoffman (2014) stated that addressing data privacy proactively will protect the brand, provide an edge over the competition by integrating measures into products and services, and will create new services devoted to protect personal data. The use-case assessed in the survey also proved with means of 5.90 in strong agreement that enhancing data privacy has positive implications for businesses as it is preferred by consumers and respectively

improved its image. Nonetheless, how to monetize this enhancement is not clear as answers are distributed randomly. The experts also questioned whether non-privacy-sensitive users are willing to pay a surplus. However, experts said that data privacy-sensitive users respond to data privacy enhancements and regular users respond only after data breaches have occurred. According to interviewee 7, firms that do not understand the benefits of data privacy only follow data protection regulations to prevent fines and compensation claims. However, firms that have understood that data protection will and cannot be an efficiency gain, pursue it because of their long-term orientation (Lobschat et al., 2021). According to interviewee 2, transparent data flows can reduce unnecessary iterations as well as information security breaches and lastly, improve data quality.

Kannan & Li (2017) stated that key factors for creating or sustaining CA are the brand itself as well as its customers. Trust was cited in the interviews as one of the key components for businesses to generate valuable data from subjects. Thus, businesses must establish a relationship in which users share their data and perceive the brand as trustworthy as interviewee 2 explained: *"as long as you are sensitive and respectful of the data"* customers are willing to share their data. Trust and the associated transparency can be ensured via the privacy UX. Approaches for this will be elaborated further in the subsequent section. Resuming, the analysis has shown that it is of immense importance to build trust and secure it accordingly. The interviews and the survey both revealed that trust associated with regular users is weakened by breaches and that it is enormously complex to re-establish this relationship between user and company as confirmed by interviewee 3.

In the following section, a comprehensive concept will be developed to gain a competitive edge by leveraging prioritizing data privacy to address consumer concerns.

Concept

A comprehensive concept must address the identified consumers' concerns that were identified about data privacy. The survey, for instance, showed that consumers are concerned when data breaches occur as a result of inadequate security measures. Moreover, according to Martin & Murphy (2017) lack of transparency and insufficient control of personal data lead to a worse consumer perception. There are numerous scenarios in which data privacy can be enhanced. In the following, a comprehensive approach is pursued, intended to illustrate concrete measures to leverage user concerns to one's own advantage.

Data Governance Maturity Model

According to interviewees 5 and 7, data privacy is a component of data governance. Data governance defines the responsibilities in data management as well as regulations on how these decisions are appropriately implemented with the aim of maximizing the value of data assets in enterprises (Otto, 2011). Interviewee 7 stated that the firm's maturity level is crucial for identifying necessary steps to improve data governance. Data governance maturity models provide holistic frameworks in which data governance practices are continuously improved, data quality improved, trust with users enhanced, and data management effective (Varshney, 2021). Hence, implementing a data governance maturity model can help firms to improve data quality, efficiency, security, and compliance with the data governance measures. Figure 4 illustrates, for instance, the IBM data governance maturity model. Maturity can thus be measured by being unaware of the importance of data and reactive processes in the first level up to the last level which involves the reduction of redundancies and optimized measures and policies. To reach a high maturity level, measures must be defined and taken accordingly. Ultimately, the objective is to leverage new privacy measures to address user privacy concerns, thereby establishing a trusted relationship. This is taken to be crucial, as the qualitative analysis suggests.

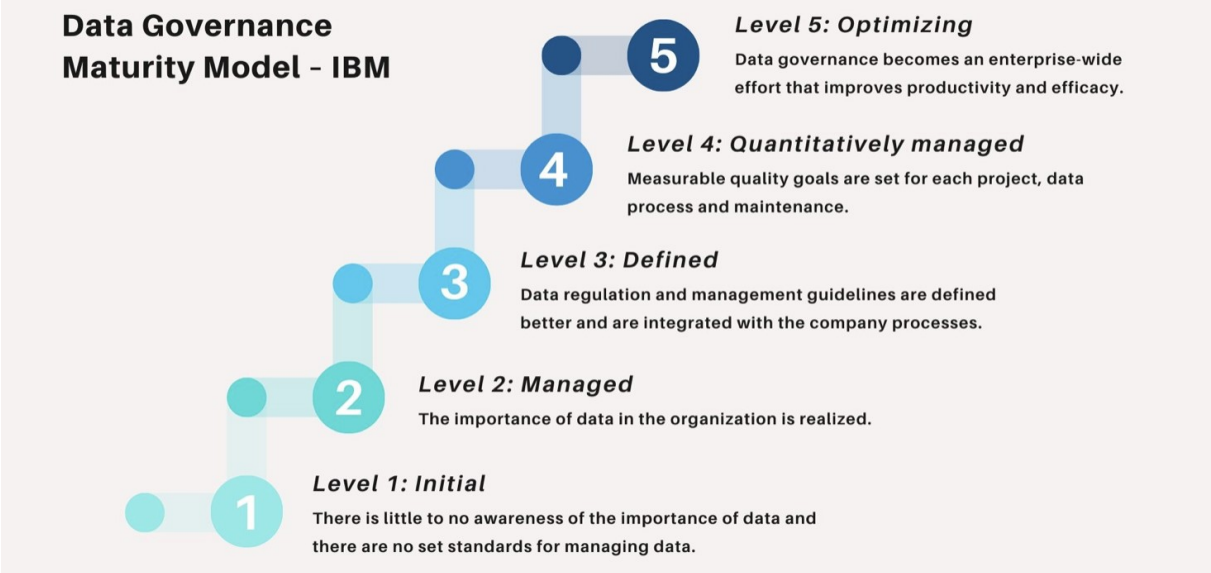

Figure 4: Data Governance Maturity Model – IBM (Taylor, n.d.)

Trust can be established by creating transparency through ethical and respectful graphical interfaces, as mentioned by interviewee 1. Interviewee 5 highlighted the importance of a pragmatic approach in which complexity must be reduced and the privacy policy being easily

understandable. Therefore, it should be easy to understand and thus comply with the GDPR. Transparency can be achieved through privacy. Privacy UX refers to the user experience of privacy-related features and functionality in a product or service. It involves designing and implementing features that allow users to understand and control their privacy settings and preferences, and that respect and protects their personal information (Sebastian, 2021). Fouad et al. (2020) state that 87.5% of 20,218 analyzed cookies do not provide a cookie policy to provide data processing purposes. Interviewee 4 said that next to the findings of Fouad et al. (2020) most consent management platforms are not compliant as it is more complex to decline or opt-out of the cookies. Hence, clearly explaining what data is collected and how it is analyzed and used in combination with obtaining consent through explicit opt-in mechanisms will build trust with the user and reduce the risk of fines due to non-compliance with the GDPR. This includes having a comprehensive and transparent data privacy policy to demonstrate the commitment toward data privacy. Although the survey indicated that users care about data privacy and value transparency efforts, it is debatable whether customer loyalty will increase despite image improvement. The findings of the interviews confirmed that non-sensitive users did not perceive or value data privacy efforts in practice, which corresponds to the privacy paradox. Moreover, providing the user with control over their data by offering opt-out possibilities of specific data collection and use practices will help a firm to be perceived as responsibly handling data. The experts agreed that designing a clear and simple consent management platform is the first step for addressing consumers' data privacy concerns and preventing fines.

Together with providing the user with a choice of opting in or out as well as a comprehensive data privacy policy, an efficient DLM is required. DLM is the process of managing the entire lifecycle of data, including generating data, securely storing it, responsibly analyzing, internally or externally disseminating the sourced data, and lastly disposing of data that is not needed or must be treated according to given retention periods. Additionally, ad-targeting will be limited due to the loss of third-party cookies. According to interviewee 2, firms must pursue an *"own your data"* strategy in which the quality of the collected first-party data plays an essential role.

Integrating data privacy into the core of business processes as *"privacy by design"* is important in the light of this thesis. As described by various experts, privacy by design refers to the concept of including privacy features at every step of the development of products and services. Integrating privacy in every stage instead of considering it as an add-on helps to protect personal data while complying with regulatory requirements. Treating privacy as an integral part of core

functionality, organizations act proactively, and when privacy breaches occur there are procedures in place. Moreover, the approach includes setting privacy by default instead of requiring users to actively opt-in or opt-out to those (Barth et al., 2022). For privacy by design to be embraced within the organization, key departments must be sensitized and trained, as interviewee 5 suggested. Interviewees 6 and 7 highlighted that next to an educated organization, a competent DPO is a crucial resource to ensure that integrating privacy measures into the design and development is independently controlled. Privacy by design is a critical element of effective data governance in which compliance with regulations is monitored by clearly established policies and responsibilities.

Lessig's (2007) principle of regulating the use of data was discussed as organizational privacy self-regulation. The interviews indicated that this is feasible through a content management platform and a concrete policy as already discussed. The principle of traceability led to PETs. Before certain technologies can be exploited, for instance, to pseudonymize data sets, a DPO is a critical capability that a company must deploy for ensuring accurate data governance. Moreover, the GDPR offers scope for innovative data sourcing methods, allowing companies to operate in the *"gray area"*. As mentioned by interviewee 2, *"the business is running ahead of the jurisdiction"*. Creative methods, such as differential privacy, were invented due to regulations. Interviewee 2 said that by randomly adding mathematical noise individual data is obscured and protected while still being able to process them.

Summarizing, businesses can benefit from privacy-enhancing measures in the following ways:

(1) Increasing customer trust by obtaining consent through an explicit opt-in mechanism on the consent management platform. Moreover, creating transparency through a comprehensive and easy-to-understand data privacy policy describing data collection and processing purposes, etc. This also entails providing users with more control over their own data.
(2) Setting up an efficient DLM will lead to increased efficiency in data analytics and reduce unnecessary data. Moreover, shaping data-efficient end-to-end processes will reduce complexity, redundancies, and effort to comply with the GDPR.
(3) Privacy by design enables organizations to answer rather proactively and not reactively when privacy breaches occur. Embedding privacy into the design improves functionality and results in a reputational gain.

(4) Implementing technical standards and best practices, such as differential privacy, offer a possibility to obscure data and henceforth protect personal information which will strengthen trust.

6. Conclusion

6.1. Conclusion

Given increasing customer concerns, data privacy is of increasing managerial importance. This thesis has strategic implications for organizational reputation, financial performance, and regulatory compliance. In this regard, company-specific factors such as motivation for data privacy, data privacy concerns, and challenges may impact decisions depending on the nature of the business and the competitive environment.

Based on the triangulation, it emerged that the main motives that drive businesses to engage in privacy at this stage are to address user concerns to gain CA by meeting legal and regulatory requirements; avoiding fines; effectively managing, governing, and protecting consumer data through DLM, data governance and the privacy by design approach; and gaining reputation.

Data privacy must not be considered merely a requirement pursued solely for regulatory and legal motivational reasons. It is crucial to understand data privacy as part of data governance to demonstrate that data privacy is an efficiency gain at all levels in a company. To some extent, companies can capitalize on consumer concerns about data privacy, with the degree of company-specific data dependency influencing the challenges and opportunities. Smaller companies may lack the capabilities and knowledge to effectively leverage customer concerns as a combination of technical skills, legal knowledge, and organizational processes are required. However, when it comes to data-driven businesses, it is essential that data privacy is considered in a holistic approach in terms of data governance. An appropriate data governance strategy can thus effectively address consumer privacy concerns and help establish trust with customers and create transparency. The introduction of an appropriate data governance maturity model enables the recording of the maturity level and the identification of required steps to achieve a higher maturity. In all cases, however, compliance with the GDPR and robust data privacy policies for the responsible treatment of personal data must be in place to reduce compliance costs.

By adopting a global data privacy policy calibrated to the highest given standard, such as the GDPR, companies can reduce complexity, for example by standardizing the handling of requests. This would ensure uniformity and stable processes and reduce compliance costs and achieve overall increased efficiency. Finally, data management can be optimized, and redundant processes eliminated. This also makes it easier to expand and, if necessary, respond minimally to local regulations.

Thus, based on the above-mentioned arguments, privacy policies can lead to unique positioning and consequently provide a competitive advantage when the measures have (1) an explicit opt-in mechanism on the consent management platform, (2) efficient DLM, (3) privacy by design, and (4) technical best practices, such as differential privacy, are properly executed with consideration to the company-specific use case as well as the internal resources and capabilities.

6.2. Limitations

By triangulating primary and secondary research, it was possible to include contemporaneous insights into current trends, preferences, risks, and benefits related to the topic of data privacy. The topic was considered holistically, which is why the insights cannot be specifically broken down into one industry or company. But as we live in a data-driven economy, where the importance of data will continue to grow, managing data privacy and consumers' privacy concerns will play a major role in the future.

The experts all work in a variety of industries and have professions, including consulting, software development, and legal representation, as founders, or data privacy managers. This allowed the research question to be analyzed from a broad perspective. Nevertheless, the interviewees were committed to data privacy, which is why the results might be affected by a selection bias due to interviewees' interest in proactively fostering data privacy within business.

The survey reached a broad spectrum of participants. However, the group was very homogeneous, as the societal average was not represented. In addition, other factors such as nationality, level of education, or profession were not surveyed, which could possibly skew findings. Nevertheless, the results may be deemed valid, since responses of a very relevant age group for data privacy were represented.

6.3. Future Research

How to achieve an edge over competitors by addressing consumers' privacy concerns is a fruitful domain for further research. It would be valuable to analyze how marketing campaigns influence consumer perception and especially how consumer behavior will change once they are more aware and familiarized with the data handling process. Furthermore, research should investigate how the ad industry will change with disabling of third-party cookies and whether the business model of free services, such as weather forecasts, can survive. Finally, it is interesting to examine how consumer participation in the data trading process could affect the market and lead to disruption of the data-driven economy.

List of References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, *30*(4). https://doi.org/10.1002/jcpy.1191

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. In *Journal of Economic Literature* (Vol. 54, Issue 2). https://doi.org/10.1257/jel.54.2.442

Adams, W. C. (2015). Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation: Fourth Edition*. https://doi.org/10.1002/9781119171386.ch19

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). The consumer-data opportunity and the privacy imperative. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Apple. (2021). Apple Privacy Policy. *Apple Inc.* https://www.apple.com/legal/privacy/en-ww/

Bala, M., & Verma, D. (2018). A Critical Review of Digital Marketing . *International Journal of Management*, *8*(10).

Barone, A. (2022). Digital Marketing Overview: Types, Challenges, and Required Skills. *Investopedia*. https://www.investopedia.com/terms/d/digital-marketing.asp

Barth, S., Ionita, D., & Hartel, P. (2023). Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Computing Surveys*, *55*(3). https://doi.org/10.1145/3502288

Belani, S., Tiarks, G. C., Mookerjee, N., & Rajput, V. (2021). "I Agree to Disagree": Comparative Ethical and Legal Analysis of Big Data and Genomics for Privacy, Consent, and Ownership. *Cureus*. https://doi.org/10.7759/cureus.18736

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3). https://doi.org/10.1016/j.ijresmar.2020.03.006

Brodherson, M., Broitman, A., Macdonald, C., & Royaux, S. (2021). The demise of third-party cookies and identifiers. *McKinsey & Company*.

https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-demise-of-third-party-cookies-and-identifiers

Brunnee, J., & Toope, S. (2006). Norms, Institutions and UN Reform: The Responsibility to Protect. *Journal of International Law and International Relations*, *2*.

Cambridge Dictionary. (n.d.). Meaning of Privacy - Business English. *Cambridge Dictionary*. Retrieved January 3, 2023, from https://dictionary.cambridge.org/dictionary/english/privacy

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). https://doi.org/10.1016/j.giq.2018.04.002

Chen, H. T. (2018). Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist*, *62*(10). https://doi.org/10.1177/0002764218792691

Christensen, C. M. (2001). The Past and Future of Competitive Advantage. *MIT Sloan Management Review*, *42*(2). https://doi.org/10.1126/science.1123633

Cinar, N., & Ateş, S. (2022). Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4041963

CMS Legal. (2022). GDPR Enforcement Tracker. In *CMS Legal*. https://www.enforcementtracker.com

Dagnino, G. B., Picone, P. M., & Ferrigno, G. (2021). Temporary Competitive Advantage: A State-of-the-Art Literature Review and Research Directions. *International Journal of Management Reviews*, *23*(1). https://doi.org/10.1111/ijmr.12242

de Winter, J. C. F., & Dodou, D. (2010). Five-point likert items: T test versus Mann-Whitney-Wilcoxon. *Practical Assessment, Research and Evaluation*, *15*(11).

Demir, N., Theis, D., Urban, T., & Pohlmann, N. (2022). *Towards Understanding First-Party Cookie Tracking in the Field* (Sicherheit'22).

Devi Prasad, B. (2019). Qualitative content analysis: Why is it still a path less taken? *Forum*

Qualitative Sozialforschung, *20*(3). https://doi.org/10.17169/fqs-20.3.3392

European Parliament, & Council. (2016). *ARTICLE 4 - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

European Parliament, & Council of the European Union. (2016). General Data Protection Regulation (GDPR). *Gdpr.Eu*. https://gdpr.eu/tag/chapter-1/

European Union. (2012). Charter of fundamental rights of the European Union. *2012/C 326/02*.

Fouad, I., Santos, C., al Kassar, F., Bielova, N., & Calzavara, S. (2020). On Compliance of Cookie Purposes with the Purpose Specification Principle. *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*. https://doi.org/10.1109/EuroSPW51379.2020.00051

Gregory, V. W. (2022). CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE. *International Organisations Research Journal*, *17*(1). https://doi.org/10.17323/1996-7845-2022-01-03

Grewal, D., Hulland, J., Kopalle, P. K., & Karahanna, E. (2020). The future of technology and marketing: a multidisciplinary perspective. In *Journal of the Academy of Marketing Science* (Vol. 48, Issue 1). https://doi.org/10.1007/s11747-019-00711-4

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2019). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. https://doi.org/10.1109/BigData.2018.8622621

Helbig, R., Höveling, S., Solsbach, A., & Marx Gómez, J. (2021). Strategic analysis of providing corporate sustainability open data. *Intelligent Systems in Accounting, Finance and Management*, *28*(3), 195–214. https://doi.org/10.1002/isaf.1501

Hijmans, H., & Raab, C. D. (2018). Ethical Dimensions of GDPR. *Commentary on the General Data Protection Regulation*, *January 2016*.

Hoffman, D. (2014). Privacy Is a Business Opportunity. *Harvard Business Review*.

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general

data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1). https://doi.org/10.1080/13600834.2019.1573501

Hox, J. J., & Boeije, H. R. (2004). Data Collection, Primary vs. Secondary. In *Encyclopedia of Social Measurement*. https://doi.org/10.1016/B0-12-369398-5/00041-4

Humby, C. (n.d.). *Think Big: Britain's Data Opportunity*. Retrieved October 25, 2022, from https://www.wandisco.com/assets/blt3981bd6367154c1b/BigDataBreakfastReport.pdf

iapp. (2021). *2021 Privacy Tech Vendor Report*. Iapp.Org. https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf

Issa, D. T., Chang, A. V., & Issa, D. T. (2010). Sustainable Business Strategies and PESTEL Framework. *GSTF INTERNATIONAL JOURNAL ON COMPUTING*, *1*(1). https://doi.org/10.5176/2010-2283_1.1.13

Jack, E. P., & Raturi, A. S. (2006). Lessons learned from methodological triangulation in management research. *Management Research News*, *29*(6). https://doi.org/10.1108/01409170610683833

Javidan, M. (1998). Core Competence: What Does it Mean in Practice? *Long Range Planning*, *31*(1). https://doi.org/10.1016/s0024-6301(97)00091-5

Jones, N. (2018). How to stop data centres from gobbling up the world's electricity. In *Nature* (Vol. 561, Issue 7722). https://doi.org/10.1038/d41586-018-06610-y

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4). https://doi.org/10.9734/bjast/2015/14975

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. In *Journal of Advanced Nursing* (Vol. 72, Issue 12). https://doi.org/10.1111/jan.13031

Kannan, P. K., & Li, H. "Alice." (2017). Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing*, *34*(1). https://doi.org/10.1016/j.ijresmar.2016.11.006

Kaplan, S. (2015). Mixing quantitative and qualitative research. In *Handbook of Qualitative Organizational Research: Innovative Pathways and Methods*.

https://doi.org/10.4324/9781315849072-54

Kraus, R. (2021). The result of Apple's new privacy policy? More money for Apple. *Mashable*. https://mashable.com/article/apple-privacy-policy-advertising-increase

Laird, J. (2022). What is a Privacy Policy? *PrivacyPolicies.Com*. https://www.privacypolicies.com/blog/what-is-privacy-policy/

Lessig, L. (2007). The Code of Privacy. In *Proceedings of the American Philosophical Society* (Vol. 151, Issue 3, pp. 283–290). JSTOR. http://www.jstor.org/stable/4599071

Lieberman, M. (2021). Is Competitive Advantage Intellectually Sustainable? *Strategic Management Review*, *2*(1). https://doi.org/10.1561/111.00000016

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, *122*. https://doi.org/10.1016/j.jbusres.2019.10.006

Marotta, V., Abhishek, V., & Acquisti, A. (2019). Online tracking and publishers' revenues: An empirical analysis. *Workshop on the Economics of Information Security (WEIS)*.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2). https://doi.org/10.1007/s11747-016-0495-4

Mehrat, S. K. (2020). Data privacy and antitrust in comparative perspective. In *Cornell International Law Journal* (Vol. 53, Issue 1).

O'Flaherty, K. (2022). Apple's Privacy Features Will Cost Facebook $12 Billion. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2022/04/23/apple-just-issued-stunning-12-billion-blow-to-facebook/

Onik, M. M. H., Kim, C. S., & Yang, J. (2019). Personal Data Privacy Challenges of the Fourth Industrial Revolution. *International Conference on Advanced Communication Technology, ICACT*, *2019-February*. https://doi.org/10.23919/ICACT.2019.8701932

Oró, E., Depoorter, V., Garcia, A., & Salom, J. (2015). Energy efficiency and renewable energy integration in data centres. Strategies and modelling review. In *Renewable and Sustainable Energy Reviews* (Vol. 42). https://doi.org/10.1016/j.rser.2014.10.035

Otto, B. (2011). Data Governance. *Business & Information Systems Engineering*, *3*(4), 241–

244. https://doi.org/10.1007/s12599-011-0162-8

Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & de Colle, S. (2010). Stakeholder theory: The state of the art. In *Academy of Management Annals* (Vol. 4, Issue 1). https://doi.org/10.1080/19416520.2010.495581

Petroff, A., & Fauser, B. (2022). So machen Unternehmen Online-Privatsphäre zum Wettbewerbsvorteil. *Think with Google*. https://www.thinkwithgoogle.com/intl/de-de/zukunft-des-marketings/datenschutz-und-nutzervertrauen/online-privatssphaere-wettbewerbsvorteile/

Porter, M. E. (1985). Competitve Advantage: Creating and sustaining competitive advantage. In *Creating and Sustaining Competitive Advantage: Management Logics, Business Models, and Entrepreneurial Rent*.

Renaud, K., & Gálvez-Cruz, D. (2010). Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. https://doi.org/10.1109/ISSA.2010.5588297

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, *35*(3–4). https://doi.org/10.1108/01409171211210154

Saunders, M, Lewis, P & Thornhill, A. (2016). Research Methods for Business Students. In *Pearson Education Limited 2*.

Scheibner, J., Raisaro, J. L., Troncoso-Pastoriza, J. R., Ienca, M., Fellay, J., Vayena, E., & Hubaux, J. P. (2021). Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis. In *Journal of Medical Internet Research* (Vol. 23, Issue 2). https://doi.org/10.2196/25120

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information and Management*, *59*(4). https://doi.org/10.1016/j.im.2022.103638

Schomakers, E. M., Lidynia, C., & Ziefle, M. (2020). All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity. *Electronic Markets*, *30*(3). https://doi.org/10.1007/s12525-020-00404-9

Sebastian, G. (2021). A cross-sectional study on improving privacy policy read rate and

comprehension via better UX/UI design. *IBIMA Business Review*, *2021*. https://doi.org/10.5171/2021.168594

Statista. (2022). *Digital Advertising worldwide*. Statista. https://www.statista.com/outlook/dmo/digital-advertising/worldwide#ad-spending

Talagala, N. (2022). Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires. *Forbes*. https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/?sh=7424939ec208

Taylor, K. (n.d.). *Data Governance Maturity Models Explained*. Retrieved December 28, 2022, from https://www.hitechnectar.com/blogs/data-governance-maturity-models-explained/

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1). https://doi.org/10.1007/s10603-018-9399-7

van Selm, M., & Jankowski, N. W. (2006). Conducting online surveys. In *Quality and Quantity* (Vol. 40, Issue 3). https://doi.org/10.1007/s11135-005-8081-8

Varshney, S. (2021, July 20). *Data Governance Maturity Models and How to Measure It?* OVALEDGE. https://www.ovaledge.com/blog/data-governance-maturity-model

von Soest, C. (2022). Why Do We Speak to Experts? Reviving the Strength of the Expert Interview Method. *Perspectives on Politics*, 1–11. https://doi.org/10.1017/S1537592722001116

Wang, H.-L. (2014). Theories for competitive advantage. *Being Practical with Theory: A Window into Business Research*.

Wolford, B. (2020). *What is GDPR, the EU's new data protection law?* Gdpr.Eu. https://gdpr.eu/what-is-gdpr/

Appendices

Appendix A: List of Interviewees

ID	Name	Position	Reason for Interview
1	Tilman Harmeling	Senior Expert Data Privacy	Constructing an overview of the connectivity between regulations, movements and the current state of data privacy
2	Robin Zederbauer	Director Competence Center Consultancy	Corporate knowledge to gain insights of data privacy measures in the industry
3	Malte Schadendorff	Software Developer	Gain deeper insights from a technical perspective
4	Edda Pernice	Trainee Data Protection Consultancy	Understand capabilities and requirements for compliance review and training
5	Christopher Schmidt	Lawyer Data Privacy IAPP Advisory Board Member CoE Expert on Data Protection	Expert on the jurisdiction. Comprehend the jurisprudence in the field of data privacy and the gaps between as-is and to-be
6	Dr. Frank Schemmel	Practice Lead International Data Privacy & Compliance	Management experience within a position and severe knowledge about the implications the GDPR has
7	Daniela Will	Data Protection Professional	Lead a data protection organization of a global corporation
8	Noah Fenell	CEO and Founder of DataEarn	First-hand experience in the data subject request process allowing individuals to access data stored from big tech.

Table 6: List of Interviewees

Appendix B: Interview 1 Summaries Key Insights

Interview 1:

Interviewee: Tilman Harmeling

Occupation: Senior Expert Data Privacy

- I mean with the Google Privacy Sandbox and other browsers, third-party cookies are being eliminated more and more, which makes the market super difficult for publishers and the ad tech industry in general.
- Apple with the introduction of the ATT and not sharing the IDFA has, of course, created a walled garden where they make it possible to efficiently collect and use this first-party data.
- Privacy has interventions in mainly 2 big areas and one is just the legal side and the other is the marketing side. From the legal side, you want to achieve the reduction of stickers and penalties. You have some very large budgets and those are designed to grab data from end users. Yes, for various campaigns, remarketing, retargeting, and conversion optimization.
- 2 big goals why companies should do data protection. One is they need to do it, so kind of reduce those penalties and the other is if they do it, then you still need to do it too. Trust relationship. Build a trusted environment with the end user to at least a little gather a bit more data or, respectively.
- The advantages are simply that one now builds up the trust to perhaps also long-term, benefits like customer loyalty, but also that they could simply be willing to share their data. That you really transparently show what happens with the data.
- To build trust, a responsive web design company needs a solid privacy UX for the user journey, which consists of the Consent Management Platform, the Data Privacy Policy, and an efficient Data Subject Request.
- Contextual consent is one way to optimize the user journey and show what happens to the data in the exact moment but also differential privacy where you obscure the data
- Google tries to group certain groups if no consent is given and to form cohorts with approximately the same interests. For this, data is masked in the background by pseudonymization, masking, or by differential privacy with a mathematical noise. Thereby one can create a kind of privacy.
- Regulations can become an innovation blocker, but also offer an opportunity to optimize the maximum of what is possible regarding the legal requirements.

- Trust: The person who trusts your company shares their data with you. It is also the case that trusted companies get their data from customers. You can also spin innovations about that.
- With publishers, you don't know what you're opted in for and it's super hard to reject the banner.
- If we limit too much now, then the services that are offered for free will disappear. That is the trade-off - do you want to interfere in this service?
- The cookie duration is limited, which simply reduces the effectiveness of the marketing measures and the EU simply loses billions in tax revenue.
- The EU wants to crack down on walled gardens and is considering whether it is not the right of all companies to have access to customer data.

Appendix C: Interview 2 Summaries Key Insights

Interview 2:

Interviewee: Robin Zederbauer

Occupation: Director M^2 Business Consulting Competence Center Manager GDPR

- Accompaniment of Cookie Banner Roll-Out and calculation of the value for the click on accept all at Consent Banner.
- You must deal with data protection at some point and in Germany, you don’t come around to data privacy.
- A variety of reasons to protect consumer data.
- All companies will become more and more customer-centric no matter whether that is now an Apple or the like. All look only at the customer and develop actually to the customer and on what do they develop?
- Data privacy is crucial to continue to collect data from customers and therefore this customer data protection is of course particularly important. What you should pay attention

to so that the customers continue to disclose the data. And at the end of the day data protection is important because of course you want to protect the customer data and as long as you are sensitive and appreciative of the data, we will continue to get data from customers, and therefore we can develop.

- Financially, because expertise does not exist.
- Process analysis for the data structure in the company.
- Trust is the key, which makes responsive web design possible.
- Creating a trust can be done with a visual theme like the policy page or the cookie draw, where the customer is told again, ok we collect your data if you agree. You can decide freely and then also again give a transparent overview, ok what do we do with the data - how is it tracked?
- Marketing Spendings are higher due to lower ROAS because not all data can be used and so e.g., fewer customers can be acquired.
- Corporations want to do their core competence and not only data protection – the automotive company has the core competence to produce cars.
- Apple has made online marketing expensive through ATT and IDFA, creating walled gardens.
- After individuals or people become more and more sensitive in the context of data and especially their personal data - meanwhile health insurance companies can adjust health insurance premiums with credit card data, e.g., when buying cigarettes.
- Business methods are more innovative and more advanced than jurisdiction, where there is no plaintiff there is no judge.
- There is a competitive advantage through data, which is why all companies pursue the first-party strategy, i.e., own your data, group strategy depends on the brand. The trade-off between benefit and risk.
- The USA has greater opportunities to use data, but in Europe, you simply can't get around data protection.
- Is of course an innovation blocker because people are afraid of legal consequences
- The difference in the company: The data protectors in a company always say no, no, no, when it comes to data privacy because it is of course the safest way, but online marketing or now Data Scientists who would like to use the data they would always like to shout yes, yes, yes, when collecting data.
- Gray area allows taking a calculated risk (example. Newsletter doubles opt-in with an email

address or lead magnet (checklists) by costless purchases, to build so technically that data trespasses cannot be traced exactly. Consentless tracking for sub-areas where case law is not yet so far ahead).

- Stray effect: iso-certification help analyze data streams and reduce potential duplication and inefficiencies. This can identify what is needed, whether you might be able to save on licensing fees or need certain tools and need to train staff.

Appendix D: Interview 3 Summaries Key Insights

Interview 3:

Interviewee: Malte Schadendorff

Occupation: Software Developer

- So of course, we have a lot to do with that because we have to take certain things into account when creating our software, especially due to GDPR or DSGVO, and also with regard to Privacy by Design.
- 2 branches of Google, for example in Europe, had so-called standard contractual clauses with the company headquarters in the USA where it was stated that, for example, the headquarters in the USA is obligated to pay damages to the branch in Europe -> not legally valid always in the gray area on the road, even concerning the fact that data has been shared with the USA.
- For 2 customers who actually got a warning, because in these web pages Google funds were included.
- We are affected by the development. Customers are responsible for their own compliance

with data protection regulations, but we provide guidance and technical background.

- Motives are clearly regulatory.
- More sensitive users are willing to pay more for it and that can lead to a competitive advantage, but standard users are not.
- A moral idea to write data protection big -> unsure if this is such a big driver in the business environment.
- Loyalty increases and marketing is positive if the measures are implemented correctly
- On the one hand, you have of course increased costs which are quite clear so whether it is now through penalties or simply by the fact that you have to take care of these things. A data protection officer has to be hired and developments have to be taken care of, which increases the effort for us but also for the customers to control.
- For customers, the process is more complex, cookie banner that we would not have without GDPR at all, and I think many people do not understand why they now always click on accept reject, super opaque, and dark patterns exist.
- Tension: a combination of still making it as user-friendly as possible and still privacy friendly.
- Skills: Data privacy by design - the development of software so from the beginning you make sure that you are as data sparse as possible and take data privacy into account from the beginning in the processes.
- It needs legal support because software developers can't do that.
- Technological knowledge to be able to assess where the traps for breaches are.
- Google Privacy Sandbox and Walled Garden will of course lead to big players having data sovereignty.
- I can say again from my point of view as a data protectionist that this has a big effect. I don't know how it is with people who are not so tech-savvy.
- Very hard to restore that credibility. So, for example, WhatsApp with end-to-end encryption. If another company had said that now, maybe people would believe it more than they do now with WhatsApp, and I think also always the question is what a company announces for marketing reasons and what really happens technically in the background. So that the same thing doesn't happen with data protection as with greenwashing.

Appendix E: Interview 4 Summaries Key Insights

Interview 4:

Interviewee: Edda Pernice

Occupation: Trainee Legal Consultancy

- I think starting off, I would say the main reason is obviously legal because it is requirement for organizations that fall under the scope of the GDPR. They have to follow the GDPR. The GDPR requires privacy by design and default.
- I was going to say that the second motive is definitely financial because of imposing fines.
- Big social media corporations can for example afford the fines. I would say it's so high that the 2% or 4% of annual revenue or like 10 to 20 million USD is too less. They can generate more value from the data.
- Socially the reputation is at risk if failing to respect the GDPR.
- But I think obviously the benefit is that they benefit from it. People who do have knowledge about data privacy, like me, are influenced by businesses complying with the GDPR. I don't know if the average consumer values that fact and say I'm going to use this app or this software because I know that they're compliant compared to somebody who don't. I think that the average person does not necessarily Care. I think they take it for granted that my data is going to be used in order to use the product.
- Disadvantages relating to data privacy are the associated investments. Training and consultancies cost, but in the end, it is a long-term investment.
- A lot of them are not aware of how to properly manage data and might not even know what their requirements are and like what it means in practice.
- Encryption is basic and there can be so much more. I mean it does not necessarily have to be super technical, there obviously have to be both organizational and technical measures in place. So obviously you have encryption, and authentication, but they also have to consider legal measures.
- Your repetition improves because it shows that you sort of care about your customer, care about their personal data, and again for somebody knowledgeable in the area, you are keener to trust. But again, I don't know if that's something that the average consumer values.
- Expanding in other countries is easier.

- I think it's definitely a big disadvantage for small businesses to sort of make it so hard. Ad tech industry relies on data and the moment that ads are not running targeted the way they, you know, used to.
- I can see why smaller businesses might find it harder to be compliant. It is too complex for them to implement the measures. The knowledge and the IT infrastructure are missing.
- VPN, for example, has its costs, state-of-the-art devices have their cost and sometimes the technical requirements can be a cost.
- You're supposed to have retention periods - storage limitation is a disadvantage for businesses.
- Accepting the cookies is highlighted and the rejecting is just fitting in the background that's also Not, you know, not considered compliant.
- There is definitely room for improvement in the GDPR itself.

Appendix F: Interview 5 Summaries Key Insights

Interview 5:

Interviewee: Christopher Schmidt

Occupation: Lawyer Data Privacy

- The regulatory focus currently predominates, or at least traditionally predominates.
- These are all nice attempts, but you can see that is being taken out of the financial side, and there is the second part of the reputation risk. So that's the reputation damage, what you don't want to risk.
- Companies want to leverage data and say they’re sitting on a stock of value. Let's take advantage of it.
- If we don't take advantage of the opportunity now, we're going to be behind on AI. That's why your own data set needs to be ideally aligned.
- The greatest possible value is simply extracted from the data, so that we really don't simply bear an innovation disadvantage, even perhaps as a location in Europe.
- I think the advantage for companies is sometimes not visible at first glance. But I think it

becomes visible when the effort for later adjustments is reduced. For this, data life cycle management is of utmost importance.

- But also in the meantime, we are out of the time that data protection is perceived as paralyzing and only costly. I am firmly convinced that data protection offers an advantage in the long run and can act in a cost-saving and sales-maximizing way through privacy by design and ultimately strengthen trust in the brand.
- Apple has positioned itself well and sold the ATT and IDFA to the customer. The advantage of the right strategies is omnipresent if one uses them meaningfully
- Data processing should remain understandable and is characterized by complexity in this era. It should be more pragmatic and clear thinking - a simple page with simple buttons or explanations or ways to configure things.
- An 18-page privacy policy is more of an imposition than creating transparency and that can't be serious.
- On the enterprise side, however, I think privacy for processes is a way to get it right.
- Deletion concepts are not in place. Everybody wants to collect, collect, collect, and nobody has a good penetrated data life cycle management, especially for deletion and the simple collection of only necessary data. Data is only about keeping it, using it, and not giving it away again.
- Companies have not really integrated data protection, leaving 2 or 3 people to carry the burden alone, making the process less than ideal.
- Dark patterns in consent management.
- Of course, it's extra work, but data protection is an advantage if you do it right and keep at it.
- The trade-off is between fine risk and compensation, but in itself, it is firstly additional effort and rather important in the long term.
- If certain basic concepts of Privacy by Design are not understood, I am not sure if it is an innovation driver.
- The topic is in my view a mood killer in the departments and therefore rather a brake on innovation. The roles must be perceived as really important.

Appendix G: Interview 6 Summaries Key Insights

Interview 6:

Interviewee: Dr. Frank Schemmel

Occupation: Data Guard with experience in labor law, formerly in management, now compliance product responsible, IAPP.

- Establish data protection practices in Germany.
- GDPR had the objective of harmonizing the law. To a large extent, it has succeeded. It serves as a framework for all 27 EU member states and has become an international role model. Basic principles such as data minimization and right of access, as well as regulatory and organizational measures, are the basic building blocks. Since its introduction, landmark case law and decisions have also laid down clear guidelines for practice.
- The supervisory authorities have executive power and can distribute fines. However, no legislative power.
- Especially in Germany, the value of data is immense.
- The GDPR is definitely not a brake on innovation because it is really worded in a very technology-neutral way. There are also simplifications in many areas. For example, there is a generous exception for research, where, after all, there is always innovation. When privacy by design is lived. When new software or whatever is launched on the market and data protection is integrated from the outset, there are empirical studies that show that not only risks are avoided, i.e., risks of fines, but also reputational risks and liability risks. But conversely, you also strengthen the trust of the user of the consumer, which is becoming increasingly important in digital business models today, and despite data-driven business models. Trust is one of the highest assets.
- Data governance is becoming increasingly important. Who owns the data, and what is the data flow? Data protection is a building block here.
- A competent data protection officer, who is involved in all processes and, in the best case, is employed internally, simply leads to higher compliance. Nowadays, to do proper data protection management you should also invest money in IT, but what I rather mean is to anchor data privacy as a process in the company from the very beginning.
- If the data protection officer is only involved in the process at the end, this only leads to additional work to make the process's data secure. If this is ignored, the fines do not pay off in the long run.

Appendix H: Interview 7 Summaries Key Insights

Interview 7:

Interviewee: Daniela Will

Occupation: Lead of data protection organization of a global corporation

- The organization must be globally and practicably auditable, and the maturity level should be taken as the decisive factor.
- Now it depends on whether a company has understood what benefit data protection brings if it has not understood it. The actual benefit, then it makes data protection exclusively in terms of consumer protection data but the consumer then exclusively due to the regulatory and the sanctions to be feared or also claim damages and that goes into the money or leads to reputational damage.
- Businesses who have understood that data protection is basically data governance, and that data transparency will not be an efficiency gain. They do this because they have understood that if they have transparent data flows, they realize where they have repetition iteration that only money. Also say where appropriate have been uncertainties they have lured, have information security gaps.
- I look at processes and I may. Confirm probably already had somewhere else where I collect data multiple times for example. That creates an integrity issue, but the picture also creates an efficiency issue because I now have multiple efforts.
- Yes, now the large one in things information security in the enterprise does not come at all that they make a large information security problem, which I do not see at all. In this respect, they don't even notice the conclusion at this point. Only with annual temporally clear delay notice that they get lost in patents.
- DPO looks at the process to track the data with the right glasses and is similar to the quality function often decoupled to remain independent.
- Privacy by Design, if you think that around, your privacy from the beginning within the product development or in the process. New reconstruction with and not to come in the end effect on the fact that at the end the data protection official is brought in and then it becomes apparent that everywhere gigantic for British for example arise.
- You have to start at the beginning of a process development boss process development. This price looks at design in view.

- Is a project of our company that always goes over several years and you need complex structures and infrastructures, really, you also need the process and experts.
- Data is the money. It is so incredibly valuable.
- In that, I create transparency in the processes you can only exploit the added value.
- What many have forgotten data costs money – licenses.

Appendix I: Interview 8 Summaries Key Insights

Interview 8:

Interviewee: Noah Fernell

Occupation: Senior Expert Data Privacy

- Leverage article 21 where you have ownership and people can buy this type of data. We know they sell this type of data. This data might be very valuable for some sort of brand or some sort of advertising agency. The hard part with us though is used to get, you know, to a certain amount of scale, right? So, we need to get like a million users on our platform to enable a marketplace for data.
- They store the data and don’t send it, so it might be a subject to penalty
- I look at it as you know, you can use it to your advantage, right? Like if you know what's trying to be targeted towards you like you're a step ahead of, you know, the advertiser or if you like this, you know, type of content. You know, you can kind of be more aware as kind

of like a human being of what's forcing you to, you know, stay on Instagram and things like that.

- Motives for companies, you know, care about data privacy is trust with your users. Once that trust is broken or once you've exposed, you know, my position or my data. That's a valuable asset that you know, they're just kind of let free. You're uploading your subconscious into these apps.
- Leverage the information to identify the business history, followers, and performance. you see how you were operating and use it as a strategic advantage. These kinds of bigger tech companies are trying to essentially not allow you to use all this data to your advantage.
- Privacy UX and Privacy subject request needs to be more transparent
- Mid-tier companies are afraid as they don't have the infrastructure
- We've shown how much money you make through Snapchat add revenue
- Big corporations create their own ecosystem in which they own the data
- There are all these algorithms that are happening behind your screen, but you don't necessarily know how they work, but you know they exist. So, I always think transparency makes things more efficient
- I know what type of content you're going to be showing me. I don't necessarily know exactly how, but it's still way better than me just seeing on my phone and not actually having a record open at all and there should be more knowledge about this
- I think now definitely the people that are more tailored towards privacy are. But I think once you create a monetization aspect around it, it's going to spread like wildfire to just people, not within the privacy space, because everyone loves making more money, right?

Appendix J: Correlation Table

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13
Q1	1.00												
Q2	0.57	1.00											
Q3	0.70	0.56	1.00										
Q4	-0.32	-0.31	-0.44	1.00									
Q5	-0.16	-0.25	-0.33	0.50	1.00								
Q6	0.04	0.15	0.18	-0.10	-0.38	1.00							
Q7	0.40	0.40	0.39	-0.34	-0.16	0.04	1.00						
Q8	0.10	0.12	0.18	-0.05	-0.26	0.59	0.02	1.00					
Q9	0.12	0.17	0.15	-0.11	-0.16	0.39	0.26	0.42	1.00				
Q10	0.24	0.26	0.38	-0.25	-0.15	0.17	0.31	0.14	0.27	1.00			
Q11	0.32	0.26	0.42	-0.26	-0.14	0.11	0.28	0.13	0.17	0.66	1.00		
Q12	0.06	-0.06	-0.06	0.05	0.12	-0.25	0.13	-0.35	-0.28	0.11	0.10	1.00	
Q13	0.21	0.12	0.13	-0.05	0.05	-0.28	-0.03	-0.30	-0.36	-0.09	-0.07	0.60	1.00

Table 7: Correlation Table

Appendix K: Graphical illustration correlations

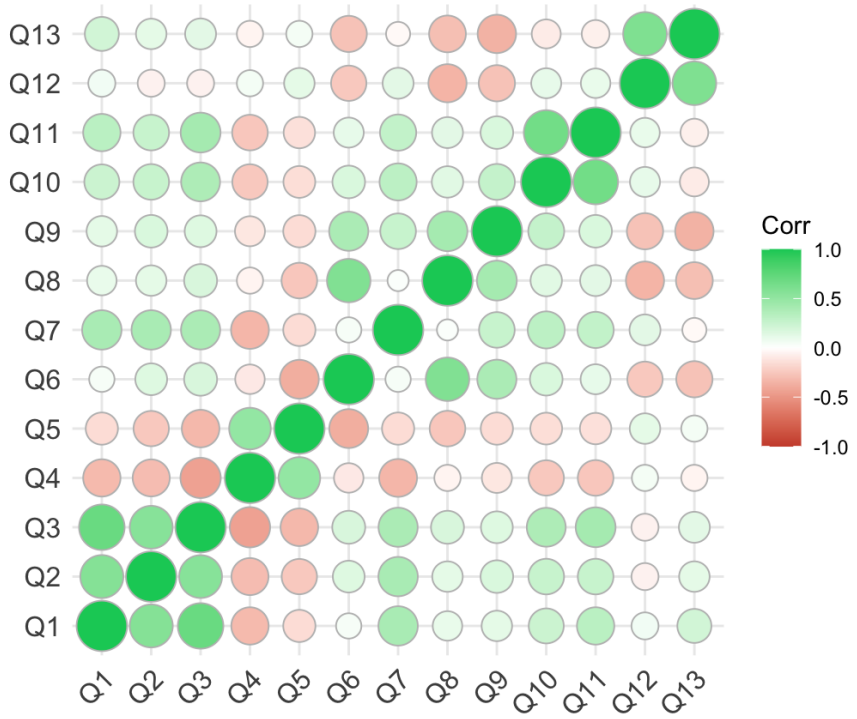

Figure 5: Graphical illustration correlations