

Lappeenranta-Lahti University of Technology LUT

School of Business and Management

Master's Degree Programme in International Marketing Management

Master's Thesis

**CONSUMERS' ATTITUDES TOWARDS DATA PRIVACY:
DIFFERENCES BETWEEN YOUNGER AND OLDER CONSUMERS**

Mia Nummila

2019

1st examiner: professor Asta Salmi

2nd examiner: professor Juha Väättänen

ABSTRACT

| | |
|---------------------|---|
| Author: | Mia Nummila |
| Title: | Consumer's attitudes towards data privacy: differences between younger and older consumers |
| Faculty: | School of Business and Management |
| Master's Programme: | International Marketing Management (MIMM) |
| Year: | 2019 |
| Master's Thesis: | Lappeenranta-Lahti University of Technology LUT 63 pages, 31 figures, 2 tables, 3 appendices |
| Examiners: | Professors Asta Salmi and Juha Väättänen |
| Keywords: | Data privacy, online privacy, data exchange, personal data privacy, data protection legislation |

This study was conducted to investigate consumers' attitudes towards data privacy. As data privacy is a growing concern, there have been studies on consumers' attitudes towards data privacy over the years. Previous research results suggest that age has an impact on consumer attitudes towards data protection. The purpose of this study is to compare the attitudes of younger and older consumers to find significant differences.

The research data was collected using an online questionnaire and the results of the survey were analysed with variance analysis (ANOVA). The results of the analysis show that there are differences in the attitudes of younger and older consumers to data protection. Younger consumers see sharing of personal information online as a part of the modern economy and unlike older consumers do not set such high importance on the consents whenever their activities are being tracked online. Similarly, the younger consumers are not as worried about single data breaches as older consumers. In addition, younger consumers take more proactive action such as adjust their privacy settings and use data security software's to protect their personal data where older consumers shift this responsibility to companies.

It is expected that consumers' growing awareness and critical attitude towards data privacy will be an increasingly important factor in the processing of personal data, and it is important for the consumer product companies to take this into account when designing their marketing strategies. Data protection requirements should not be seen as a burden, but as an effective way to build consumer trust in the company.

TIIVISTELMÄ

| | |
|-----------------------|---|
| Tekijä: | Mia Nummila |
| Otsikko: | Kuluttajien asenteet suhteessa tietosuojaan: eroavaisuudet nuorempien ja vanhempien kuluttajien välillä |
| Tiedekunta: | Kauppakorkeakoulu |
| Maisteriohjelma: | International Marketing Management (MIMM) |
| Vuosi: | 2019 |
| Pro Gradu -tutkielma: | Lappeenrannan-Lahden teknillinen yliopisto LUT 63 sivua, 31 kuvaa, 2 taulukkoa, 3 liitettä |
| Tarkastat: | Professorit Asta Salmi ja Juha Väättänen |
| Avainsanat: | Tietosuoja, yksityisyys verkossa, tiedonvaihto, henkilökohtainen tietosuoja, tietosuojalainsäädäntö |

Tämä tutkimus tehtiin kuluttajien asenteiden selvittämiseksi suhteessa tietosuojaan. Koska tietosuoja on kasvava huolenaihe, on vuosien varrella tehty tutkimuksia tähän liittyen. Aiemmat tutkimustulokset viittaavat siihen, että iällä on vaikutusta kuluttajien asenteisiin suhteessa tietosuojaan. Tämän tutkimuksen tarkoituksena on verrata nuorempien ja vanhempien kuluttajien asenteita merkittävien eroavaisuuksien löytämiseksi.

Tutkimusaineisto kerättiin verkkokyselylomakkeella ja kyselyn tulokset analysoitiin käyttäen apuna varianssianalyysia (ANOVA). Analyysin tuloksista käy ilmi, että nuorempien ja vanhempien kuluttajien asenteissa suhteessa tietosuojaan on eroja. Nuoremmat kuluttajat kokevat henkilötietojen jakamisen verkossa osaksi nykytaloutta. Toisin kuin vanhemmat kuluttajat, nuoremmat kuluttajat eivät aseta yhtä suurta merkitystä suostumuksille aina, kun heidän toimintaansa seurataan verkossa. Nuoremmat kuluttajat eivät myöskään ole yhtä huolestuneita yksittäisistä tietosuojarikkomuksista kuin vanhemmat kuluttajat. Lisäksi nuoremmat kuluttajat tekevät enemmän ennaltaehkäiseviä toimia suojellakseen henkilötietojaan, kuten muokkaavat tietosuoja-asetuksiaan ja käyttävät tietoturvaohjelmistoja, kun taas vanhemmat kuluttajat siirtävät tämän vastuun yrityksille.

On oletettavaa, että kuluttajien kasvava tietoisuus ja kriittinen asennoituminen on jatkossa yhä merkittävämpi henkilötietojen käsittelyä ohjaava tekijä ja on tärkeää, että kuluttajatuoterytykset ottavat tämän huomioon suunnitellessaan markkinointistrategioitaan. Tietosuojan asettamia vaatimuksia ei suinkaan tulisi nähdä taakkana, vaan tehokkaana keinona rakentaa kuluttajien luottamusta yritystä kohtaan.

TABLE OF CONTENTS

| | | |
|----------|--|-----------|
| 1 | Introduction..... | 1 |
| 1.1 | Background | 1 |
| 1.2 | Statement of the problem..... | 2 |
| 1.3 | Research questions and objectives..... | 4 |
| 1.4 | Main concepts and delimitations..... | 5 |
| 1.5 | Conceptual framework..... | 6 |
| 1.6 | Structure of the thesis..... | 7 |
| 2 | Consumers' attitudes towards data privacy..... | 8 |
| 2.1 | Online privacy..... | 8 |
| 2.1.1 | Data security and privacy..... | 9 |
| 2.1.2 | Ethical aspects of data security and privacy..... | 10 |
| 2.1.3 | Concerns over online privacy..... | 11 |
| 2.2 | Data exchange | 11 |
| 2.2.1 | Data collection and web analytics | 12 |
| 2.2.2 | Personalisation..... | 13 |
| 2.2.3 | Attitudes towards data exchange | 13 |
| 2.3 | Personal data privacy | 14 |
| 2.3.1 | Building consumer trust through data security and privacy..... | 15 |
| 2.3.2 | Perceptions of personal data privacy..... | 16 |
| 2.4 | Data protection legislation | 17 |
| 2.4.1 | EU's data protection laws..... | 18 |
| 2.4.2 | Awareness of specific data protection laws..... | 20 |
| 2.5 | Summary of the literature review..... | 20 |
| 3 | Research design | 21 |
| 3.1 | Research methods..... | 21 |
| 3.2 | Hypothesis testing..... | 22 |
| 3.3 | Data collection..... | 23 |
| 3.4 | Sample selection..... | 24 |
| 3.5 | Research process | 24 |
| 4 | Results and discussion | 25 |
| 4.1 | General description of data | 25 |
| 4.2 | Descriptive statistics | 25 |
| 4.2.1 | Online privacy concerns..... | 25 |

| | | |
|----------|---|-----------|
| 4.2.2 | Attitudes towards data exchange | 29 |
| 4.2.3 | Perceptions in personal data privacy | 35 |
| 4.2.4 | Awareness of specific data protection laws | 43 |
| 4.3 | Analysis of variance | 45 |
| 4.3.1 | Difference in concerns over online privacy | 46 |
| 4.3.2 | Difference in attitudes towards data privacy | 47 |
| 4.3.3 | Difference in perceptions of personal data privacy | 49 |
| 4.3.4 | Difference in awareness of specific data privacy laws | 50 |
| 4.4 | Summary of findings | 51 |
| 4.5 | Discussion | 52 |
| 5 | Conclusions, limitations and suggestions for further research..... | 54 |
| 5.1 | Summary..... | 55 |
| 5.2 | General conclusions | 55 |
| 5.3 | Limitations..... | 56 |
| 5.4 | Suggestions for further research | 58 |
| | References..... | 59 |

Appendix 1: Web-questionnaire

Appendix 2: Survey results

Appendix 3: ANOVA results

LIST OF TABLES

| | |
|---|----|
| Table 1: Research objectives | 5 |
| Table 2: Summary of the literature review | 20 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1: Conceptual framework..... | 6 |
| Figure 2: Structure of the thesis..... | 7 |
| Figure 3: Research process | 24 |
| Figure 4: Personal information on computer, smartphone or tablet can only be accessed with a permission | 26 |
| Figure 5: Confidentiality of emails and instant messages is guaranteed | 27 |
| Figure 6: Tools for monitoring activities can only be used with a permission | 28 |
| Figure 7: The level of concerns over data privacy online | 29 |
| Figure 8: Sharing data and personal information online is part of modern economy | 30 |
| Figure 9: Exchange of personal information is essential for the smooth running of modern society | 30 |
| Figure 10: I am happy with the amount of personal information I give to companies | 31 |
| Figure 11: I feel more aware of how my data is used and collected than in the past..... | 32 |
| Figure 12: I feel more comfortable with the idea of exchanging some personal data with companies than I did previously..... | 32 |
| Figure 13: Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy..... | 33 |
| Figure 14: The average level of control in specific areas of data exchange | 34 |
| Figure 15: Actions taken to protect personal data..... | 36 |
| Figure 16: Activities that consumers would allow companies to analyse by using software programs in order to send targeted advertisements or coupons..... | 37 |
| Figure 17: Factors that increase consumers trust in companies in protecting personal information when online..... | 38 |
| Figure 18: I am more likely to purchase from companies that I believe protect my personal information..... | 39 |
| Figure 19: I avoid purchasing from companies that I do not believe protect my personal information..... | 40 |
| Figure 20: Even a single data breach would negatively impact my likelihood to buy from a company in the future | 40 |

| | |
|--|----|
| Figure 21: I would be forgiving of company that had one single data breach of my personal data as long as they quickly addressed the issue | 41 |
| Figure 22: I believe most companies are adequately protecting my personal information..... | 42 |
| Figure 23: I know which companies protect my personal information | 42 |
| Figure 24: Awareness of the General Data Protection Regulation (GDPR)..... | 44 |
| Figure 25: Awareness of the ePrivacy Regulation (ePR) | 45 |
| Figure 26: Analysis of variance in question 4..... | 46 |
| Figure 27: Analysis of variance in question 5..... | 47 |
| Figure 28: Analysis of variance in question 6..... | 47 |
| Figure 29: Analysis of variance in question 7..... | 48 |
| Figure 30: Analysis of variance in question 11..... | 50 |
| Figure 31: Analysis of variance in questions 12 and 13 | 51 |

ACKNOWLEDGEMENTS

Writing my thesis has been a challenging yet rewarding task. It has taken many hours and a plenty of coffee to finish this job. During this process I have learned a lot, not only academically but also about myself.

I would like to express my gratitude towards all the people who have been a part of this journey. First and foremost, I would like to thank you my friends and family, who have motivated me and kept a sense of humour when I had lost mine. I would also like to thank my supervisor Asta Salmi, for the help to get my research focus and giving me helpful tips for finalising my thesis.

Lastly, I would like to express my appreciation to the academic staff and my fellow students in the Lappeenranta-Lahti University of Technology LUT for the great time during my master's studies.

Helsinki 3.3.2019

Mia Nummila

1 INTRODUCTION

This research is conducted to identify differences and similarities in attitudes towards data privacy between younger and older consumers. The introduction chapter will present the background of the research as well as statement of the problem. In reflection to the research problem, the research question and objectives are given to justify the more specific goals the research aims to cover. Finally, the structure of the research paper is presented to give the reader a general picture of the upcoming.

1.1 Background

Since the advent of the Internet, there has been an exponential growth in the production of data and the amount is only expected to grow as more and more, electronic devices are connected online (Baker 2018). The popularity of mobile applications, e-commerce, and social media sites proves the benefit that consumers are enjoying from information and communication technologies (Romanosky & Hoffman & Acquisti 2014). The technological developments and increase in computing power and data storage capacity, have provided the opportunity for marketers to generate large amounts of data about their customers (Hazari & Brown 2013, Tene & Polonetsky 2012). Thus, data has become a source of submerge economic and social value for the global economy (Polonetsky 2013).

According to Chris Combemale (2017), customers prefer to receive personalised advertisements from above any other type of content and data is the only way marketers can offer the relevance they demand. Data comes from interactions with a brand (first-party data) and a range of other different sources (second- and third-party data). By combining different data sets, marketers can improve the relevancy of their advertising. Lindsay Tjepkema (2018) says data-driven marketing has become a fundamental part of advertising and overall business strategy. Insights pulled from the analysis of big data allows to form predictions about customers future behaviours. Both consumers and businesses benefit from the personalised marketing, clear-cut clarity, multi-channel experience, refined customer experience and better product development that are made possible with only data-driven marketing.

At the same time, the amount of personal data collected and the uncertainty of how it is used and shared has raised security and privacy concerns among consumers (Kaushik 2007, 25). Consumers feel they have lost control over the sharing of their personal information and are concerned about

the possible misuse of their data (Pingitore & Vikram & Cavallaro & Dwivedi 2017). Since 2005, an estimated over 2,800 data breaches have occurred with 543 million records being lost (Romanosky & Hoffman & Acquisti 2014) The problems with customer data were highlighted in Facebook's data leak (O'Reilly 2018), where the social networking site broke its own privacy policy by transmitting identifying information to multiple of advertising and Internet tracking companies (Steel & Fowler 2010). Data breaches have become one of the biggest problems for companies (Ayyagari 2012) and any unauthorised access or inadvertent disclosure of that information can have severe consequences (Steel & Fowler 2010). The problem lies on companies building detailed databases on people in order to track them online (Steel & Fowler 2010).

Due to threats to personal data, consumers are taking data privacy seriously (Denham 2018) and this has affected consumers' willingness to share information to companies (Chellappa & Sin 2005). For consumer product companies to be trustworthy in the eyes of their customers, the companies need to be able to ensure that their information is carefully handled and protected (Uzialko & Writer 2018, Ridley-Siegert 2015). Companies need to meet the consumer expectations regarding data privacy and data security, where "data privacy" refers to precaution's companies take in the ways they use and share consumer data, and "data security" refers to the precaution's companies take to prevent others from stealing consumer data (Conroy, P. & Milano, F. & Narula, A. & Singhal, R. 2014).

The governments around the world have created strict data privacy regulations to balance the customer's right to privacy with the legitimate interests of companies wanting to serve them better (DMA 2018). The law makers aim to increase the effectiveness of the right to privacy and to put individuals in control of their own personal data (Oldwick 2017). The General Data Protection Regulation (GDPR) came into force in May 2018, bringing new obligations to marketers. In the future, companies should only collect information about their customers they need to in order to do a specific job, and when they got it they need to include restrictions on how to use it and delete the data when they no longer need it (O'Reilly 2018).

1.2 Statement of the problem

The regulatory compliance and operational safeguards are necessary, but the companies should also listen to their customers. Consumer product companies may not be completely aware of how much is required of them for consumer trust around data privacy and security. By understanding consumers' attitudes towards privacy and adapting the best practices into their operational standards and marketing strategies, companies increasingly build consumer trust and brand loyalty.

There are some researches made over the years on consumers' attitudes towards data privacy. Direct Marketing Association (DMA) has conducted a study in 2012 and again in 2017 on how consumers feel about privacy and their data in UK. Their latest edition was conducted against the backdrop of the fourth industrial revolution of rapid innovation in technology and major modernisation of the legislative framework especially referring the GDPR. Deloitte University Press prepared an article on data privacy and security. *Building consumer trust – protecting personal data in the consumer product industry* is based on two Web-based surveys conducted in August 2014. Other survey polled 70 US consumer product industry executives and managers, the other 2000 adult US consumers. The research also included executive interviews. Another study by Deloitte University Press, *To share or not to share – What consumers really think about sharing their personal information*, encompasses the results of J. D. Power and Associates/SSI consumer survey conducted in 2012 and 2014 and Deloitte/SSI consumer survey conducted in 2016.

These studies are important in order to learn what the consumers think about data privacy. According to Deloitte University Press' study, recent data breaches have heightened consumer's awareness of data security and privacy, therefore companies need to reassure consumers that they are protecting the privacy and security of their personal information. Furthermore, the attitudes towards data privacy seem to vary by age and the shift in attitudes suggest that the younger consumers aged under 35 are less concerned about their privacy than consumers 35 or over (DMA 2018). According to DMA (2018), younger consumers feel they have more control over their data and show more acceptance of data exchange. According to Deloitte University Press' study (Conroy & Milando & Narula & Singhai 2014), also the willingness to share information with companies differs by age. The older consumers show less confidence in sharing personal information, but younger consumers are taking more protective actions to secure their data. Similarly, the results from DMA suggest that the understanding for data protection laws is higher among younger consumers than older consumers.

The differences could be partly explained by variation in technological adaption between different generations. Consumers under 35 years are either Millennials or post-Millennials, where the consumers 35 or over are mainly consists of Generation Xers and Baby Boomers and Silent Generation. According to Jingjing Jiang (2018) Millennials and post-Millennials stand out for their technology use and lead older generations in the technology adaption. Almost all of the Millennials own a smartphone, compared to older generations where the number is relatively lower. Similarly, the majority of Millennials use social media and have adopted relatively new platforms. Yet, the older generations, especially Generation Xers seem to increasingly embrace digital life. Yet, there is no specific academic study that researches this phenomenon and as such provides a great setting for

this research. In this study we want to research whether there are significant differences in attitudes towards data privacy between younger and older consumers and if so, to describe what these differences are. These results are expected to help marketers in their managerial decisions and in designing customer-oriented strategies. These results can be used to make future predictions on what direction are the attitudes going in the future, as the generational shift will occur.

1.3 Research questions and objectives

Based on the earlier studies it seems that there is a relationship between age and attitudes towards data privacy. Drawn from the research problem, we assume that:

There is a significant difference in attitudes towards data privacy between younger and older consumers

Scientific methods are used in order to test the hypothesis. In reflection to the hypothesis, the purpose of this study is to identify differences in attitudes towards data privacy between younger and older consumers. In order to support the research aim, the research question and sub-questions are formed.

Main research question – Are there differences in attitudes towards data privacy between younger and older consumers? If so, what are the differences.

Sub-questions

- a) Is there a significant difference in online privacy concerns between younger and older consumers?
- b) Is there a significant difference in attitudes towards data exchange between younger and older consumers?
- c) Is there a significant difference in the perceptions of personal data privacy between younger and older consumers?
- d) Is there a significant difference in the understanding of specific data protection laws between younger and older consumers?

Research questions are formed into research objectives in order to state what the study is expecting to achieve. Research objectives also illustrates the focus of the study in order to identify the main concepts that are being investigated in the research.

Table 1: Research objectives

| Question | Research question | Research objective |
|-------------------------------|--|---|
| Main research question | Are there differences in attitudes towards data privacy between younger and older consumers? If so, what are the differences. | To identify if there is a difference in attitudes towards data privacy between younger and older consumers |
| Sub-question a | Is there a significant difference in online privacy concerns between younger and older consumers? | To discover if there is a difference in online privacy concerns between younger and older consumers |
| Sub-question b | Is there a significant difference in attitudes towards data exchange between younger and older consumers? | To discover if there is a difference in attitudes towards data exchange between younger and older consumers |
| Sub-question c | Is there a significant difference in the perceptions of personal data privacy between younger and older consumers? | To discover if there is a difference of perceptions in personal data privacy between younger and older consumers |
| Sub-question d | Is there a significant difference in the understanding of specific data protection laws between younger and older consumers? | To discover if there is a difference in the awareness of specific data laws between younger and older consumers |

1.4 Main concepts and delimitations

Below are presented the main concepts relevant to the study. The theoretical meaning of these concepts is explained as it is used in this research paper.

Data privacy

Data privacy is the aspect of information technology that deals with handling of data concerning, consent, notice, sensitivity, and regulatory concerns as well as the practical issues around how data can be shared with third parties and how data is collected and stored.

Online privacy

Online privacy is the level of privacy and securities over personal data that is made available on Internet.

| | |
|-----------------------------|---|
| Data exchange | Data exchange is the process of collection and sharing of data between different computer programs. |
| Personal data privacy | Personal data privacy is individuals understanding of different data safeguards and actions taken to protect one's personal data. |
| Data protection legislation | Data protection legislations are specific laws that protect the personal information of individuals. |

There are some delimitations to the research. Firstly, study will be concentrating only on consumer product companies and therefore the same concept cannot be utilized to every organisation. Secondly, the research will focus on the digital environment and the privacy issues related to online activities and data-driven marketing. Third, the study is done with some practical delimitations, including market and international focus. The survey study will be conducted in Finland and therefore the research will also concentrate mainly on the legislative obligations in EU.

1.5 Conceptual framework

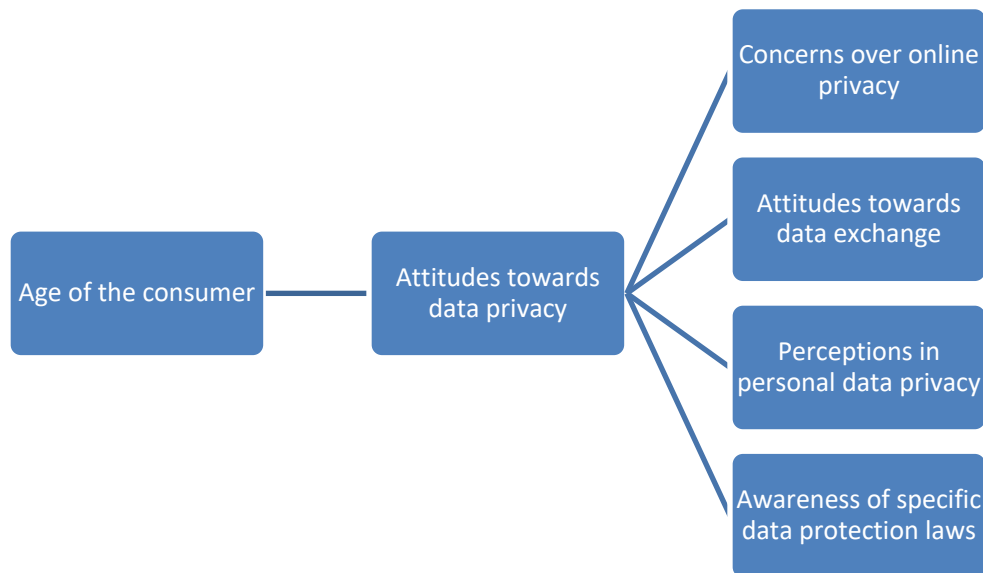


Figure 1: Conceptual framework

The conceptual framework in figure 1 demonstrates the linkage between the main concepts in order to test the phenomenon that is studied in this research. Age is expected to have an effect on the consumers attitudes towards data privacy. Attitudes towards data privacy is considered to be subject to individuals experience and knowledge on data privacy and data security such as concerns about

online privacy, attitudes towards data exchange, awareness of personal data privacy and understanding of specific data protection laws.

1.6 Structure of the thesis

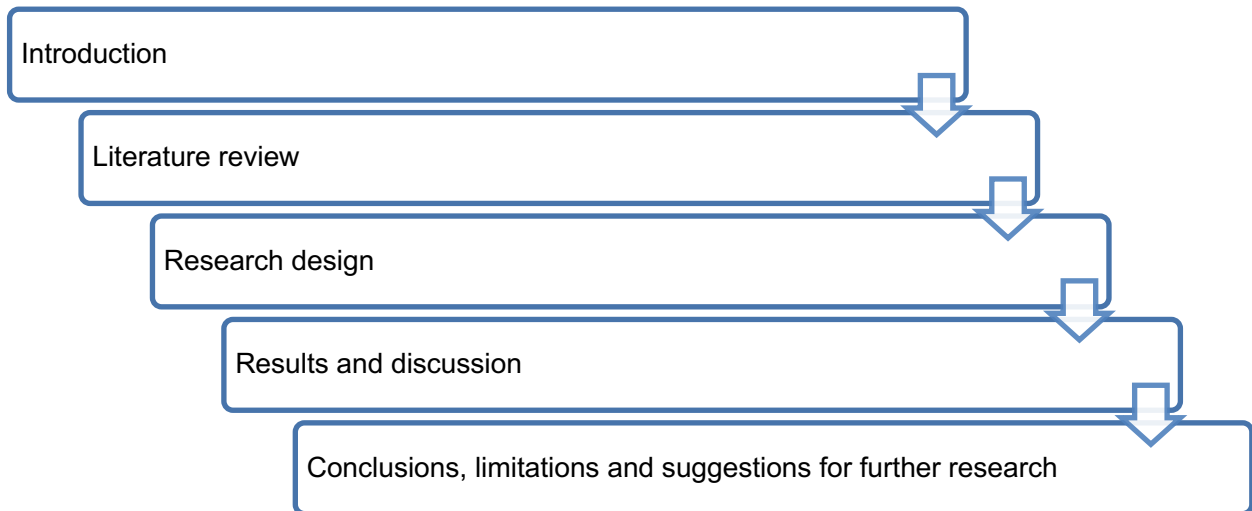


Figure 2: Structure of the thesis

The structure of the thesis is following the traditional order of master's thesis as seen in the Figure 2. The introduction chapter will present the background of the study and statement of the problem as well as define the research questions and objectives. Chapter 2 contains the literature review of consumers' attitudes towards data privacy based on earlier researches, including online privacy, data exchange, personal data privacy and data protection legislation.

In chapter 3, the research design is explained to determine the methods that are used to conduct the research. Chapter 4, results and discussion gives a general overview of the survey results and further discusses the findings in reflection to the research objectives. Finally, in chapter 5, conclusions are based on the main findings and suggestions for further research are presented.

2 CONSUMERS' ATTITUDES TOWARDS DATA PRIVACY

The growth in the production of data and technological developments have provided companies the possibility to collect large amounts of data about their customers (Baker 2018, Schneck 2018). The collected data helps companies to better understand their customers preferences and can lead to more effective marketing and increase in sales (Combemale 2017). The importance of customer data is recognised across all industries and more than 90 % of marketer's position data management as a priority for their organisation (Meinert 2018, Evans 2017). Driving innovation productivity, efficiency, and growth, data is extremely valuable for the businesses and governments but also individuals (Polonetsky 2013).

Digital content distribution gives great opportunities for commercial content providers and consumers, but also carries some threats, as digital content can be easily illegally copied and distributed (Petkovic & Jonker 2007, p. 21). Furthermore, the amount of personal data that organisations store in their databases, as well as the ways this data is collected and shared, has raised some concerns about privacy (Baker 2018, Karjoth & Schunter & Waidner 2003).

There have been several studies on consumer attitudes towards privacy including concerns about online privacy, attitudes towards the collection and use of personal data and perceptions of data protection. The literature review will provide a comprehensive picture on the consumers' attitudes towards data privacy today and more specifically if there can be identified any differences in the attitudes between younger and older consumers in the earlier researches.

2.1 Online privacy

Internet is raising privacy issues in relation to personal data as digital devices are increasingly present everywhere. According to Milan Petković and Willem Jonker (2017, p. 46), data collection and sharing can violate the privacy of an individual when personal data such as phone numbers or addresses are made publicly available. Similarly, the online monitoring can cause privacy issues if the information is collected in a way that is not visible for the data subject. Any collected information can easily be used to create elaborate records about the data subject. According to Nancy King (2016) personal data protection risks can give rise also when the individuals don't have control over the use of their personal data. Thus, it is difficult for them to prevent the misuse of personal data that may cause significant harm for them such as exposure of sensitive information.

2.1.1 Data security and privacy

Data security and privacy practices are necessary in order to find the balance between consumers' privacy and data protection rights and the rights of companies to collect and use data for commercial purposes (King 2016). The emerging technologies such as advances in digital storage and communication technologies have placed new requirements on data security (Petkovic & Jonker 2007, p. 19, 20). There is also a risk of privacy violation, as the data may expose consumers to possible online fraud or identity theft (King 2016).

Many privacy issues arise from the rapid increase in the use of digital technologies and the universal connectivity of people and companies through electronic technologies. People allow companies to track their activities online and are granting access to their personal data, such as financial transaction, credit card payments, business transactions, email addresses and even personal healthcare records to get personalised product and services in return from companies. The collected data from individuals typically includes personal information and is therefore essentially privacy sensitive. (Petkovic & Jonker 2007, p. 20)

Data privacy is the ability of individual to separate themselves or their personal information and therefore have the ability to disclose them selectively. There are many privacy issues related to personal information, including the ability of an individual to have control over their data, the organisations ability to data replication and avoidance of data loss, leakage and unauthorised modification or fabrication as well as clarifying which party is responsible for ensuring legal requirements for personal information and to what extend third parties are involved in the processing of data. In practice, this means the application of privacy laws, mechanisms, standards and processes by which personally identifiable information is managed. (Wei, L. & Zhu, H. & Cao, Z. & Dong, X., Weiwei, J. & Chen, Y. & Vasilakos, A. 2014)

Data mining technologies are increasingly used, and companies are creating large databases from the collected data (Petkovic & Jonker 2007, p. 7) The databases are vulnerable and there is a threat of misuse and revealing of individual data records (Petkovic & Jonker 2007, p. 36) and companies need to protect the data against unauthorised access, intentional break-ins or disruptions (Petkovic & Jonker 2007, p. 42). Data breaches can lead to severe consequences and losses via reputational damage, legal liability or ethical harms (Kshetri 2014) and therefore data security has become very important when designing any information systems (Petkovic & Jonker 2007, p. 36).

Data security can be defined as the protection of data confidentiality, data integrity and data availability. When sensitive information is stored in the databases it is important to ensure the

confidentiality of the data. This often means use of authentication and access control strategies which increases the reliability and trustworthiness of data storing. Also, the data integrity is a critical component of any information technology system. It means that the data is protected from unauthorised access that can emerge as modification, deletion or fabrication of the data. Data availability means ensuring that data continues to be available to the end users at required level and in case accidents occur to data it can be recovered. (Wei, L. & Zhu, H. & Cao, Z. & Dong, X., Weiwei, J. & Chen, Y. & Vasilakos, A. 2014)

2.1.2 Ethical aspects of data security and privacy

The data security and privacy measures are meant to protect but it is also possible that they can cause harm. The ethical analysis of data security and privacy issues largely takes place in computer ethics that analyses the moral responsibilities of computer professionals, computer users and public policy makers in information security. The analysis of the ethical issues can help to recognise and resolve moral dilemmas and generate ethical policies and guidelines (Petkovic & Jonker 2007, p. 36-38).

Probably the most obvious harm that can be caused by data breach is economic harm, losses of time, money and resources, when valuable data is damaged or corrupted or has even become unavailable. Violation of property or privacy rights may occur when the confidentiality of information is compromised by accessing, copying or disseminating information which may cause reputational harm to the organisation. Similarly, the compromises of the availability of information can violate the freedom of information. In extreme cases, data breaches of computer security may even cause serious harm or have life-threatening consequences that arise from situations where computer systems are used to construction work, control of aircrafts or making medical diagnosis. Another, more recent concern in information security has been the possibility of cyberterrorism, which is defined as a politically motivated act that intends to cause harm. (Petkovic & Jonker 2007, p. 36-38, 42)

There is a broad recognition of a right to personal privacy in western countries. It is often defined as the right of individual to control access or interference by others into their private matters and it is cherished for several reasons. Most often it aims to protect individuals from external threats, such as identity theft and exclusion. The most important principle in privacy protection is the ability for individuals then to voluntarily give up their privacy. Yet many disputes related tension between individuals right to privacy and organisations interests (Petkovic & Jonker 2007, p. 42, 45)

2.1.3 Concerns over online privacy

Consumers have expressed a growing concern over companies' data collection methods accessibility by third parties (Ksethri 2014). Nevertheless, according to recent studies the overall privacy concerns have in fact declined and 75% of the consumers claimed to be concerned about their privacy in DMA's latest study. Younger consumers seem to be even less concerned as just 58% of younger consumers claimed to be concerned about their privacy (DMA 2018).

Consumers are often uncomfortable when they feel that companies know more about them than they are willing to voluntarily provide (Ksethri 2014), yet majority of consumers seem to be happy with the amount of personal information they share with companies. Interestingly, only the consumers between ages 45 and 55 seemed to be less convinced than the average (DMA 2018).

Direct Marketing Association (DMA 2018) is presenting a theory, according to which the consumers can be divided into three segments according to their attitudes towards data privacy. These groups are: pragmatists, fundamentalists and unconcerned. The 'Data pragmatists', are the consumers who are willing to share data in return for something, like special offers or preferential treatment. Pragmatists are willing to trade their data but only on a case-by case basis when the service or enhancement of service is worth the information requested. In contrast, the 'Data fundamentalists', are the consumers who are against sharing data. Regardless of what they may receive in return, the fundamentalists are unwilling to exchange their personal information. Then there are the 'Unconcerned' who are the consumers who are not concerned about the collection and use of personal data. For them, it is just a part of the modern economy. The pragmatists are the largest segment and consists of roughly half of the consumers. More and more Generation Xers fall in this category but still there is a slight decline in this category due to Millennials shifting to the unconcerned category that is growing steadily. At the same time, the number of fundamentalist consumers is declining, and this category mainly consists of Generation Xers and Baby Boomers, which is likely due to older demographics conventionally displaying higher levels of concern and discomfort around data exchange. Younger consumers are more likely to adopt a pragmatic or unconcerned attitude, and the 'digital natives' like Millennials are likely to be slightly more discerning about data privacy issues and more demanding of incentives in return for personal information.

2.2 Data exchange

The advertising today centres around data (Schneck 2018). With data companies make better business decisions (Uzialko & Writer 2018). For marketers, data is providing totally new information about customers that can be used to improve the relevancy of their advertising (Combemale 2017).

Moreover, data has made it possible for marketers to deliver more precise people-based communications (O'Reilly 2018, Evans 2017) and this can be done with half the money and effort than in traditional marketing that now seems broad and untargeted (Baker 2018). Data comes from interactions with the company or other sources such as activity websites, mobile app usage, social media or customer surveys (Combemale 2017). The collected data can be further combined into datasets from which the companies are able to make inferences or draw conclusions about data subjects (King 2016).

2.2.1 Data collection and web analytics

Data-driven marketing is a widely used process where marketers draw insights and make decisions based on data (Tjepkema 2018). By analysing customer behaviour through data, the company can make future predictions and better understand their customers' needs (Uzialko & Writer 2018, Tjepkema 2018) Most importantly, data-driven marketing allows for multi-channel experience (Uzialko & Writer 2018) and when implemented successfully, the company can gain: clear-cut clarity, multi-channel experience, refined customer experience and better product development (Tjepkema 2018).

Web analytics is a cornerstone for data-driven marketing strategy (Kaushik 2007, 1-2) and helps companies improve productivity and managerial performance (King 2016). It allows companies to experiment, learn and measure the performance and helps businesses make smarter, more informed decisions about their marketing and web presence (Kaushik 2007, 1-2, Leone 2016). Data can be collected from a wide variety of sources, both online and offline (King 2016 & O'Neill 2018). The different technical appliances such as smart phones, tablets, and computers enable real-time interactions between individuals and companies (Hazari & Brown 2013). As consumers are browsing online, companies can follow their activity by using different tracking technologies (van Eijk 2012). The most obvious places to track the consumer activity are company website and social media pages. (Uzialko & Writer 2018) The activity can be tracked in number of ways such as web log files, web beacons, JavaScript tags, packet sniffers and built-in data collection mechanism (Kaushik 2007, 24-25) but cookies are the most invaluable tool in online tracking (van Eijk 2012). In addition to tracking, companies can collect customer information either directly asking from the customers or by appending other sources of customer data (Uzialko & Writer 2018). This can include data such as credit ratings, profiles build from online activities or tax records or data collected by other businesses (King 2016). Where the first-party data is a key building block, the third-party data can often provide a much better picture of customer's profile (Combemale 2017).

Often, both situational data and personal data are collected (O'Neill 2018). Personal data is considered as any kind of information relating to a person, including their name, photograph, email address or bank account details and even the messages posted on public websites, medical data or a computer's IP address (Krystlik 2017). Situational data is usually easier to access, and it does not have the same tracking or privacy issues as in personal data. Situational data helps to identify customers based on the environment in which they are interacting with a company at any given time such as device, location or weather, it is usually easier to access, and it does not have the same tracking or privacy issues as in personal data. (Pook 2015).

Profiling is an automated processing of personal data. It allows businesses to analyse and the behaviour, preferences or locations of a data subject. In many cases, it is done without the data subject even being aware. Such processes are for example tracing and ad conversion measurement. There are many advantages to these technological advances, however they also carry inherent privacy risks. (Hunton&Williams 2016)

2.2.2 Personalisation

Data can also be used to deliver targeted marketing (King 2016) and to personalise the customer experience (Tjepkema 2018). In personalisation, the information about data subject is collected and analysed (Petkovic & Jonker 2007, p. 23) to get insights about individuals' preferences (Chelappa & Sin 2005). Consumers prefer to be communicated to with relevant and tailored message (Krafft & Ardena & Verhoefb 2017) and data is the only way marketers can offer customers the relevance they demand (Combemale 2017).

Personalisation is noticed to increase customer loyalty and it can be considered even as a competitive necessity as every company online offers some level of personalisation to their customers. Personalisation is dependent on two factors: vendor's ability to acquire and process information and the individual's willingness to share data. The advanced tracking technologies have provided the companies the ability to create sophisticated consumer profiles in order to gain insights about individuals' preferences. However, the consumers may not be willing to share information about themselves due to privacy concerns and therefore the company needs to communicate them the benefits of sharing their personal information. (Chelappa & Sin 2005)

2.2.3 Attitudes towards data exchange

According to DMA's latest study (2018), the consumers increasingly regard their personal data as an asset that they can use to their advantage in data exchange. Trust in a business is the dominant prerequisite when engaging consumers and transparency is a consumer priority for data exchange. Interest in data security is growing and at the same time the importance of ensuring that the benefits derived from data sharing are communicated with consumers has increased. When asked about specific areas of data exchange, consumers felt that the areas where they had lesser control were choosing the rewards or benefit received in return for sharing data with companies and the privacy settings that allow them to choose how much data they choose to share.

Most consumers appear to be open to share their information as (Pingitore, Vikram, Cavallaro and Dwivedi 2017) and see data sharing as a part of the modern economy (DMA 2018). Likewise, majority of consumers claim they are more aware of how their data is used and also increasingly comfortable with sharing their data for with companies where the percentage rises significantly among 18-24-years-olds, reaching 61% (Ridley-Siegert 2015). Furthermore, the studies suggest the willingness to share information with companies varies by age (Ridley-Siegert 2015). Perhaps due to the fact that younger consumers have grown up in the digital word, they are more comfortable with data exchange and more open for data sharing (DMA 2018).

A study by University of Pennsylvania's Anneberg School for Communication, argues against the assumption that consumers are gladly sharing their information. Many consumers feel that collecting data has become such a common practice in the digital age that they have no other option than to comply. According to a study by Deloitte University Press (2017), the consumers are concerned of the misuse of their personal information and as high as 81 % of the consumers feel they have lost control over the way their personal data are collected and used (Pingitore, Vikram, Cavallaro and Dwivedi 2017). Most of the consumers feel they are lacking the knowledge of how to control and protect their own data (Claveria 2018).

2.3 Personal data privacy

Personal data is considered as any information, such as location, genetic and biometric data (Travelyan 2018), that could identify and individual (Meinert 2018) either as such or when it is combined with other data (Hunton&Williams 2016).

There are several safeguards and activities that consumers can do to protect the privacy of their personal data. Personal data is considered as any information, such as location, genetic and

biometric data (Travelyan 2018), that could identify and individual (Meinert 2018) either as such or when it is combined with other data (Hunton&Williams 2016).

Consumers should always know with whom they share their information with and be critical before deciding to share personal information. Consumers should also be careful of oversharing on social media sites. Sharing preferences can be controlled by adjusting the privacy settings. Electronic devices can be kept secure by using security software, avoiding phishing emails and using public wireless networks with discretionary. Consumers should also make sure a website has a clear privacy policy that provides information on how websites maintain accuracy, access, security, and control of personal information it collects as well as how it uses the information and whether it provides information to third parties. (Federal Trade Commission 2012)

2.3.1 Building consumer trust through data security and privacy

All organisations have personal data to protect in their customer databases and therefore privacy plays an important role for every company (Krystlik 2017). There is a connection between consumer's perceptions of data privacy and the security practices and commercial success, hence trusted stewards of consumer data can be used to stand out from the competition (Conroy, P. & Milano, F. & Narula, A. & Singhal, R. 2014). Privacy should be seen in a positive light and implementing the regulations is good business sense as the companies can benefit on telling the customers about these extra efforts they have made to secure their data (Pearse 2012). Companies need to be transparent and open to its customers how it collects, processes, or uses data (Combemale 2018, Schneck 2018). Companies that acknowledges these factors can also use this to provide a better user experience and consequentially when the consumers trust the company, they are more willing to share their data and do long-term business with them (Ridley-Siegert 2015).

The level of trust is based on a commitment to the quality of the customer experience (O'Reilly 2018) A study by Deloitte University Press (Conroy & Milando & Narula & Singhai 2014) suggests that data privacy and security is also an important factor in a great customer experience. Consumers have a good awareness of the risks surrounding data privacy, and many businesses are overestimating the extent to which they are meeting the consumer expectations. Companies are also underestimating the opportunity for competitive advantage associated with data privacy and security. Data privacy should not just be seen as a risk management issue, but as a possibility to differentiate themselves through a reputation for strong data privacy and security practices.

There are several things to help keep consumers' trust. Firstly, companies should enforce privacy measures to prevent breaches in the first place by encrypting data at rest, destroying consumer data when not needed. Secondly, in case of a data breach, the companies should systematically control the damage after a breach has occurred, identifying affected systems and isolate them, gather all available evidence, and analyse it to determine cause, severity, and impact as well as document and report the findings on the incident to relevant stakeholders. After this, the companies should assess the possibility of insider involvement and strengthen networks security and improve protocols by enhancing monitoring to mitigate the risk of future breaches. Thirdly, companies should develop an integrated enterprise-level approach to data governance and ensure the leader of this initiative is an executive of appropriate level. (Gina Pingitore, Vikram Rao, Kristin Cavallaro, and Kruttika Dwivedi 2017)

2.3.2 Perceptions of personal data privacy

In general, consumers are hesitant to knowingly allow companies to use their information for marketing purposes. Somewhat comfortable the consumers were to share their purchase history and demographic information but only 20% would allow their online search history to be analysed and even fewer would allow their social media postings of content of their emails for companies to use in order to send targeted advertisements or coupons. (Conroy & Milando & Narula & Singhai 2014)

Consumers are more comfortable to share their information when companies are transparent about what they are doing with the data and more than 80 % of consumers state that transparency over data collection the terms and conditions are important when sharing personal information with companies (DMA 2018) Also, 75 % of the consumers state that they are more willing share their data if there was a clear benefit for them and companies can encourage consumers to share their data more freely by offering valuable benefits for those consumers who choose to share their data and customise (Pingitore, Vikram, Cavallaro and Dwivedi 2017) Companies also need to allow consumers easily to change their data sharing preferences at any time (Pingitore & Vikram & Cavallaro & Dwivedi 2017).

The link between purchase decision and perceived data security is stronger than many believe, and strong privacy and security practices should be seen as a competitive opportunity. The study by Deloitte University Press (Conroy & Milando & Narula & Singhai 2014) shows that half of the consumers are more likely to buy from companies that are perceived to be protecting their personal information. Similarly, majority of consumers avoided of purchasing from brands that they do not believe protect their personal information. A negative brand experience can quickly lower consumers

trust and harm the brand image and same applies to data breaches. More than half of consumers think that the knowledge of a data breach at a company would negatively impact their brand image and likelihood of buying from that company in the future. Still, many consumers say that they would be forgiving of a company that experienced a breach as long as the company quickly addressed the issue. Yet, only few consumers believed that most companies were adequately protecting their personal information and even fewer knew which companies best protect their personal information and even fewer think that they know which companies best protect their information.

The consumers state they want more protection and security over their data (Pingitore & Vikram & Cavallaro & Dwivedi 2017). Consumers also appear to nurture clarity and transparency around data privacy and data security practices, as well as by the ability to control how their data is used, 75% of consumers agreed that easily understandable privacy policies increase their trust in companies with regard to the protection of their personal information. (Conroy & Milando & Narula & Singhai 2014) Trust in a company is a dominant prerequisite when engaging consumers within the data economy and at the same time interest in ad blocking among consumers is growing and this brings a challenge for marketers (DMA 2018). Younger consumers seem to take more proactive action to protect their data than older consumers (Conroy & Milando & Narula & Singhai 2014). The younger consumers show more interest towards security and ad blocking software's (DMA 2018) and younger consumers were more likely to provide fake information on websites than older consumers and take more protective actions, such as adjusting privacy settings due to privacy concerns (Conroy & Milando & Narula & Singhai 2014).

2.4 Data protection legislation

Since the advent of Internet, the law makers have been desperately trying to keep up with the digital and technological developments (Mullock 2012). As data is growing its importance in marketing consumers are concerned about their privacy (Kaushik 2007, 25) and the law makers are amending privacy rules to protect the privacy of individuals (van Eijk 2012).

The right to privacy is recognised as a fundamental right around the world. In the majority of countries, it is considered as a constitutional right and an international human right and in most of the law's privacy is a basic principle. With the rise of the computer era, the Organisation for Economic Cooperation and Development (OECD) issued guidelines on the protection of privacy and use of personal data already in 1980. Its main principles are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation and accountability. These principles have played an important role in the development of privacy laws in the EU and other jurisdiction. (Petkovic & Jonker 2007, p. 27-29).

2.4.1 EU's data protection laws

The earliest data protection laws in EU originate from 1995, when the Data Protection Directive was introduced (Mullock 2012, Hunton&Williams 2016). The directive's aim was to control the emerging digital issues related to personal data with seven basic principles: notice, purpose, consent, security, disclosure, access and accountability (Krystlik 2017).

The ePrivacy Directive, also known as the 'the cookie law' (Consentric 2018), entered into force in 2012. (Pearse 2012, Voss 2017). The ePrivacy Directive was meant to work together with The Data Protection Directive (Meinert 2018). The main idea was to adapt the existing regulatory framework to keep up with the latest technological developments by underlying a high level of protection for individuals' privacy and personal data by ensuring, that regardless of the technology used, the electronic communications were secure and confidential (Saxby 2008, van Eijk 2012).

The ePrivacy Directive is still in force but the Data Protection Directive was replaced by the General Data Protection Regulation (GDPR) when it entered into force in May 2018 (Consentric 2018, Meinert 2018). The GDPR is probably the biggest shakeup to data privacy since the creation of Internet (Meinert 2018). The new regulation aims to create consistency and simplify the regulatory environment in the EU (Oldwick 2017). One of the most significant changes brought by GDPR (O'Brien 2016) is that it legislates all personal data, regardless and the physical location of where the data is hosted is no longer relevant (Krystlik 2017). The regulation applies to any company or entity in the EU (Uzialko & Writer 2018) and entities and companies established outside EU but who are processing personal data of individuals in the EU through their activities (Combemale 2018).

The GDPR has placed out much stricter rules on the collection and use of personal information (Uzialko & Writer 2018) including requirements for data protection officers (DPO), data audits, data protection by design and PIAs, security breach, expanded consent requirements, data portability, jurisdictional reach, data transfers and the right to be forgotten (Mullock 2012). In addition, the European Commission wanted to bring the threat of fines for non-compliance (Pearse 2012). For non-compliance companies can be fined as much as 4% of their worldwide turnover and up to 20 million euros (Krystlik 2017).

Under GDPR an individual should have the right to be forgotten or in legal terms 'right to erasure' and it should be accessible to everyone (Krystlik 2017, Meinert 2018). Another important individual right is 'the right to data portability'. The data portability is referring to an individual right where the

data subject can request their data from one data controller and have that data transmitted to another data controller. Individuals should also have the right to access their data in a free, electronic format. This right is expanded with a notion of 'privacy-by-design', which refers to the requirement that companies should at every stage of a product's design and development include proper privacy protections measures (Meinert 2018) and when designing or upgrading any processing system, procedure, policy or data-sharing initiative, privacy should be built into systems and promoted as a default setting. (Dickie 2017, Hunton&Williams 2016, Koops & Leenes 2013) Furthermore, as many marketers no longer collect the customer data themselves but are using the information from other vendors, there are also rules for "third party" data and companies must make sure those vendors are following GDPR standards (O'Reilly 2018). According to GDPR, any data breaches should be reported to the supervisory (Travelyan 2018) and every company should appoint a data controller who should be contactable by any supervisory authority (Krystlik 2017). In some cases, there is also a requirement for a data protection officer (DPO) who designs and deploys privacy policies in the organisation. (Karjoth & Schunter & Waidner 2003, Hunton & Williams 2016).

Not long after the GDPR was presented, there was a proposal for a new ePrivacy Regulation (Voss 2017). The ePrivacy Regulation (ePR) is expected to be released in the Autumn of 2019 (Trick 2018a), however the exact date is not yet known (Consentric 2018). Together, GDPR and ePR are forming the updated EU data protection framework and while GDPR is concerned solely with personal data, ePR is focused on the confidentiality matters of any data involved in electronic communications and aims to defend the integrity of information at any form by obliging additional controls over cookies and other tracking technologies on electronic devices and applications (Trick 2018b).

Even though there is legislation to protect the data protection rights of an individual, there are still a number of uses of data that fall into a so called "regulation grey area". Hence, there is a need for a company-level privacy policy that include the best practices ensuring privacy and security of customer data (Kshetri 2014). It is important that privacy protection is part of the design and use of a technology, even in the absence of a legal obligation or legal risks the individual must be informed and, in many cases, must give his consent where privacy invasions are necessary as part of the use of the technology or the service (Petkovic & Jonker 2007, p. 31). It is also important to be clear for to the customers if their data is collected and also to specify what kind data is collected (Kaushik 2007, 25). Anyone who places cookies or other types of tracking technology needs to provide users with clear and comprehensive information about their purpose and require informed consent from data subjects (van Eijk 2012).

2.4.2 Awareness of specific data protection laws

Companies who are reluctant in privacy compliance are the companies who seem untrustworthy in the customers eyes (Ridley-Siegert 2015). According to DMA's report (2018) 88% of consumers cite transparency as the key to trust. Correspondingly GDPR requires companies to consider the impact on privacy and the risks in the processing of any personal data of their customers and find the balance between privacy and innovation. Although the consumers say they have become more aware of personal data privacy the report show that the awareness of specific data protection laws is still quite low as in 2017, only 39% indicated they were familiar with the GDPR that was, rising to around half among 18-34-year-olds, but this was before the regulation came into force.

2.5 Summary of the literature review

In digital world, everything runs on data and the data collected of individuals is highly important for today's businesses. While consumers are enjoying information and communication technologies, companies are increasingly tracking their activity online to draw insights for marketing purposes. With personal data, the companies are able to understand better their customer and make better business decisions. Data analytics has become a key part of creating marketing strategies and it requires large amounts of personal data. Along with all its benefits, the amount of personal data and how it is collected and shared has raised some concerns in relation to data privacy and data security. Earlier studies on consumer's attitudes towards data privacy suggest that consumers are concerned about their online privacy and feel they have lost control over their personal data.

The theory around data privacy is very broad as it has a lot of interconnection in relation information technology, marketing and legal principles. Thus, the main concepts in this research are online privacy, data exchange, personal data privacy and data protection legislation and the main points on each concept are presented in table 2.

Table 2: Summary of the literature review

| Concept | Main points |
|----------------|--|
| Online privacy | <ul style="list-style-type: none">- Consumers are concerned about the privacy of their personal data (Ridley-Siegert 2015).- Consumers feel they have lost control over their personal data (Pingitore & Vikram & Cavallaro & Dwivedi 2017)- Younger consumers are less concerned about online privacy (DMA 2018). |

| | |
|-----------------------------|---|
| | <ul style="list-style-type: none"> - Younger consumers are most likely to adopt pragmatic or unconcerned attitude (DMA 2018). |
| Data exchange | <ul style="list-style-type: none"> - Data has become a fundamental part of advertising (Tjepkema 2018) - Consumers increasingly regard their personal data as an asset that they can use to their advantage in data exchange. (DMA 2018) - Consumers are more willing to share data when there is a clear benefit (Pingitore, Vikram, Cavallaro and Dwivedi 2017) - Younger consumers are more comfortable with sharing their data for companies (Ridley-Siegert 2015). |
| Personal data privacy | <ul style="list-style-type: none"> - There is a connection between consumer's perceptions of data privacy and the security practices and commercial success (Conroy, P. & Milano, F. & Narula, A. & Singhal, R. 2014) - Trust in a company is a dominant prerequisite when engaging consumers within the data economy (DMA 2018) - Younger consumers seem to take more proactive action to protect their data than older consumers (Conroy & Milando & Narula & Singhai 2014). |
| Data protection legislation | <ul style="list-style-type: none"> - The law makers aim to increase the effectiveness of the right to data protection and to put individuals in control of their own personal data (Oldwick 2017). - Younger consumers are more familiar with the GDPR than older consumers (DMA 2018). |

3 RESEARCH DESIGN

In this chapter, the chosen research methods are presented, and research process is discussed.

3.1 Research methods

Quantitative research uses numeric and quantifiable data to generalise a certain phenomenon. This study aims to answer the research question "is there a difference in the attitudes towards data privacy between younger and older consumers?" It is expected that the attitudes towards data privacy is dependent on the age of the consumer. Thus, the variables that are being measured are consumers age and attitudes towards data privacy. This is done by dividing the consumers into two group

according to their age: younger and older consumers. The groups are divided so that the younger consumer are consumers under 35 years old and the older consumers those of 35 and over.

The research aims to statistically analyse the potential difference in attitudes towards data privacy between younger and older consumers. ANOVA (Analysis of Variance) is a collection of statistical models and their associated estimation procedures used to analyse the differences among group means in a sample (Girden 1992, p. 1). In this research one-way ANOVA is used to compare the answers between younger and older consumers in order to test the hypothesis. The purpose of the ANOVA analysis is to determine the extent to which the effect of an independent variable (which in this case is the age) is a major component (Girden 1992, p. 1). The ANOVA analysis is made with Webropol Professional Statistics Tool. For those questions that are not possible to be analysed through ANOVA, more descriptive approach is used to identify the differences between the two groups.

3.2 Hypothesis testing

Quantitative research allows to investigate the phenomenon that there is a difference in consumers' attitudes towards data privacy between younger and older consumers. In this study we claim that there is a relationship between age and consumers' attitudes towards data privacy. Therefore, the hypothesis is:

H1 There is a significant difference in attitudes towards data privacy between younger and older consumers

In order to test the alternative hypothesis, the null hypothesis need to be formed. The null hypothesis assumes that there is no difference and expects that the results are equal (Kanji 2006, p. 2). In this case, the null hypothesis is: "*H10 There is no significant difference in attitudes towards data privacy between younger and older consumers*".

There are two possible outcomes for testing hypothesis. The results will even reject the null hypothesis or fail to reject the null hypothesis. In order to test this, a critical region needs to be chosen and with left-sided critical region we reject H0 if the test statistic is less or equal to the critical value (Kanji 2006, p. 2).

Also, the size of the critical region needs to be chosen, in order to specify how great risk there is of coming to an incorrect conclusion (Kanji 2006, p. 2). In this case we set the α to 5 %, which gives us

a 95% level of confidence. To know where to draw the line to make decision, we need to calculate the level of significance, that in this case gives us the following calculation: $\alpha = 1 - 0.95\% = 0.05$. Therefore, the level of significance (or p-value) is 0.05, which means that if the p-value of the result is less or equal to the critical value the H_0 can be rejected.

3.3 Data collection

An online survey questionnaire was used to collect the data. The questionnaire was conducted by using an online service Webropol and the questionnaire link was made public online to collect responses between 24.12.2018 - 10.1.2019. The questions were presented both in Finnish and in English. The research questionnaire was to repeating questions from earlier studies and is therefore formed by combining a selection of questions from earlier studies by Direct Marketing Association and Deloitte University Press that were reviewed in the literature review. Attitudes do not naturally exist in quantitative form, yet it is possible to develop a questionnaire that asks people to rate a number of statements (Muijs 2011, p. 2). The questionnaire can ask people to use a rating scale where their answer is chosen within the chosen scale like of 1-10, 1 being negative end and 10 being positive end or rate a number of statements on a scale as either strongly agree or agree, disagree or strongly disagree and give the answer a number like 1 for strongly disagree and 4 strongly agree.

The questionnaire (Appendix 1) consisted of 13 questions, from which the questions 1, 2 and 3 deals with respondents' basic demographic information. Rest of the questionnaire is a combination of questions from earlier studies by Direct Marketing Association and Deloitte University Press that were reviewed in the literature review. To gain a general picture of the respondents, background questions are asked. In the beginning of the questionnaire, the respondent is asked to give out their age, gender and to evaluate their online activity. It is anticipated that the distribution of age and gender would be somewhat equally divided. Other research questions are divided in four groups in relation to which hypothesis it aims to test. Questions 4 and 5 assess' the differences in online privacy concerns between younger and older consumers. These questions aim to answer sub-question a. Questions 6, and 7 represents the differences and similarities in attitudes of younger and older consumers towards data exchange and are answering the sub-question b. Questions 8, 9, 10 and 11 compares the perceptions in personal data privacy between younger and older consumers to answer sub-question c. Finally, questions 12, and 13 evaluate the awareness of specific data protection regulation of both younger and older consumers to answer sub-question d. By combining the results on the sub-questions, the main research question can be answered.

3.4 Sample selection

To conduct the research, a suitable sample from population needs to be selected. Due to the delimitation the population of this study is considered to be Finnish consumers. Due to limited time and researches the convenience sampling technique was chosen, whereas the population includes people who are easy to reach. The questionnaire link was published on the researcher's personal social media networking sites such as Facebook, Instagram and LinkedIn to attract potential respondents. On the Facebook and LinkedIn accounts it was expected to reach more of the older consumers, while the younger consumers were expected to be reached on Instagram. The idea was to have the link openly available so that anyone could take part in the questionnaire. It was also said that the questionnaire could be shared on their own newsfeed. The link was also shared via instant message on WhatsApp to researcher's personal contacts. Also, here it was requested that the link could be further shared to reach more respondents.

As the statistical test is performed to two independent means, the total sample needs to be divided into two groups. As mentioned earlier the groups are divided so that the younger consumer are consumers under 35 years old and the older consumers those of 35 and over. With desired power of .80 (80%) and alpha .05, we need at least 34 participants per group. The size of each sample groups should be somewhat equal.

3.5 Research process

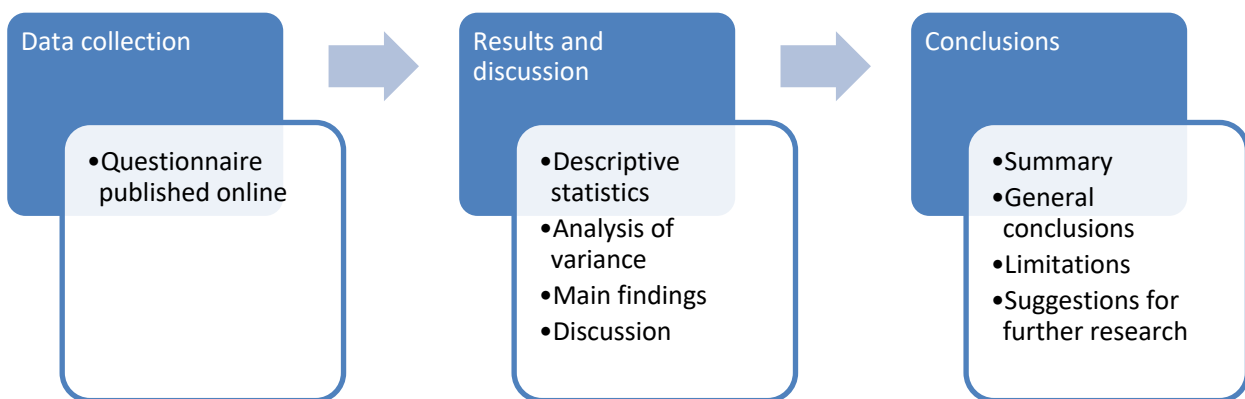


Figure 3: Research process

As presented in Figure 4 the research process, the research process starts with the data collection that is conducted according to the inquired strategy. The data collection is followed by descriptive statistics that present the general results of the survey, after which the analysis of variance is made to determine whether a significant difference exists between the means of the variables being studied. With the outcomes of the data analysis the hypothesis can be tested per each question. The

main findings are presented and followed by discussion. Finally, conclusions are made in reference to the main findings of the research to provide managerial implications and suggestions for further studies.

4 RESULTS AND DISCUSSION

In this chapter, the questionnaire results are presented and analysed. The summary of findings will give a more general picture of the results after which the results are discussed in reflection to the literature review and hypotheses.

4.1 General description of data

The research in this study encompasses the results of the online questionnaire. The survey polled 120 consumers, the non-Finnish residents were excluded from the results and the total respondents is therefore 116. From the 116 respondents, 69 of the respondents were under 35 years old and fall under the category of “younger consumers” and 47 of the respondents were 35 years old or over and fall under the category of “older consumers”. The full result file can be found in Appendix 2.

The data analysis consists of statistical presentation of the results from the questionnaire as well as analysis of variance with ANOVA to analyse the differences among the group means in the sample. The full results of this analysis are presented in Appendix 3.

4.2 Descriptive statistics

The research outcomes on consumers’ attitudes towards data privacy are presented by using statistical key figures. The results are divided into sub-chapters that are: online privacy concerns, attitudes towards data exchange, perceptions of personal data privacy and awareness of specific.

4.2.1 Online privacy concerns

Questions 4 and 5 aim to understand differences in online privacy concerns between younger and older consumers. In question 4 the importance of online privacy in different settings between younger and older consumers is reviewed. In question 5, the overall level of concerns over data privacy online is compared between younger and older consumers.

Your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission

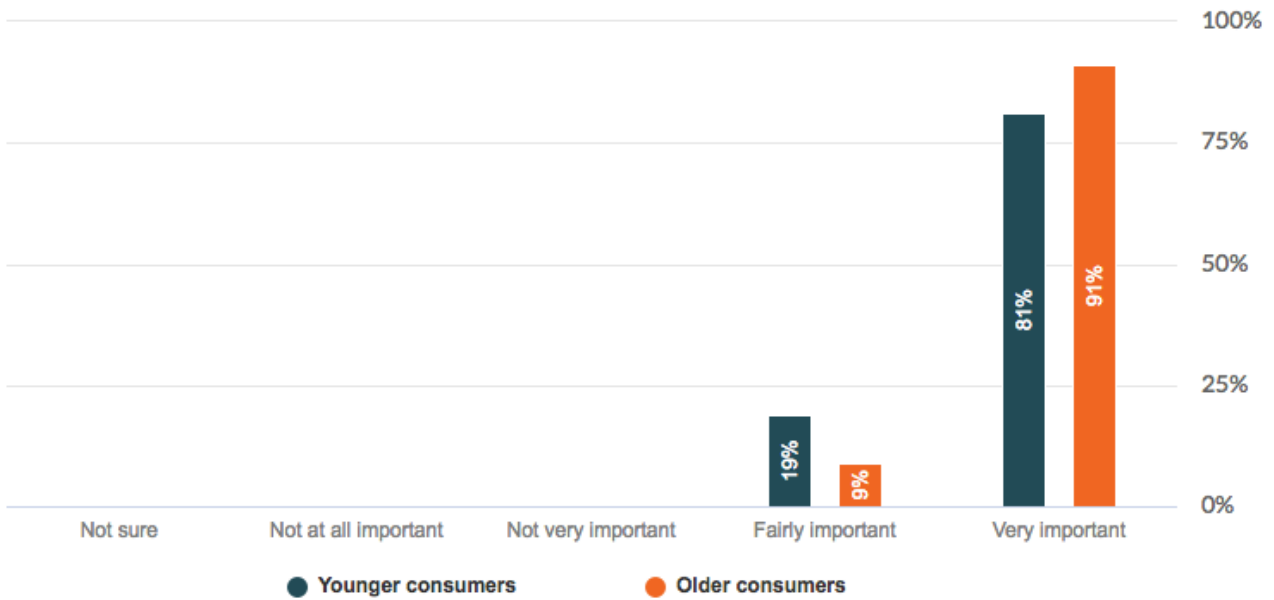


Figure 4: Personal information on computer, smartphone or tablet can only be accessed with a permission

In figure 4, “your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission”, the results show that it is very important for the consumers that their personal information can be accessed only with their permission. Also, the confidentiality of emails and instant messaging was rated very important. However, the importance of permission in online tracking showed a little difference in the opinions.

When comparing the results of younger and older consumers, the importance of permissions when personal information is accessed did not show much differences. 19% of the younger consumers rated the importance of permissions as fairly important and 81% as very important. In comparison, from the older consumers the percent who said the importance of permissions when personal information is accessed is fairly important was 9% and very important was 91%.

The confidentiality of your emails and instant messages is guaranteed

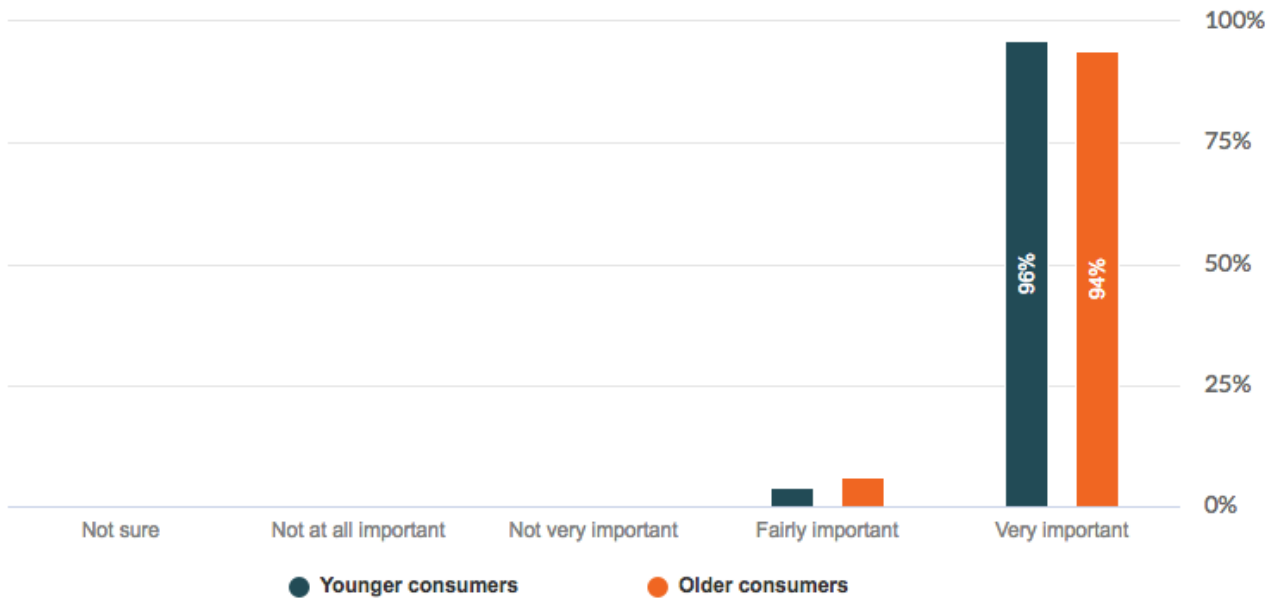


Figure 5: Confidentiality of emails and instant messages is guaranteed

In figure 5, “the confidentiality of your emails and instant messages is guaranteed”, the results show that it is also very important that confidentiality is guaranteed when individuals are using electronic communication tools. When comparing the results of the younger and older consumers, the importance of the confidentiality of emails and instant messaging, did not show almost any difference but almost every respondent rated this as very important. From the younger consumers only 4% of the consumers rated the importance as fairly important and the rest as very important. Also, from the older consumer only 6% rated the importance as fairly important and 94% as very important.

Tools for monitoring your activities online (such as cookies) can only be used with your permission

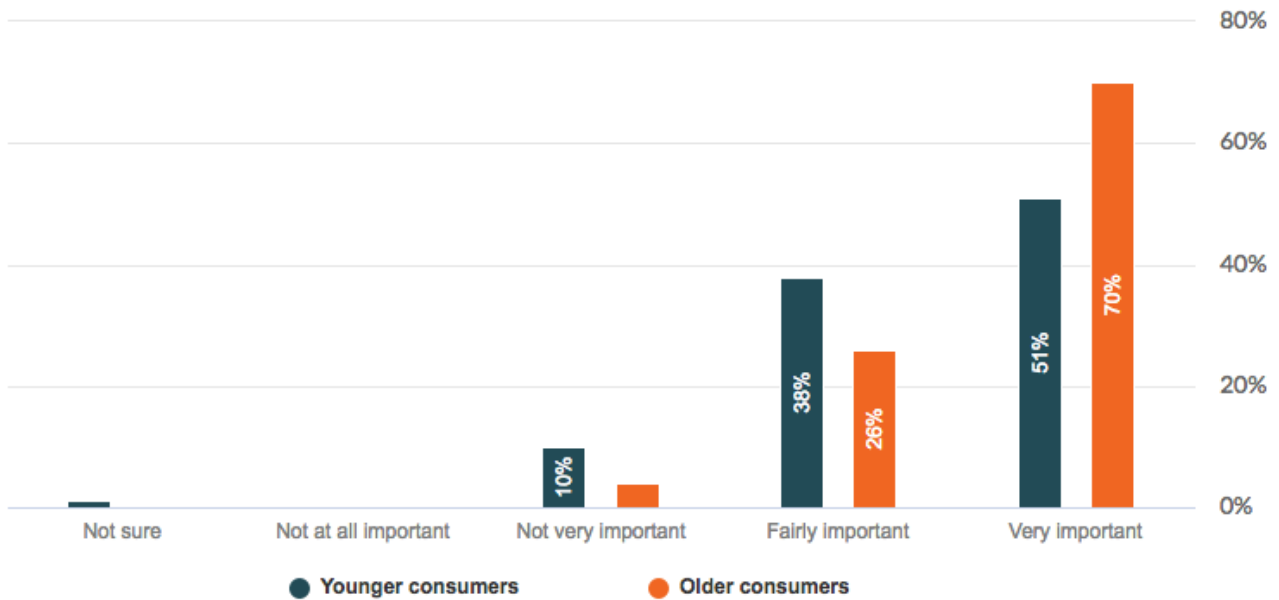


Figure 6: Tools for monitoring activities can only be used with a permission

In figure 6, “tools for monitoring your activities online (such as cookies) can only be used with your permission”, the results show a little more variation in the results than in the earlier questions as half of the younger consumers set the importance of permissions in the monitoring of online activities fairly important or not very important. The other half of the younger consumers still thought this was very important. Similar to the earlier questions, the majority of older consumers set the importance of permissions in the monitoring of online activities as very important. Only 26% of older consumers said this was fairly important and the 4% said this was not very important.

As a conclusion for question 4, when it comes to the importance of confidentiality of emails, both age groups put high importance on their consents whenever they are being tracked or their information is accessed. Also, the confidentiality of their emails and instant messaging is very important. There was not much difference in the results between younger and older consumers, but the older consumers showed a little stronger agreement on importance of the confidentiality permissions whenever information is accessed or collected, than the younger consumers.

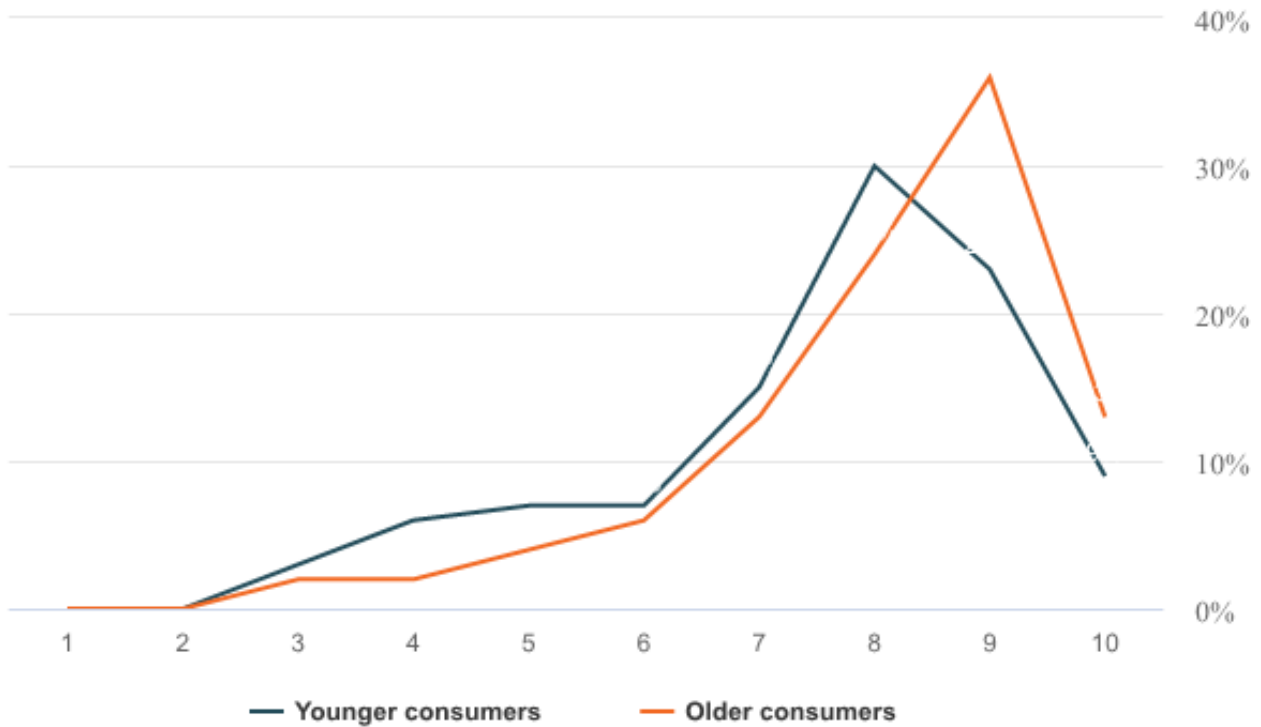


Figure 7: The level of concerns over data privacy online

From trend on figure 7, we can see that overall level of concerns over data privacy online is quite high. Majority, of the respondents set the level of their concerns between 7 and 10. As a conclusion for question 5, the overall level of concerns over data privacy online is between younger and older consumers, it can be concluded that the older consumers generally have set the level of concerns higher than the younger consumers.

4.2.2 Attitudes towards data exchange

Questions 6 and 7 aim to identify differences in attitudes towards data exchange between younger and older consumers.

Sharing data and personal information online is part of the modern economy.

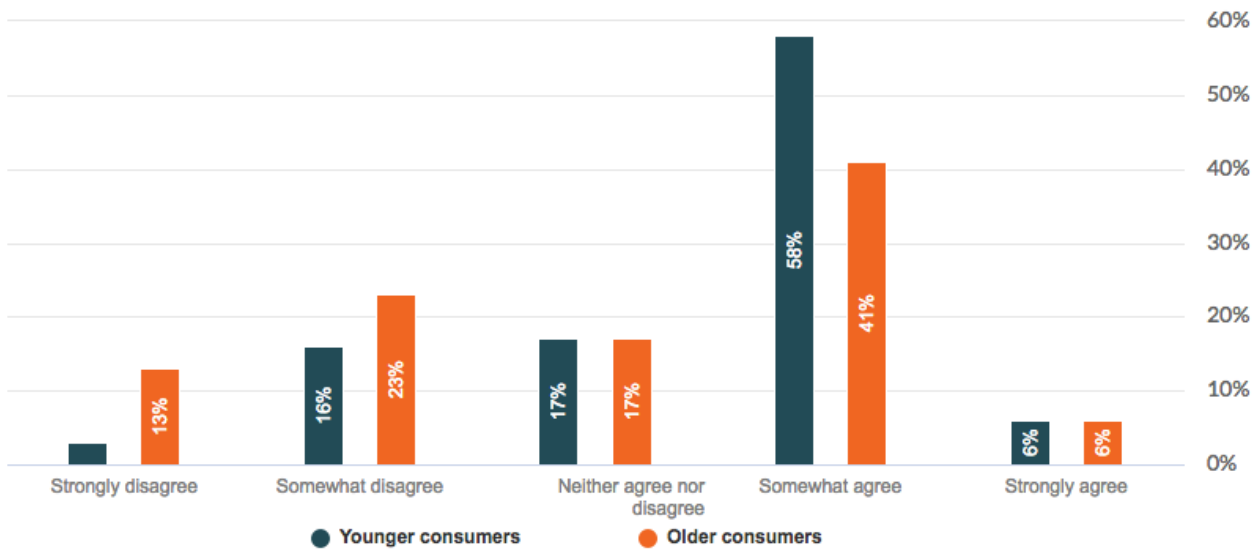


Figure 8: Sharing data and personal information online is part of modern economy

In question 6, the general attitudes towards data exchange were asked. The results on figure 8, “sharing data and personal information online is part of modern economy”, show some differences in the attitudes between younger and older consumers. Even though one fourth of the younger consumer either somewhat disagreed or strongly disagreed with the statement that sharing data and personal information is part of the modern economy, still more than half somewhat agreed or strongly agreed with the statement. Older consumers were slightly more critical and more than one third half disagreed with the statement and a little less than half of them agreed with the statement. 17% of both younger and older consumers neither agreed or disagreed.

The exchange of personal information is essential for the smooth running of modern society.

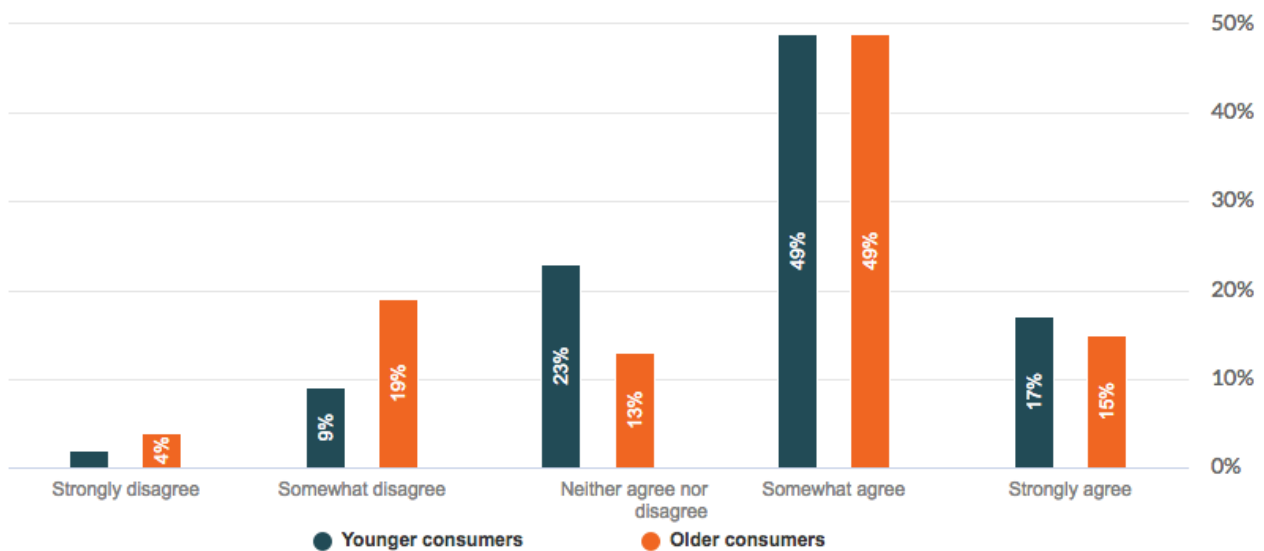


Figure 9: Exchange of personal information is essential for the smooth running of modern society

The results on figure 9, “exchange of personal information is essential for the smooth running of modern society”, show less difference in the attitudes between younger and older consumers. From younger consumer 17% strongly agreed and 49% somewhat agreed with the statement that exchange of personal information is essential for the smooth running of modern society. Also, from older consumers 49% somewhat agreed and 15% strongly agreed with the statement. 13% of younger consumers and 13% of older consumer neither agreed or disagreed. Only 9% of the younger consumers somewhat disagreed and 2% strongly disagreed with the statement. The same results for older consumers where 19% and 4%.

On the whole I am happy with the amount of personal information I give to companies.

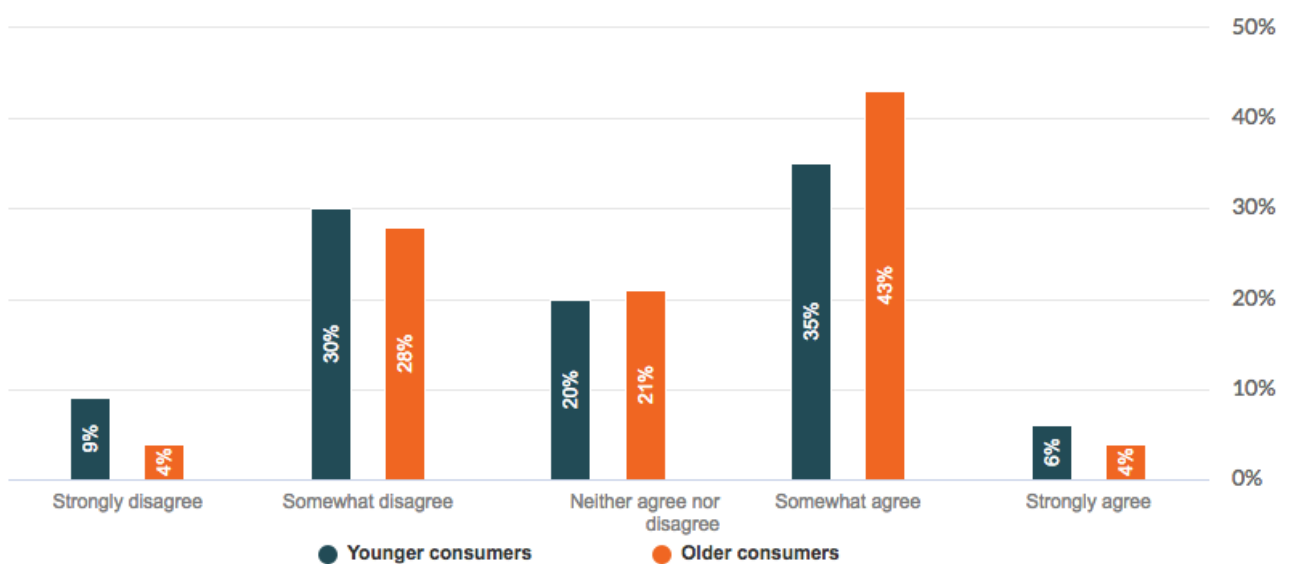


Figure 10: I am happy with the amount of personal information I give to companies

The results on figure 10, “I am happy with the amount of personal information I give to companies”, show again a little difference in the attitudes between younger and older consumers. When asked about how happy the consumers are with the amount of personal information they give to companies, only 6% of younger consumers and 4% of older consumers strongly agreed, though 35% and 43% of younger and older consumers somewhat agreed with the statement. In comparison, 30% of younger consumers and 28% of older consumers somewhat disagreed with the statement, where 9% of younger consumers and 4% of older consumers strongly disagreed with the statement. 20% of younger consumers and 21% of older consumers neither agreed or disagreed.

Today, I feel more aware of how my data is used and collected than in the past.

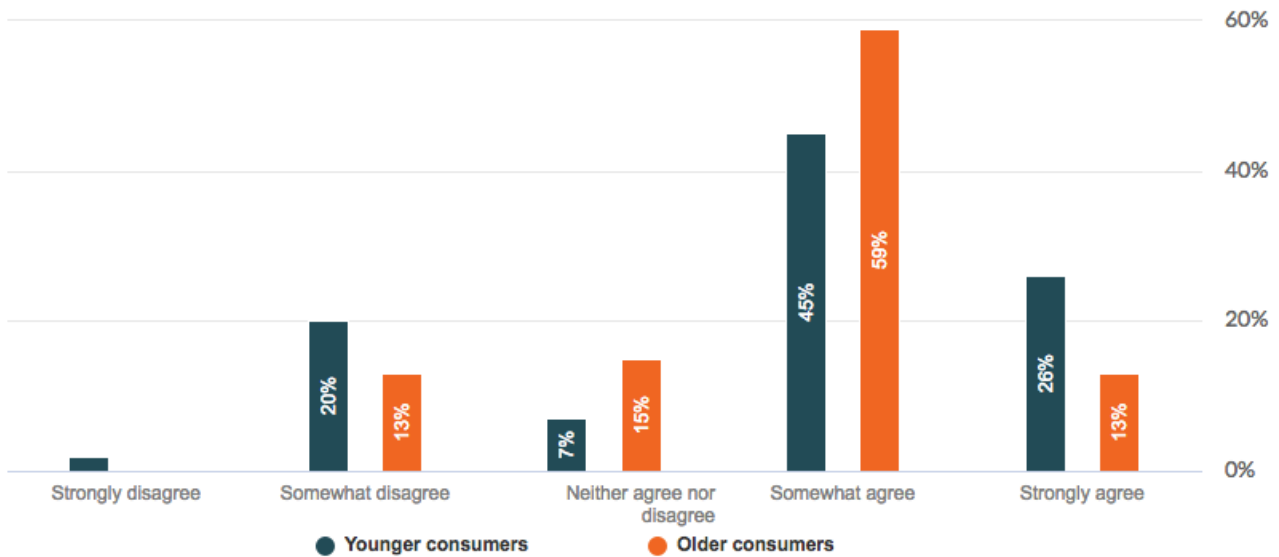


Figure 11: I feel more aware of how my data is used and collected than in the past

According to the results on figure 11, “I feel more aware of how my data is used and collected than in the past”, the majority of both younger and older consumers feel that they are more aware of how their data is used and collected than in the past. 45% of younger consumers somewhat agreed and 26% strongly agreed and of older consumers 59% somewhat agreed and 13% strongly agreed with the statement. Only 2% of younger consumers strongly disagreed and 20% of younger consumers and 13% of older consumers somewhat disagreed with this statement. 7% of younger consumers and 15% of older consumers neither agreed or disagreed.

Today, I feel more comfortable with the idea of exchanging some personal data with companies than I did previously.

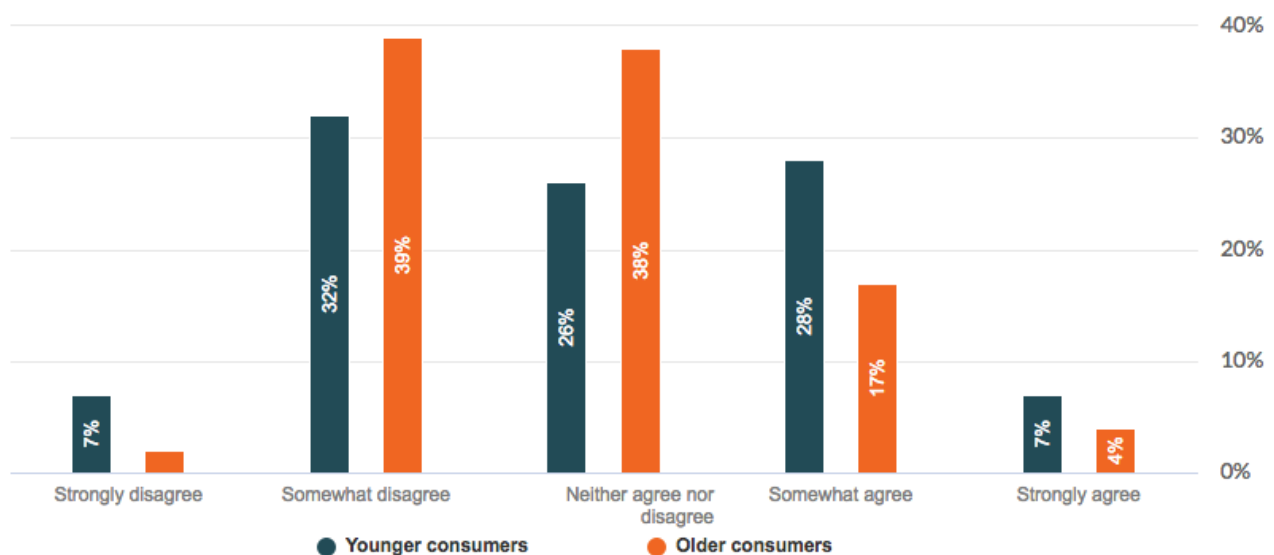


Figure 12: I feel more comfortable with the idea of exchanging some personal data with companies than I did previously

The results on figure 12, “I feel more comfortable with the idea of exchanging some personal data with companies than I did previously”, show some uncertainty with the statement as 26% of younger consumers and 36% of older consumers neither agreed nor disagreed. 32% of younger consumers and 29% of older consumers somewhat disagreed and 7% of younger consumers and 2% of older consumers strongly disagreed with the statement. In comparison, 28% of younger consumers and 17% of older consumers somewhat agreed and 7% of younger consumers and 4% of older consumers strongly agreed with the statement.

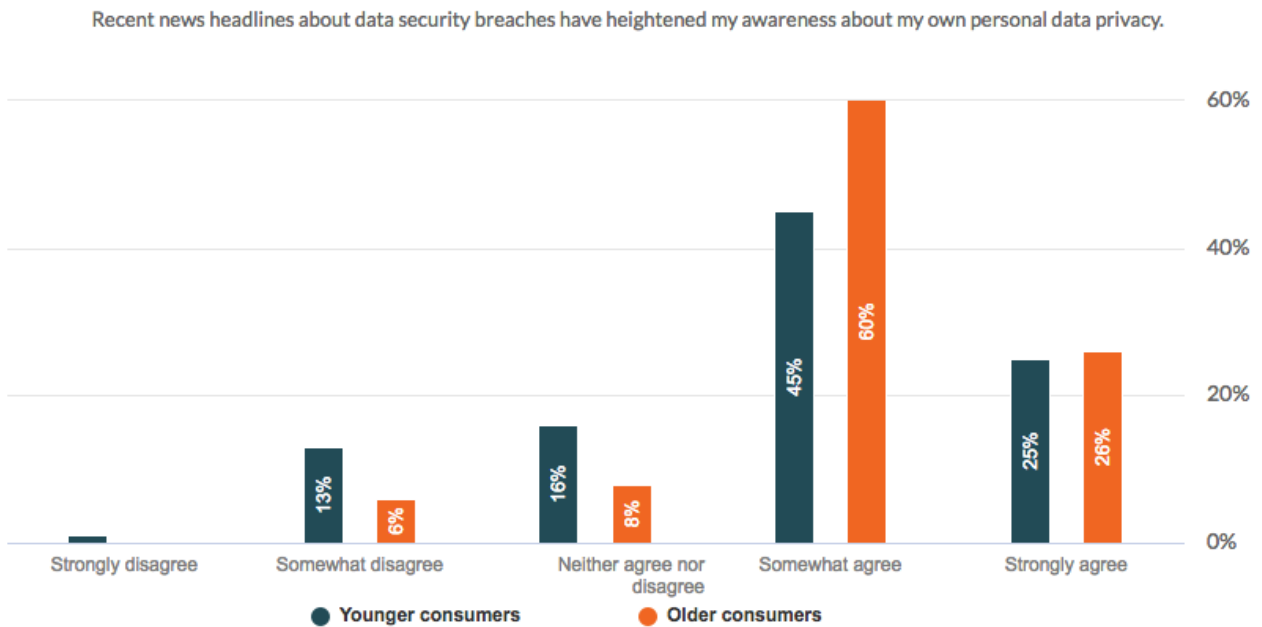


Figure 13: Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy

According to the results on figure 13, “recent news headlines about data security breaches have heightened my awareness about my own personal data privacy”, the majority of younger consumers and almost all older consumers agree that recent news headlines about data security breaches have heightened the awareness about personal data privacy. 25% of younger and 26% of the older consumers strongly agreed and 45% of younger consumers and 60% of older consumers somewhat agreed with this statement. Only 13% of younger consumers somewhat disagreed and 1% of them strongly disagreed. From older consumers 6% somewhat disagreed and none strongly disagreed with the statement. 16% of younger consumers and 8% of older consumers neither agreed or disagreed.

In question 7, the consumers were asked, how much control they feel they have when it comes to data collection and sharing. Generally, the consumers did not feel they have much control and on a scale from 1 to 10 the average in all questions was below 6.

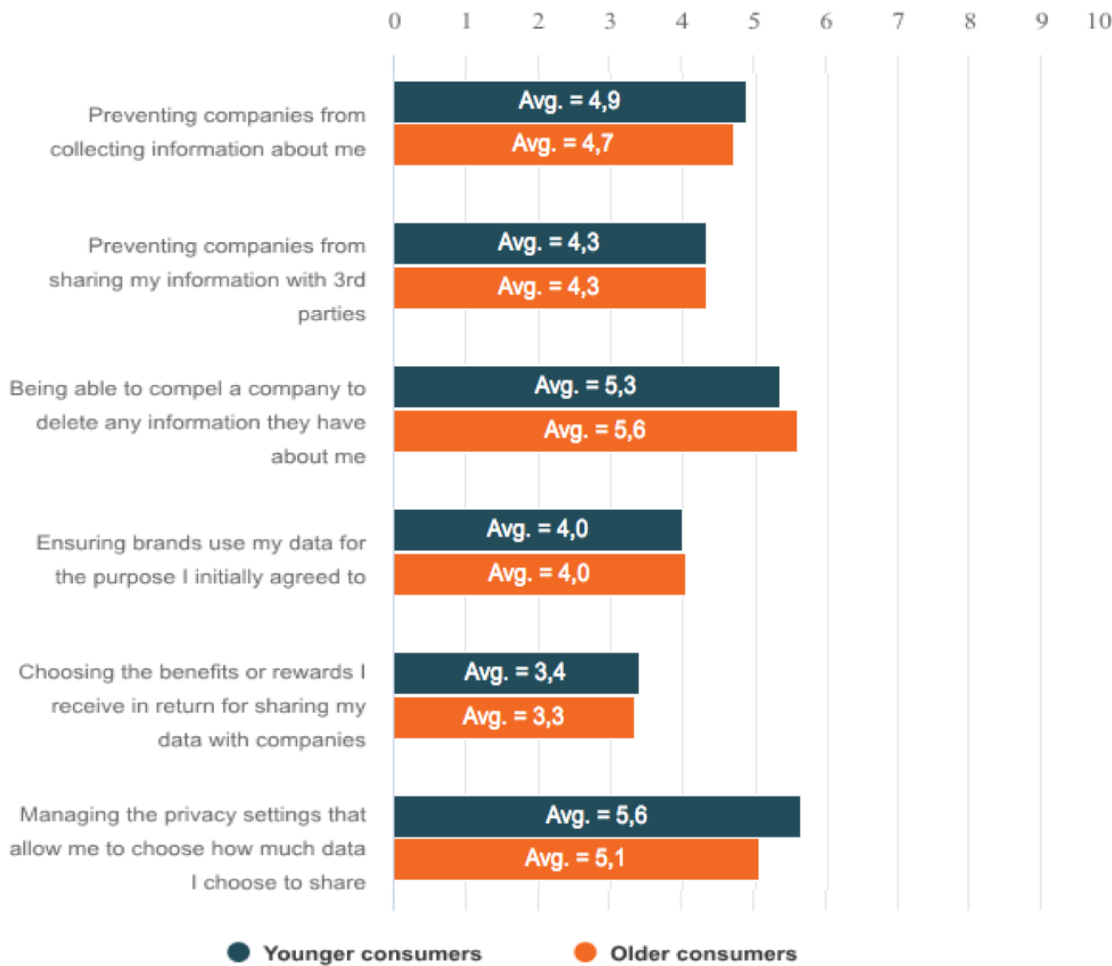


Figure 14: The average level of control in specific areas of data exchange

According to the results in figure 14, “the average level of control in specific areas of data exchange”, areas of data exchange where consumers feel they have some control are preventing companies from collecting information about them, compelling companies to delete any information about them and managing personal privacy setting. Areas where consumers feel they have only little control are ensuring brands use data for the purpose that was initially agreed to, choosing the benefits or rewards received in return for sharing personal data and preventing companies from sharing their data to third parties.

When comparing the results between younger and older consumers, the results show hardly any difference in opinions on how much control consumers have in data collection and sharing. In average, the younger consumers rated the level of control in preventing companies from collecting information about them as 4,9 and older consumers 4,7. The average of the level of control in preventing companies from sharing information for 3rd parties for both groups were 4,3. The average of the level of control in being able to compel a company to delete any information they have about

and individuals was 5,3 for younger consumers and 5,6 for older consumers. the level of concern in ensuring brands use data for the purposes that data subject initially agreed to was in average 4,0 for both groups. The average, the level of control in choosing the benefits or rewards received in return for sharing data with companies was for younger consumers 3,4 and for older consumers 3,3. Finally, when asked about the level of control in managing the privacy setting that allow to choose how much data is shared the average for younger consumers was 5,6 and for older consumers 5,1.

4.2.3 Perceptions in personal data privacy

Questions 8, 9, 10 and 11 aim to compare the perceptions in personal data privacy between younger and older consumers.

In question 8 the consumers were asked what actions they have taken within the past year to secure their data. As seen in the figure 15 below, the most common actions were adjusting the privacy settings on phone and social media as well as deleting or not downloading specific apps or visited websites that were not trustworthy when it comes to privacy. Surprisingly, many of the respondents had taken even multiple actions to protect their privacy and only 3% had not taken any of actions to secure their privacy online.

When comparing the results between younger and older consumers, the older consumers generally were taking more action to secure the privacy of their data by adjusting privacy settings or doing other pre-empt action, only expectation being adjusting the privacy settings on social media, which might be explained by the fact that the overall use of social media is more common among younger consumers. In contrast, the software's for blocking ads or online tracking were mainly used only by younger consumers.

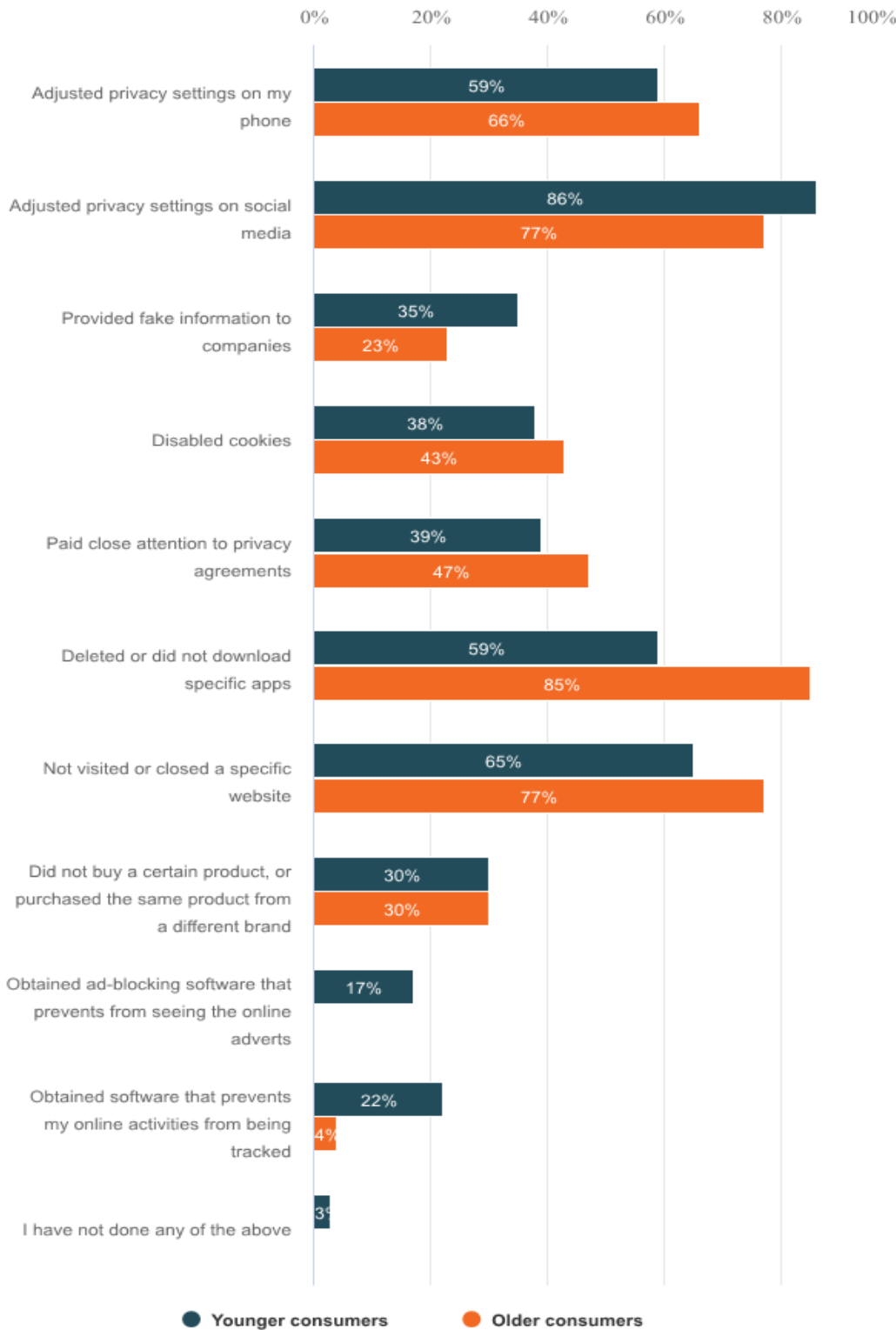


Figure 15: Actions taken to protect personal data

In question 9, consumers were asked about different personal information they were willing to share with companies to be analysed in their software programs in order to send targeted advertisements or coupons to them. As seen in the figure 16, the results show that consumers majority of consumers were willing to share some of their information and only a little more than 30% of both younger and

older consumers said they would not like to share any of the mentioned information. About half of the respondents were comfortable in sharing their purchase history and about one third were willing to share their demographic information. However, only a small part of the respondents was willing to share their online search history and or social media postings. None of the respondents would like to share the content of their emails.

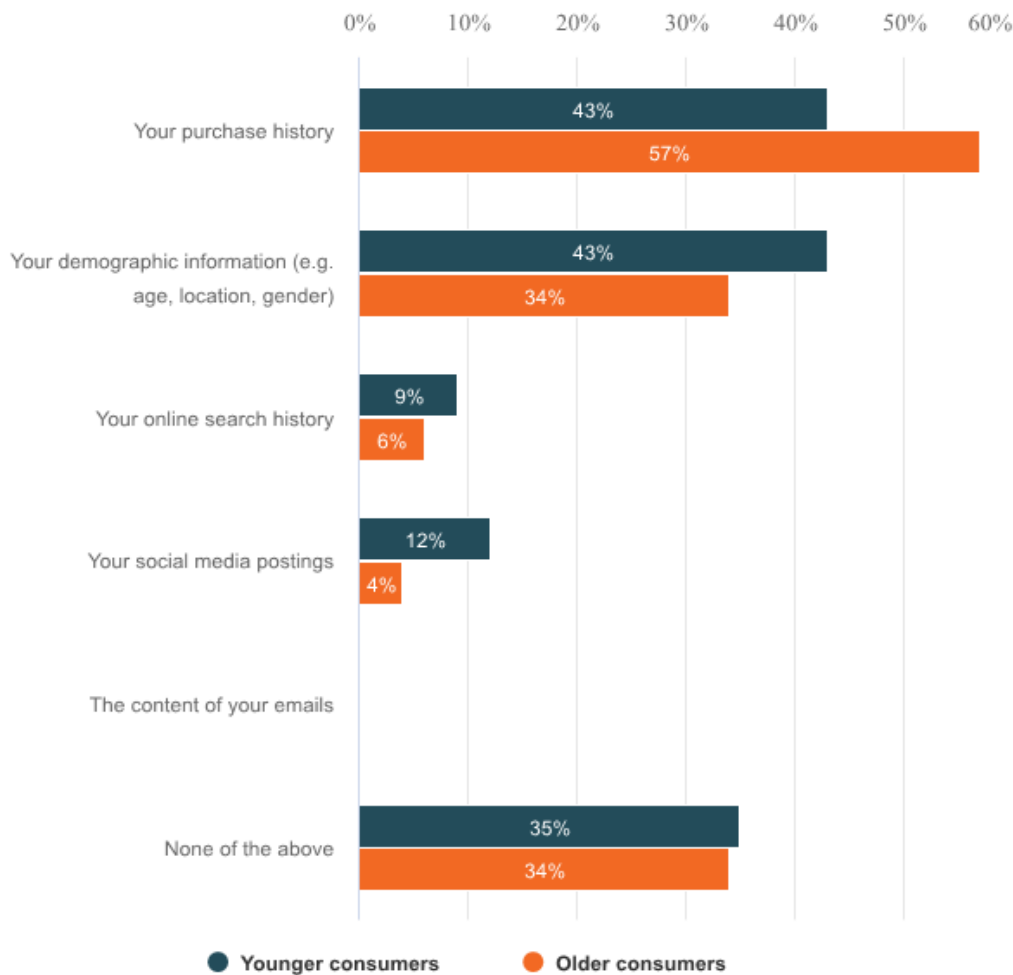


Figure 16: Activities that consumers would allow companies to analyse by using software programs in order to send targeted advertisements or coupons

When comparing the results, the younger consumers seemed to be more willing to share their demographics, online search history and social media content where the older consumers were willing to share their online purchase history.

In question 10, consumers were asked about things that increase their trust in companies in protection their personal information online, most part of the respondents agreed with all of the options.

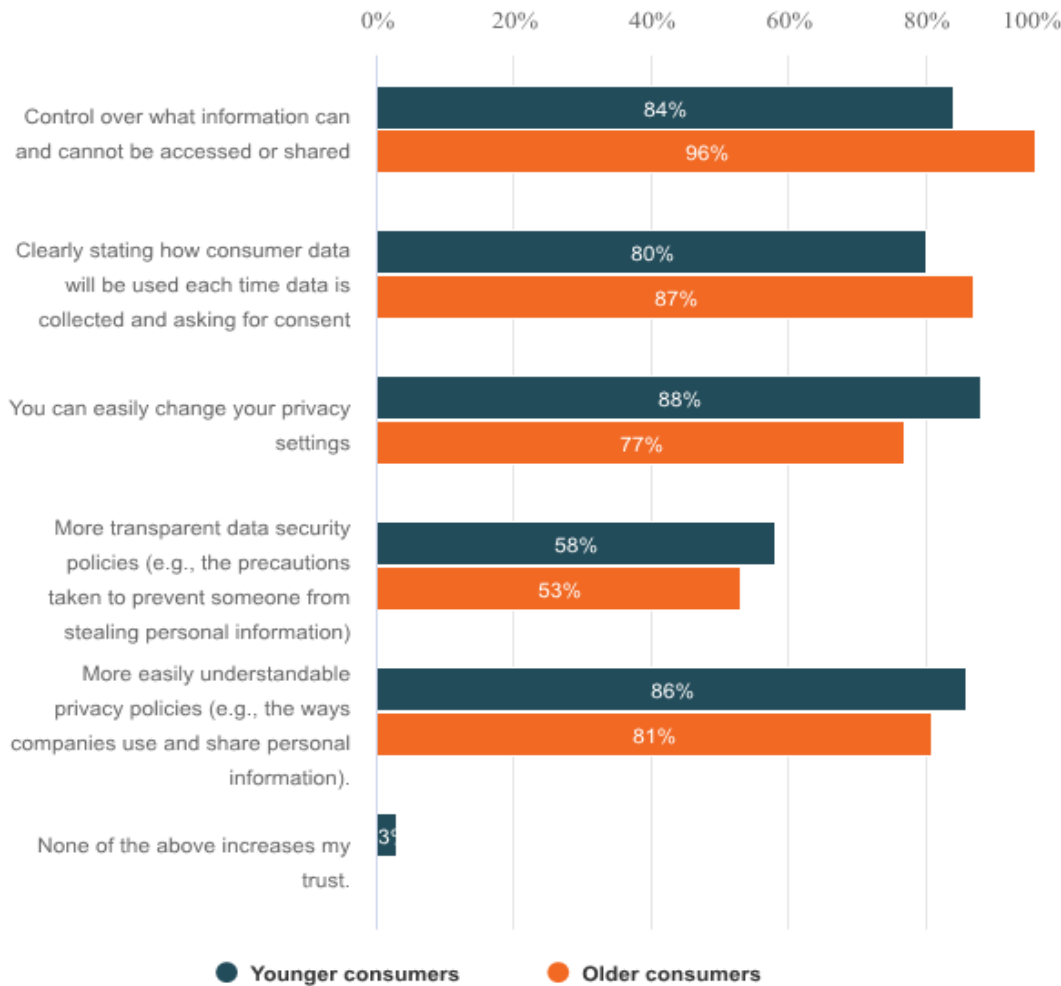


Figure 17: Factors that increase consumers trust in companies in protecting personal information when online

As seen in the figure 17, 84% of the younger consumers and as high as 96% of older consumers said that control over what information can and cannot be accessed or shared would increase their trust. Also, 80% of the younger consumers and 87% of older consumers said that clearly stating how consumer data will be used each time data is collected and asking for consents would increase their trust. 88% of younger consumers and 77% of older consumers said that the ability to easily change the privacy settings increase their trust. However, when asked about the transparent data security policies, only 58% of the younger consumers and 53% of older consumers said this would increase their trust. In contrast, when asked about more easily understandable privacy policies, 86% of younger consumers and 81% of older consumers said it would increase their trust. Only 3% of the younger consumers and none of the older consumers thought none of the options would increase their trust.

When comparing the results between younger and older consumers, the results were quite similar but younger consumers valued more the ability to change privacy settings and nearly all of the

consumers thought that the control over what information can and cannot be accessed or shared would increase their trust.

In question 11, consumers were asked about their general attitudes on data privacy when making purchasing decisions. Generally, majority of consumers were more likely to purchase from companies who protect their information and would avoid purchasing from companies who they did not believe protect their information. According to the results, even a single data breach would impact consumers likelihood to buy from a company in the future, neither were the consumers that forgiving on the data breaches. The opinion of believing that most companies adequately protect consumers had difference in the opinions, some had even a strong response of non-agreement while some felt that companies in fact were protecting their information effectively. However, the consumers did not know which companies best protect their information.

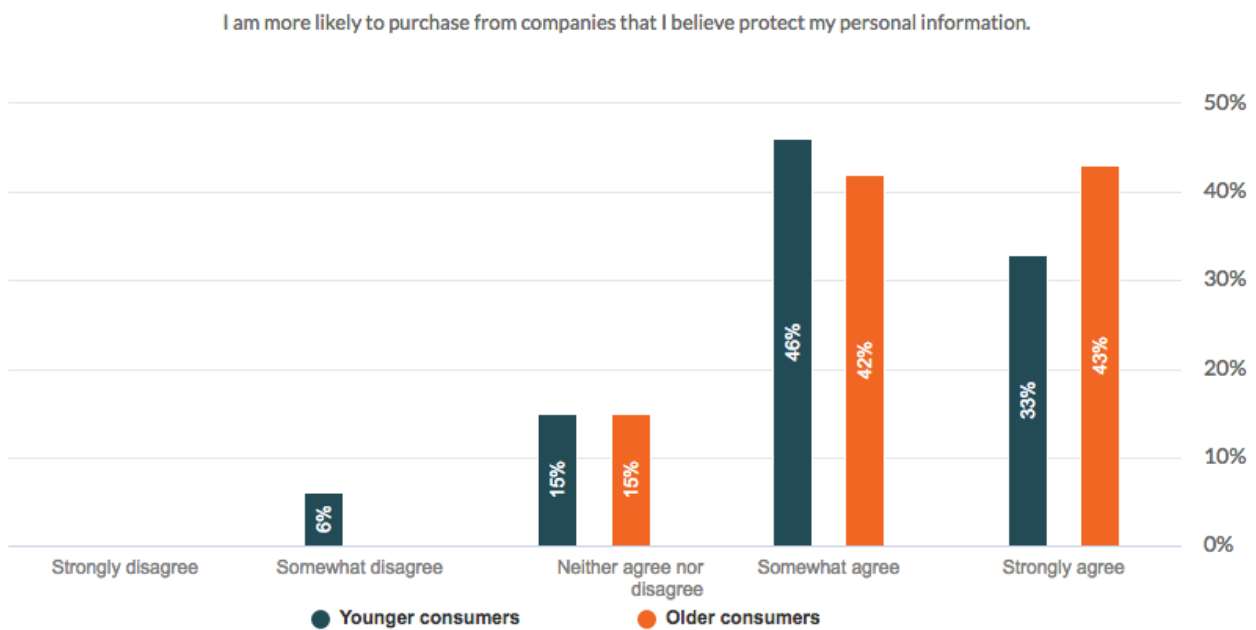


Figure 18: I am more likely to purchase from companies that I believe protect my personal information

The results in figure 18, “I am more likely to purchase from companies that I believe protect my personal information”, show that as high as 33% of younger consumers and 43% of older consumers strongly agree and 46% of younger consumers and 42% of older consumers somewhat agree with that they are more likely to purchase from companies that they believe protects their personal information. Only 15% of both younger and older consumers neither agreed or disagreed and 6% of younger consumers somewhat disagreed with this statement.

I avoid purchasing from companies that I do not believe protect my personal information.

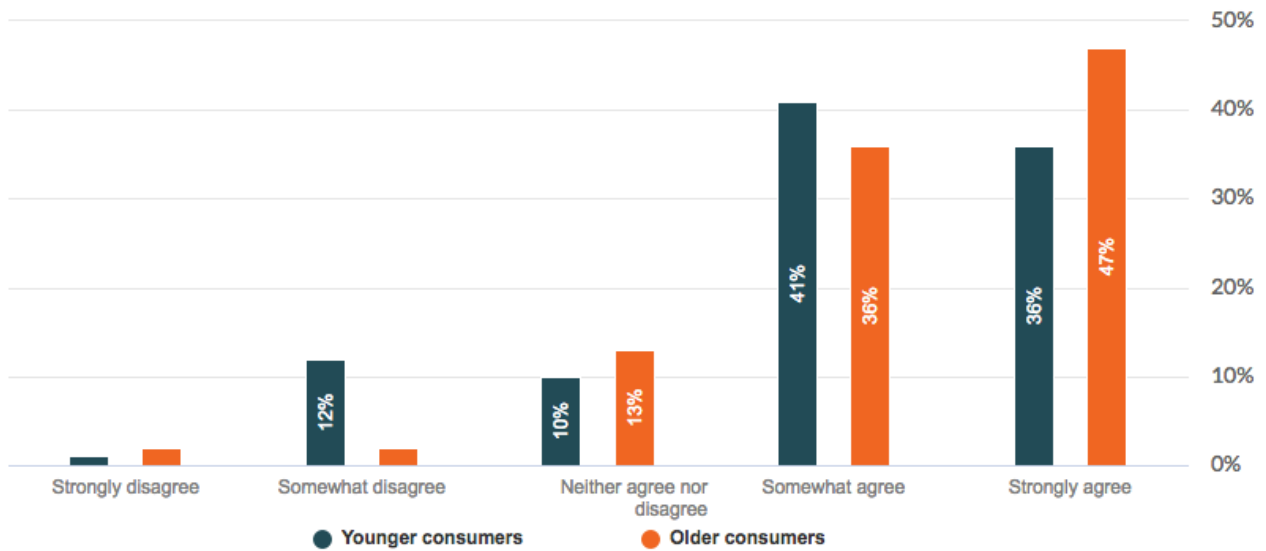


Figure 19: I avoid purchasing from companies that I do not believe protect my personal information

Similarly, the results in figure 19, “I avoid purchasing from companies that I do not believe protect my personal information”, show that 36% of the younger consumers and 47% of the older consumers strongly agreed and 41% of younger consumers and 36% of older consumers somewhat agreed with that they avoid purchasing from companies that they do not believe protect their personal information. Only 4% of the older consumers somewhat or strongly disagreed and 13% neither agreed or disagreed. From younger consumers 1% strongly disagreed, 12% somewhat disagreed and 10% neither agreed or disagreed.

Even a single data breach would negatively impact my likelihood to buy from a company in the future.

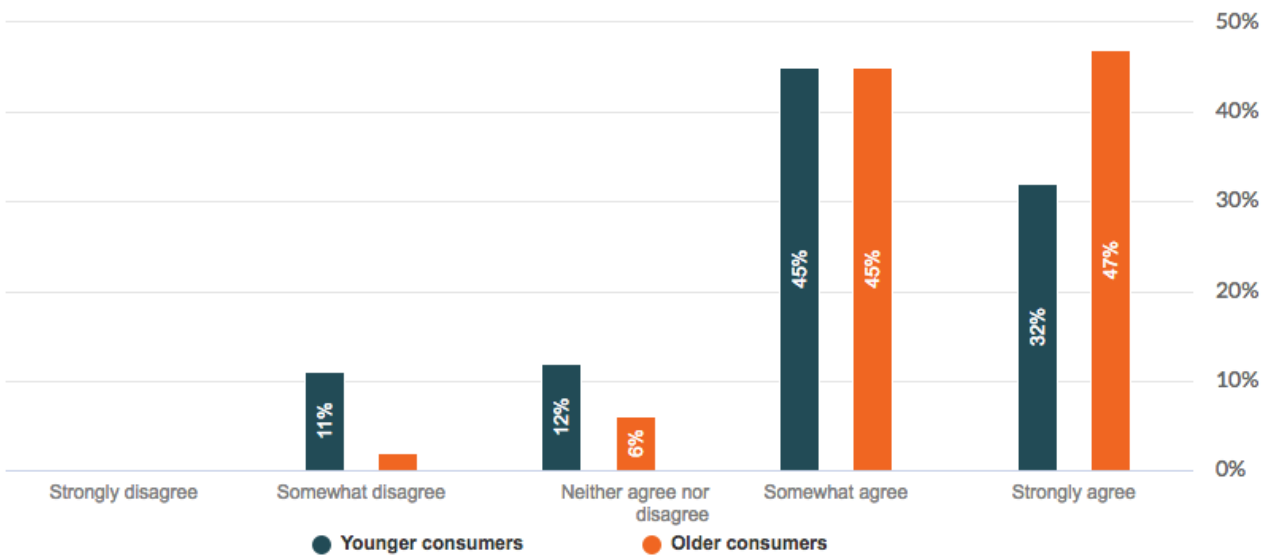


Figure 20: Even a single data breach would negatively impact my likelihood to buy from a company in the future

According to figure 20, “even a single data breach would negatively impact my likelihood to buy from a company in the future”, data security seems to be an important factor for both groups. From younger consumers 32% strongly agreed and 45% somewhat agreed with that even a single data breach would negatively impact their likelihood to buy from a company in the future. From older consumers 47% strongly agreed and 45% somewhat agreed with this. Only 12% of younger consumers and 6% of older consumers neither agreed or disagreed. Still, 11% of younger consumers somewhat disagreed with the statement but only 2% of the older consumers showed any disagreement.



Figure 21: I would be forgiving of company that had one single data breach of my personal data as long as they quickly addressed the issue

The results in figure 21, “I would be forgiving of company that had one single data breach of my personal data as long as they quickly addressed the issue”, show that big part of the consumers was not very forgiving with data breached and 12% of younger consumers strongly disagreed and 20% somewhat disagreed. From older consumers 4% strongly disagreed and 21% somewhat disagreed with the statement. Still, 49% of older consumers and 39% of younger consumers somewhat agreed with the statement and 6% of younger consumers strongly agreed. 23% of younger consumers and 26% of older consumers neither agreed or disagreed.

I believe most companies are adequately protecting my personal information.



Figure 22: I believe most companies are adequately protecting my personal information

According to figure 22, “I believe most companies are adequately protecting my personal information”, consumers are not that sure whether they generally believe that companies are protecting their information. 12% of younger consumers and 8% of older consumers strongly disagreed with this statement and 31% of younger consumers and 28% of older consumers somewhat disagreed. In comparison, 36% of younger consumers and 28% of older consumers somewhat agree and only 4% of younger consumers and 2% of older consumers strongly agreed with this. 17% of younger consumers and 34% of older consumers neither agreed or disagreed.

I know which companies best protect my personal information.

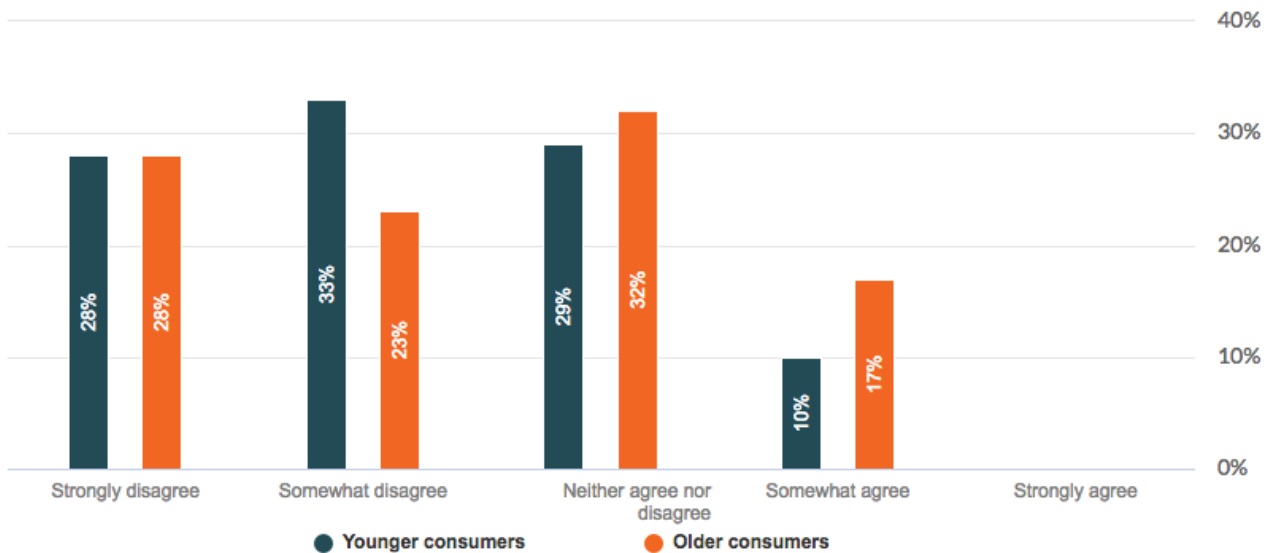


Figure 23: I know which companies protect my personal information

The results in figure 23, “I know which companies protect my personal information”, show that consumers generally don’t know which companies best protect their personal information and 28% of both younger and older consumers strongly felt they did know which companies best protect their information. Also 33% of younger consumers and 23% older consumers somewhat disagreed. Only 10% of younger consumers and 17% of older consumers somewhat agreed with that they knew which companies best protect their information. 29% of younger consumers and 32% neither agreed nor disagreed.

As a conclusion for questions regarding perceptions of personal data privacy, there seems to be some uncertainty in how consumers feel about companies when it comes to data protection. It seems to be an important factor for both younger and older consumers, however many of them are not sure which companies best protect their information. When comparing the attitudes between younger and older consumers, it seems that the data security is a bit more important for older consumers when interacting with companies, at the same time older consumers were more forgiving of possible data breaches. Both groups did show uncertainty on whether they felt that companies are adequately protecting their information and also were generally not sure which companies best protect their information.

4.2.4 Awareness of specific data protection laws

Questions 12 and 13 aim to compare the awareness of specific data protection laws between younger and older consumers.

In question 12, the consumers were asked whether they were aware of the General Data Protection Regulation (GDPR) regulation or not. In figure 24, the results show that most of the consumers are aware about GDPR. Only 19% of the younger and 13% of the older consumers did not know what about the GDPR or were not sure if they knew.

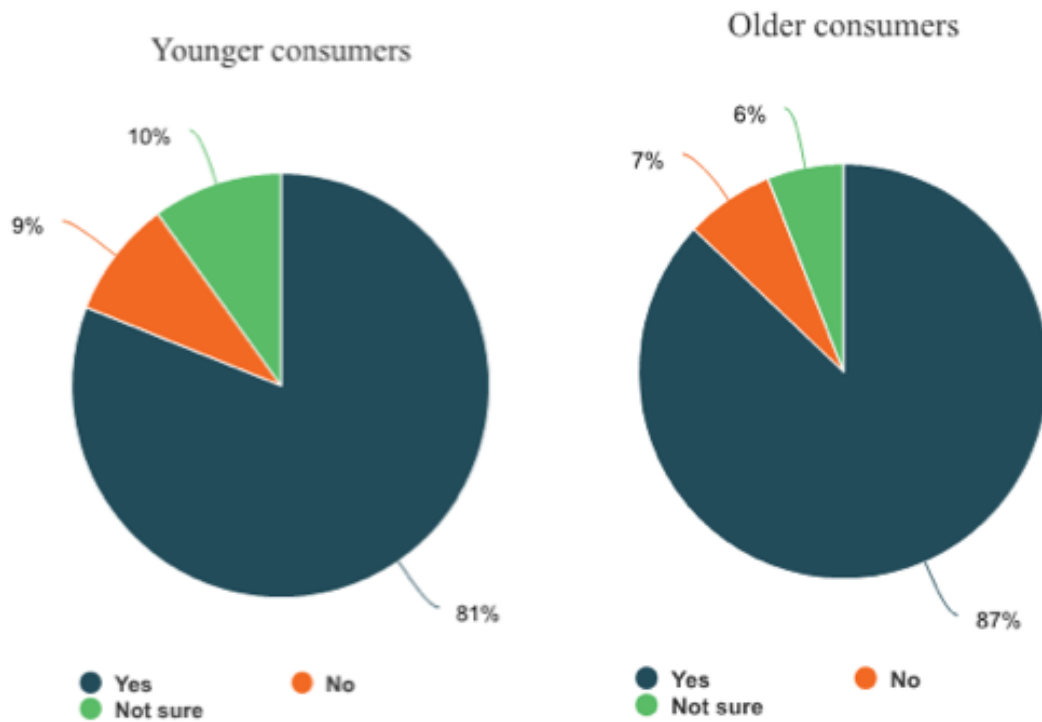


Figure 24: Awareness of the General Data Protection Regulation (GDPR)

When comparing the results between younger and older consumers, it seems that the both younger and older consumers were aware of the new regulation and there is not much difference in the results between the two groups, although the older consumers showed slightly more familiarity with GDPR.

In question 13, consumers were asked whether they were aware of the EU ePrivacy regulation or not. As seen in the figure 25, the results suggest that the consumers are less aware of the ePrivacy regulation than about the GDPR. However, many was not sure about this question and this could refer to the fact that they are aware of the upcoming legal updates but are not aware of the name of the legislation.

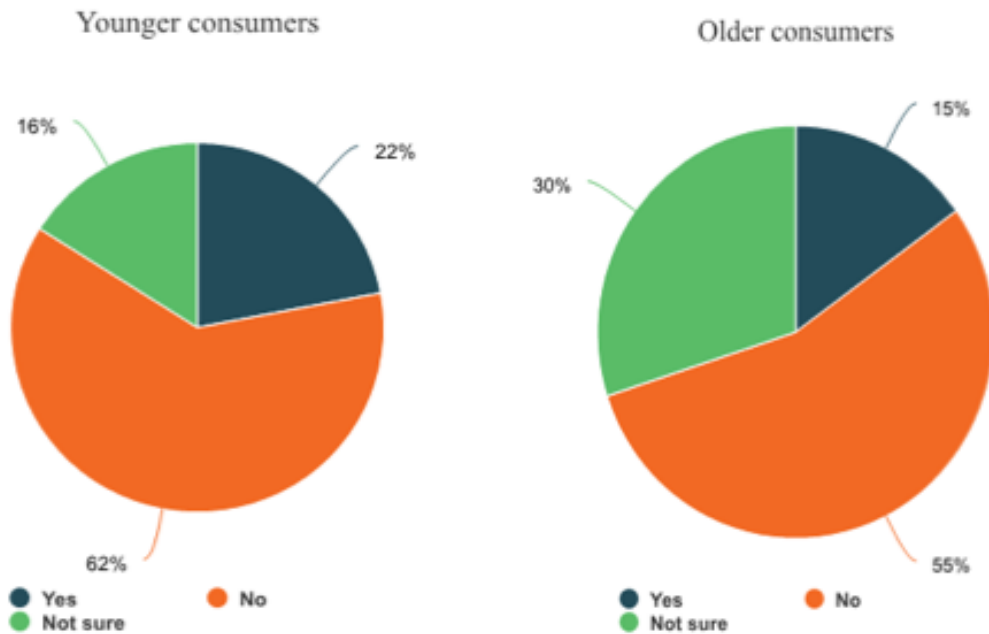


Figure 25: Awareness of the ePrivacy Regulation (ePR)

When comparing the results between younger and older consumers, it seems that the younger consumers are a little more familiar with the ePrivacy regulation. Similar to the results regarding GDPR, there is no significant difference between the two groups. There was also a mentionable part that was not uncertain whether they were familiar with the ePR, especially among older consumers. Due to this, the difference between the younger and older consumers who did not know about ePR was only 7%.

We can conclude that when it comes to awareness of specific data protection laws there is no notable difference between younger and older consumer, however older consumers seemed to be a little bit more familiar with the GDPR, where younger consumers were with the ePR.

4.3 Analysis of variance

The survey results and the variance of the results between younger and older consumers were analysed with analysis of variance (ANOVA). In Appendix 3: ANOVA analysis results, the hypotheses testing results are presented, where we either reject the null hypothesis when p-value is less or equal to the critical value 0.05 or fail to reject the null hypothesis when p-value is more to the critical value 0.05. Questions 8, 9 and 10 were not possible to analyse with ANOVA and therefore more descriptive approach was used.

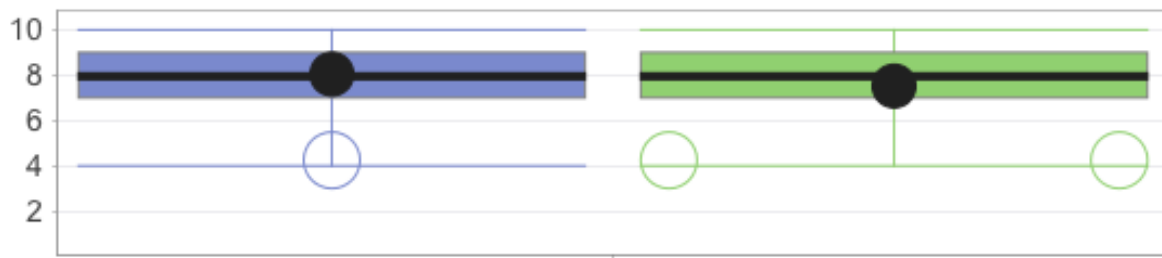
4.3.1 Difference in concerns over online privacy



Figure 26: Analysis of variance in question 4

Question 4 “How important is each of the following to you?” consisted of three different statements. The results in Appendix 3, show that the p-value for the first statement “Your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission’.” is 0.125 and based on that we fail to reject the null hypothesis. The p-value for the second statement “The confidentiality of your emails and instant messages is guaranteed” is 0.631 and based on that we fail to reject the null hypothesis. However, the p-value for the third statement “Tools for monitoring your activities online (such as cookies) can only be used with your permission” is 0.028 and based on this the null hypotheses can be rejected.

On a scale from 1 to 10, how concerned are you about data privacy online these days. 1 is 'not at all concerned' and 10 is 'very concerned'.



On a scale from 1 to 10, how concerned are you about da...

- Age of respondent:Older consumers (N=47)
- Age of respondent:Younger consumers (N=69)

Figure 27: Analysis of variance in question 5

As seen in Appendix 3, the p-value for the question 5 “On a scale from 1 to 10, how concerned are you about data privacy online these days. 1 is ‘not at all concerned’ and 10 is ‘very concerned’.” is 0.109 and based on that we fail to reject the null hypothesis.

4.3.2 Difference in attitudes towards data privacy

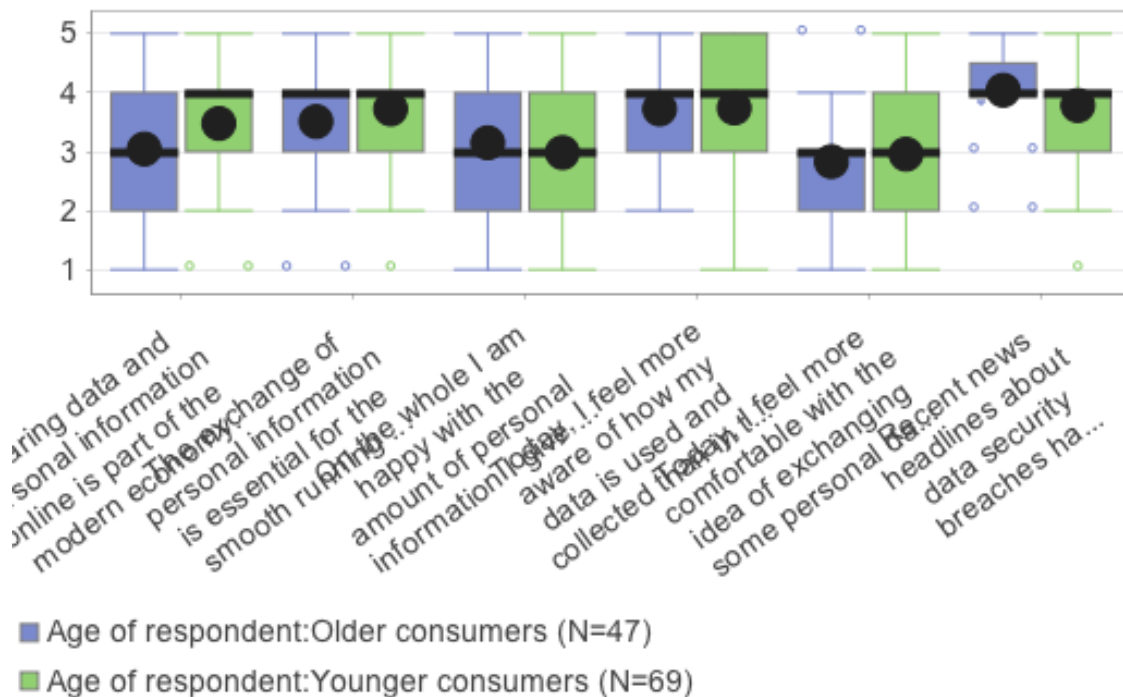


Figure 28: Analysis of variance in question 6

Question 6, “How much do you agree or disagree with the following statements?” consisted of six different statements. The results in Appendix 3, show that the p-value for the first statement “Sharing data and personal information online is part of the modern economy” is 0.030 and based on this the null hypotheses can be rejected. The p-value for the second statement “The exchange of personal information is essential for the smooth running of modern society.” is 0.255 and based on that we fail to reject the null hypothesis. The p-value for the third statement “On the whole I am happy with the amount of personal information I give to companies” is 0.425 and based on that we fail to reject the null hypothesis. The p-value for the fourth statement “Today, I feel more aware of how my data is used and collected than in the past” is 0.935 and based on that we fail to reject the null hypothesis. The p-value for the fifth statement “Today, I feel more comfortable with the idea of exchanging some personal data with companies than I did previously” is 0.511 and based on that we fail to reject the null hypothesis. The p-value for the sixth statement “Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy” is 0.140 and based on that we fail to reject the null hypothesis.

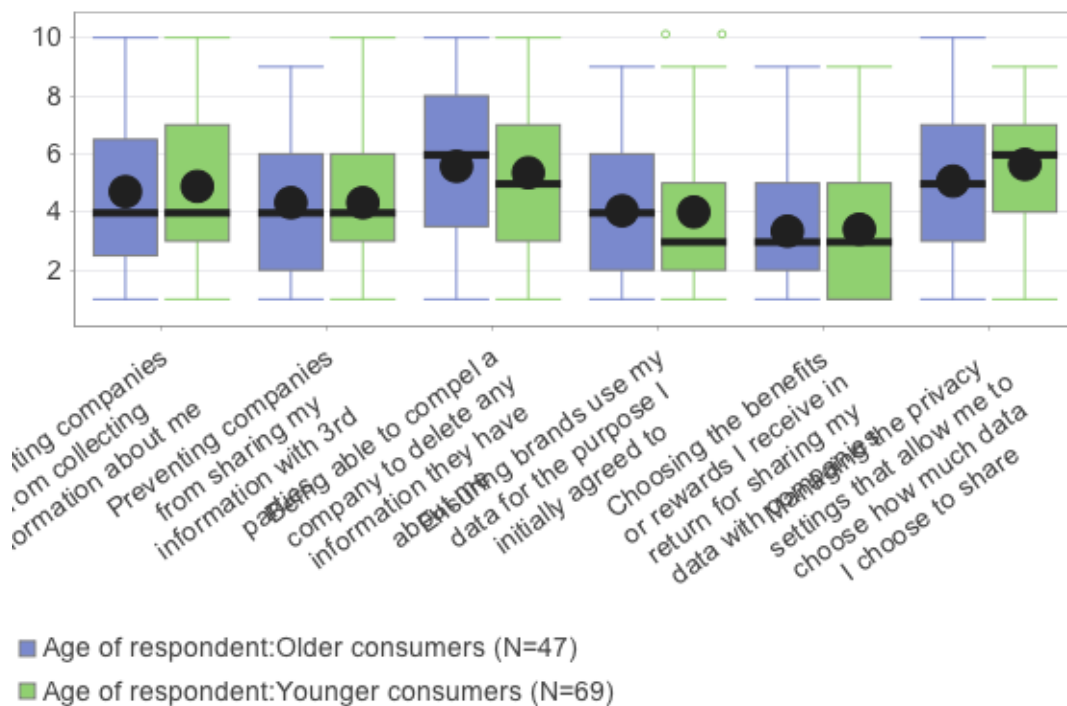


Figure 29: Analysis of variance in question 7

In question 7, “On a scale from 1 to 10, how much control do you think you have over the following.” consisted of six different actions. The results in Appendix 3, show that the p-value for the first point “Preventing companies from collecting information about me” is 0.709 and based on this the null hypotheses can be rejected. The p-value for the second point “Preventing companies from sharing my information with 3rd parties” is 0.999 and based on this the null hypotheses can be rejected. The

p-value for the third point “Being able to compel a company to delete any information they have about me” is 0.636 and based on this the null hypotheses can be rejected. The p-value for the fourth point “Ensuring brands use my data for the purpose I initially agreed to” is 0.925 and based on this the null hypotheses can be rejected. The p-value for the fifth point “Choosing the benefits or rewards I receive in return for sharing my data with companies” is 0.879 and based on this the null hypotheses can be rejected. The p-value for the sixth point “Managing the privacy settings that allow me to choose how much data I choose to share” is 0.179 and based on this the null hypotheses can be rejected.

4.3.3 Difference in perceptions of personal data privacy

In question 8 the consumers were asked what actions they have taken within the past year to secure their data. The results show that there are some differences. Older consumers seem to mainly protect their personal data privacy with preventative measures and by putting more attention to privacy agreements than younger consumers, while younger consumers find the ad-blocking software or software that prevent tracking and adjusting the privacy settings an effective way of personal data privacy protection.

In question 9, consumers were asked about different personal information they were willing to share with companies to be analysed in their software programs in order to send targeted advertisements or coupons to them. The results show that there are some differences. Younger consumers seem to be more open for sharing data about their online activities, but older consumers were more comfortable of sharing their purchasing history.

In question 10, consumers were asked about things that increase their trust in companies in protection their personal information online, most part of the respondents agreed with all of the options. The results show that there are some differences. Older consumers seem to expect more transparency from company’s side, where younger consumers want to have more control over data sharing.

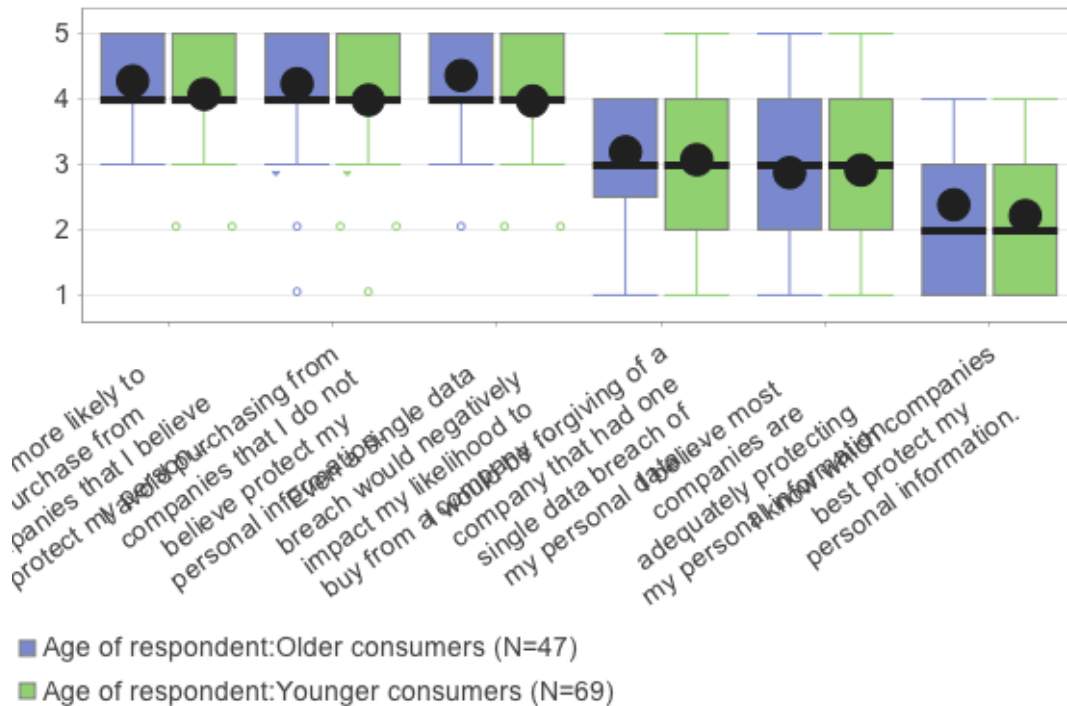


Figure 30: Analysis of variance in question 11

Question 11, “How much do you agree or disagree with the following statements?” consisted of six different statements. The results in Appendix 3, show that the p-value for the first statement “I am more likely to purchase from companies that I believe protect my personal information.” is 0.177 and based we fail to reject the null hypothesis. The p-value for the second statement “I avoid purchasing from companies that I do not believe protect my personal information” is 0.186 and based on that we fail to reject the null hypothesis. The p-value for the third statement “Even a single data breach would negatively impact my likelihood to buy from a company in the future” is 0.018 and based this we can reject the null hypothesis. The p-value for the fourth statement “I would be forgiving of a company that had one single data breach of my personal data as long as they quickly addressed the issue.” is 0.554 and based on that we fail to reject the null hypothesis. The p-value for the fifth statement “I believe most companies are adequately protecting my personal information.” is 0.843 and based on that we fail to reject the null hypothesis. The p-value for the sixth statement “I know which companies best protect my personal information.” is 0.389 and based on that we fail to reject the null hypothesis.

4.3.4 Difference in awareness of specific data privacy laws

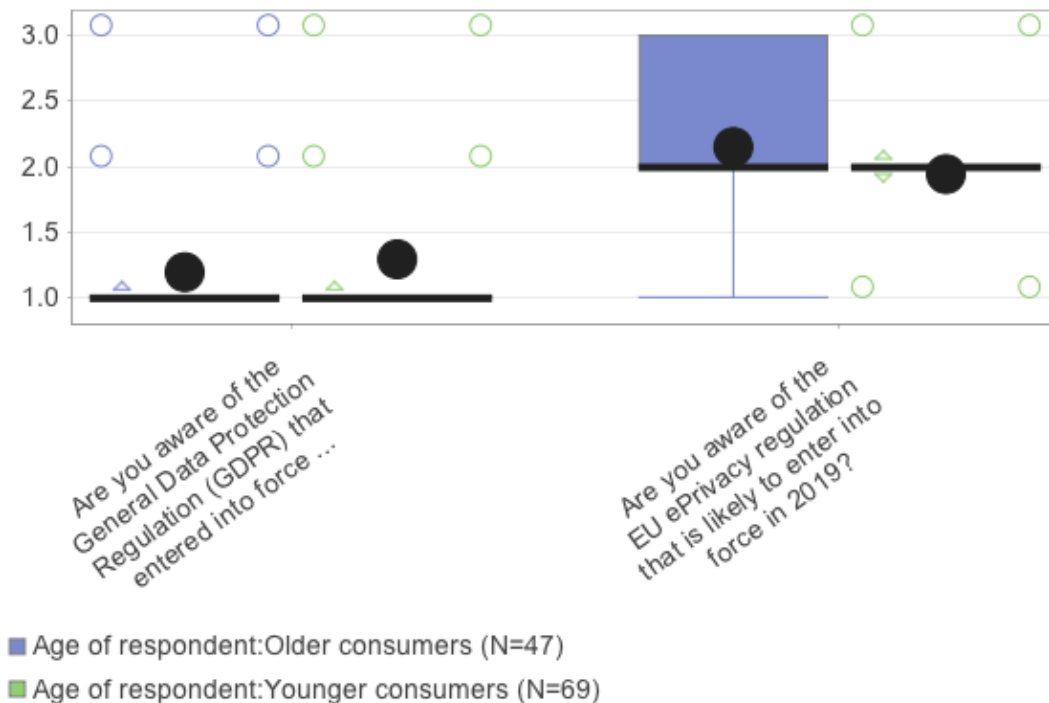


Figure 31: Analysis of variance in questions 12 and 13

In question 12 “Are you aware of the General Data Protection Regulation (GDPR) that entered into force in May 2018?” based on the results, as seen in Appendix 3, the p-value is 0.390 and therefore we fail to reject the null hypothesis. Similarly, in question 12 “Are you aware of the EU ePrivacy regulation that is likely to enter into force in 2019?” based on the results, as seen in Appendix 3, the p-value is 0.087 and therefore we fail to reject the null hypothesis.

4.4 Summary of findings

The aim of the research is to explore the differences in attitudes towards data privacy between younger and older consumers. Although the results show that in most cases there is no significant difference between the younger and older consumers, in three statements there was a significant difference. When comparing the results of younger and older consumers, the results show that younger consumers put less the importance of permissions for tools and monitoring of activities online. Younger consumers also agree more with the statement that sharing data and personal information online is part of the modern economy did result significant difference but do not feel that

We can conclude that there are some differences and main differences in attitudes towards data privacy between younger and older consumers lie on online privacy concerns, attitudes towards data exchange and perception of personal data privacy but not in awareness of specific data protection laws. In addition to this, some questions in relation to perceptions of personal data privacy could not

be analysed with ANOVA and therefore more descriptive approach was used. Based on the results we can suggest that younger consumers find the ad-blocking software or software that prevent tracking and adjusting the privacy settings an effective way of personal data privacy protection. Younger consumers also seemed to be more open for sharing data about their online activities, but older consumers were more comfortable of sharing their purchasing history. Furthermore, Older consumers seemed to expect more transparency from company's side, where younger consumers want to have more control over data sharing.

4.5 Discussion

In this chapter, the findings are discussed with regard to research question and earlier studies. Explanation of results on each question is given considering whether the results were expected or if there were anything unexpected or unusual trends.

Generally, the consumers are very concerned about their privacy online. Information confidentiality is increasingly important for consumers. Consumers want to have control over what information is collected about them and therefore their permission should be asked anytime their personal information is accessed. Suggestively, there are some differences in concerns over online privacy between younger and older consumers. According to Direct Marketing Association (DMA 2018), younger consumers are less concerned about online privacy and are more likely to adopt pragmatic or unconcerned attitude. However, the results from this study suggests that younger consumers put less the importance of permissions for tools and monitoring of activities online.

Consumers feel they have only little or almost no control over their personal data but seem to be more aware of how data is used and collected than earlier. Consumers understand the importance of data exchange and feel that exchange of personal information is essential for the smooth running of modern society. There have been multiple unfortunate data breaches lately and as it turns out, the recent news headlines about data security breaches seemed to have heightened awareness about personal data privacy among consumers. It was expected that there are some differences in attitudes towards data exchange between younger and older consumers. Direct Marketing Association (DMA 2018), younger consumers are more comfortable with sharing their data for companies, but the results from this study show that the difference rather lies on that younger consumers agree more with the statement that sharing data and personal information online is part of the modern economy.

Consequential to the increased awareness of data privacy, the consumers are acting to secure their personal data. More than half of the consumers stated that they have adjusted the privacy settings

on their phone and social media sites. Many have also deleted or not downloaded specific applications and not visited particular websites due to privacy concerns. However, not many seemed to have disabled cookies which could be explained due to the fact that most consumers see data exchange as a necessary in the modern society. Study by Deloitte University Press' (Conroy & Milando & Narula & Singhai 2014) suggest that younger consumers take more proactive action to protect their data than older consumers. However, the results from this study propose that the two age groups take different approach in securing their personal data. Older consumers seem to mainly protect their personal data privacy with preventative measures and by putting more attention to privacy agreements than younger consumers, while younger consumers find the ad-blocking software or software that prevent tracking and adjusting the privacy settings an effective way of personal data privacy protection.

Even though consumers say they prefer personalised content over any other type of content, there is some hesitation on sharing personal online activities for companies to analyse by using software programs in order to send targeted advertisements. Small part even states that the they would not be willing to share any information about their activities. In contrast, majority of consumers are willing to share some information such as purchasing history and demographics, but only small part would share their online search history or social media postings. What consumers are not comfortable to share is the content of their emails, as it is probably the most private source of information in this case. Younger consumers seem to be more open for sharing data about their online activities, yet older consumers are more comfortable of sharing their purchasing history.

Consumers expect companies to be open of how they collect, use and share data. Transparency over how data is collected and used as well as giving consumers control over what information can and cannot be accessed or shared increases their trust in companies in protection their personal information online. Older consumers expect more transparency from company's side, where younger consumers want to have more control over data sharing. Consumers want that companies clearly state how data is used and ask consents each time data is collected. The consumers also want to have the possibility to easily change their privacy settings and easily understandable privacy policies.

Data privacy plays an important role in the purchasing decision of consumers. It is notable that consumers are more likely to purchase from companies that they believe protect their personal information. The trust in a business is an important factor in consumers' willingness to share data and they expect companies to adequately protect their information they wish to share with them. To build consumer trust it is important for businesses to safeguard customer data and take a proactive approach to data protection. As expected, there was some differences in the attitudes between

younger and older consumers and the results show that younger consumers less agreed with the statement that even a single data breach would negatively impact consumers' likelihood to buy from a company in the future.

Most consumers seem to be aware of the latest data protection regulation GDPR but not many is yet familiar with ePR. Unexpectedly, there was no significant differences in the awareness of specific data protection laws between younger and older consumers. Although Direct Marketing Association (DMA 2018) did suggest that younger consumers are more familiar with the GDPR than older consumers, such conclusion could not be made with this study.

Finally, by reviewing the results on each sub-question the main research question can be answered. Based on the earlier studies it was expected that there are differences in attitudes towards data privacy between younger and older consumers. The results from this study is somewhat opposing for the earlier researched. There were couple of cases where results suggest a significant difference between the two age groups, but these were different from the results of earlier researches. In any case, it can be concluded that there are some differences in consumers' attitudes towards data privacy between younger and older consumers. First of all, younger consumers did not find it as important that tools for monitoring your activities online can only be used with your permission and suggest that younger consumers are not as concerned about online tracking than older consumers. Similarly, younger consumers agreed more that sharing data and personal information online is part of the modern economy, which suggests that younger consumers are somewhat more accepting of the sharing of personal information, which could be explained with the theory of "digital natives" that was presented in the literature review. Finally, the results suggest that there is a significant difference on the agreement that even a single data breach would negatively impact my likelihood to buy from a company in the future. Younger consumers had not such strong agreement with this statement and it suggests that a data breach would more negatively affect the customer relationship with older consumers and younger consumers maybe puts more weight on the brand loyalty and overall experience.

5 CONCLUSIONS, LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

In this chapter, a summary of the study is provided to highlight the main points of the research. After this, general conclusions are made to reason the outcomes. In addition, research limitations are overviewed to evaluate the validity of the data and reliability of the research. Finally, some

suggestions for further research are presented to provide to further test the theory and gaps identified in this research.

5.1 Summary

This study was conducted to investigate consumers' attitudes towards data privacy that has been a growing concern in recent years. Based on the earlier studies, there are differences in attitudes towards data privacy between younger and older consumers. According to Direct Marketing Association younger consumers feel they have more control over their data and show more acceptance of data exchange. Similarly, the Deloitte University Press' suggests that the willingness to share information with companies differs by age. The older consumers show less confidence in sharing personal information, but younger consumers are taking more protective actions to secure their data. Similarly, the results suggest that the understanding for data protection laws is higher among younger consumers than older consumers. Furthermore, younger consumers are most likely to adopt pragmatic or unconcerned attitude. This study aims to research the effect of age on attitudes towards data privacy between younger and older consumers. An online survey questionnaire was conducted in order to collect data for statistical analysis. Analysis of variance was used to compare the results between younger and older consumers and to identify whether there is a significant difference in the results. As it turns out, there are some differences in the attitudes towards data privacy between younger and older consumers in relation to online privacy, data exchange and perceptions in personal data privacy. These differences lie on the importance of tools and monitoring activities online can only be used with permission, agreement on the statement that sharing data and personal information online is part of modern economy and that even a single data breach would negatively impact persons likelihood to buy from a company in the future. In addition, younger consumers seem to take more proactive action to protect their personal data where older consumers shift this responsibility to companies.

5.2 General conclusions

Consumer are concerned about their privacy online more than ever and data protection has become an important factor in the purchasing decision of consumers. At the same time consumers are increasingly aware of personal data privacy and companies need to insure their costumers' data is adequately protected. The transparency in how the company collects, manages and shares the information is the key when building consumers' trust. There are some differences in the attitudes towards data privacy between younger and older consumers. Younger consumers, who are also referred as the "digital natives", see sharing of personal information online as a part of the modern

economy and similarly do not put high importance on the consents whenever their activities are being tracked online. Furthermore, younger consumers are not as worried about single data breaches and assumedly but set more importance on general customer experience and brand loyalty. Finally, younger consumers take more proactive action such as adjust their privacy settings and use data security software's to protect their personal data where older consumers shift this responsibility to companies.

It is expected that the consumer product companies are benefiting on the knowledge gained from this research and adjust their privacy policies in accordance to their customers' preferences. Companies should not be too pessimistic about the future but to communicate the benefits of sharing data to consumers. When it comes to data exchange, the most important thing is trust, as it is an important factor in consumers' willingness to share data and the level of trust between company and customer is based on a commitment to the quality of that customer experience. Consumer trust can and should be won by allowing consumers to have more information and control over how their personal data is used. The trust in a business is an important factor in consumers' willingness to share data, the consumers state they expect companies to adequately protect and secure their data and they are more willing to share their personal information when companies are transparent about data security and provide clear privacy policies.

These results do not only indicate the situation now, but from results of younger consumers it can be predicted what direction are the attitudes going in the future as the generational shift will occur. It is expected that consumers' growing awareness and critical attitude towards data privacy will be an increasingly important factor in the processing of personal data in the future. Thus, both the law makers and consumer product companies need to continue trying to balance the customer's right to privacy with the legitimate interests of companies and the rapid developments in technology.

5.3 Limitations

This study has some potential limitations, that affects its validity and reliability. These limitations are divided into two groups: those that result from the methodology and those that result from issues with the researcher.

Considerations concerning the survey research technique

First of all, there are some criticism on using Internet as a survey tool, as some argue that people who can be reached for surveys on Internet are a representative sample of the broader population. In this case, it is expected that people who are active online users have more experience and

knowledge over data privacy and as the aim is to generalise a phenomenon within larger population, the sample is somewhat bias sample for general population.

Considerations concerning the questionnaire design

The questionnaire design had some limitation as well. In the questionnaire, the age was divided into groups and the respondents did not give out their exact age. Consequence there were some limitations in the presentation of the results. Without this limitation there could for example Pearson's correlation coefficient could have been used to investigate the relationship between the two variables, but in this case both variables should have been continuous. However, study could be repeated by to get more coherent age information and this way get more possibilities for data analysis.

Considerations concerning the delimitation

Due to the delimitation the study was conducted in Finland, therefore it is all respondents are Finnish residents and the results in other countries may vary. However, at least the Western countries are quite similar in regard to technological developments and culture and therefore the results may be somewhat generalised in that sense. The research could also be repeated in another country to see whether the results are similar. With more time and financial recourses, the study could be repeater in another country and see whether the results are similar and thus the validity of data could be increased. Although there was a good number of responses, when it comes to consumer studies, the response rate is still fairly low in order to be generalised for all consumers.

Considerations concerning the sampling technique

Furthermore, there are some limitations in relation to the sampling technique. Convenience samples often have a problem of self-selected bias because the respondent is interested of the subject. Due to the limited resources, in this case the sample was selected trough researched personal connections and therefore the sample is somewhat bias. Probably due to convenience sample, there was an occurrence of low representation of men respondents as 15 % were men and 85 % women. Therefore, the results are substantial and mainly based on the responses of women. As the results may differ when the representation of genders is more balanced, the research could be repeated with a better sample to see whether it makes a difference to the outcome.

Considerations concerning the analysis technique

The chosen analysis technique could not be used to test all the questions. Therefore, these questions are analysed with more descriptive approach. Furthermore, in ANOVA comparison it is more preferable that the samples are the same size. Although the desired number of respondents

were reached in both groups, they were a bit different in size as 59% of the respondents belong to the category of “younger consumers” and 41 % of “older consumers” and this might affect the comparison.

5.4 Suggestions for further research

Finally, some suggestions for further research are presented. First of all, this study was conducted to research the relationship between the age and consumers’ attitudes towards data privacy with variance analysis. It is suggested further study this relationship with another analysis technique. The same relationship could be tested with correlation calculation where statistical evaluation is made to study the strength of the relationship between age and attitudes towards data privacy. In this case the age cannot be divided into groups, but the variables should be continuous.

Furthermore, this research argues that as the younger have been living in the time of digital revolution their technology adaption is much higher and this has an effect on the attitudes towards data privacy. But could there be some other reasons that explain these differences? Thus, there is a suggestion for a further study that is looking to explain the reasons causing the differences.

Furthermore, this research was conducted in Finland. The same research could also be repeated in another country and see whether the results differ from the results in this study. This could maybe evidence the consumers perceive privacy issues differently in different countries. In Europe, the EU countries share common marketplace and legislation, therefore it would be interesting to investigate if there are any differences in the attitudes towards data privacy between the EU countries.

As concluded in this study, it is expected that the attitudes towards data privacy has a major effect on the customer-centric marketing strategies. Therefore, a qualitative study could be conducted to research the managerial reaction to the results of this study and how they would adapt these implications to their existing marketing strategies.

REFERENCES

Ayyagari, R. 2012. An Exploratory Analysis of Data Breaches From 2005-2011: Trends and Insights. Journal of Information Privacy & Security, 8(2), p. 33-56.

Baker, G (2018). Advertising (A Special Report) --- One Year Later, It's a Different Digital World: Gerard Baker, the Journal's editor at large, introduces our report on an advertising world rocked by questions about data privacy. Wall Street Journal, Eastern edition; New York, N.Y. Jun 19, 2018, p.R.2

Chellappa, R. & Sin, R. Inf Technol Manage (2005) 6: p. 181.

Claveria, K. (2018) Customers don't like how companies collect their data – and that's a problem for brands. Visioncritical [Accessed 6.11.2018] Available: <https://www.visioncritical.com/trade-off-falacy/>

Combemale, C. (2017) Data is the only way marketers can offer customers the relevance they demand. DMA. [online document] [Accessed: 18.8.2018] Available: <https://dma.org.uk/article/data-is-the-only-way-marketers-can-offer-customers-the-relevance-they-demand> [Accessed: 18.8.2018]

Combemale, C. (2018) GDPR and making privacy a brand asset. DMA. [online document] [Accessed 21.8.2018] Available: <https://dma.org.uk/article/gdpr-and-making-privacy-a-brand-asset>

Conroy, P. & Milano, F. & Narula, A. & Singhal, R. (2014) Building consumer trust: protecting personal data in the consumer product industry. Deloitte University Press.

Denham, E. (2018). Information Commissioner's Annual Report and Financial Statements 2017-18. ICO. Information Commissioner Office [online document] [Accessed 21.8.2018] Available: <https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf>

Dickie, N. 2017. Privacy by design prevents data headaches later. Strategic HR Review, 16(2), pp. 100-101.

DMA (2018) What the consumer really thinks. DMA [online document] [Accessed 25.10.2018] Available: https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf

Evans, N. 2017. Data-driven marketing. Utility Week, p. 24.

Federal Trade Commission (2012) How to keep your personal information secure. Consumer information. [online document] [Accessed 14.2.2019] Available: <https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>

Girden, E. R. 1992. ANOVA: Repeated measures. Newbury Park, [Calif.] ; London: Sage.

Hazari, S. & Brown, C. 2013. An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. Journal of Information Privacy and Security, 9(4), pp. 31-51.

Hunton & Williams (2016) The EU General Data Protection Regulation. EU General Data Protection Regulation Guide for In-House Lawyers. Hunton Releases 2016. Business Wire.

Jiang, J. (2018) Millennials stand out for their technology use, but older generations also embrace digital life. Facttank. [online document] [Accessed 17.2.2019] Available at: <http://www.pewresearch.org/fact-tank/2018/05/02/millennials-stand-out-for-their-technology-use-but-older-generations-also-embrace-digital-life/>

Kanji, G. K. 2006. 100 statistical tests. 3rd ed. London: SAGE.

Karjoth, G. & Schunter, M. & Waidner, M. (2003) Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data. International Workshop on Privacy Enhancing Technologies. PET 2002: Privacy Enhancing Technologies pp 69-84

Kaushik, A. (2007) Web analytics. 1 hour per day

King, N. J. 2016. Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data. Computer Law & Security Review: The International Journal of Technology Law and Practice, 32(5), pp. 696-714.

Koops, B. & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. International Review of Law, Computers & Technology, 28(2), pp. 159-171.

Krafft, M. & Ardena, C. & Verhoef, V. (2017). Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions? *Journal of interactive marketing*. volume 39, august 2017, p. 39-54

Krystlik, J. 2017. With GDPR, preparation is everything. *Computer Fraud & Security*, 2017(6), pp. 5-8.

Kshetri, N. 2014. Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), pp. 1134-1145.

Leone, C. (2016) Analytics: the role of data in digital marketing. WSI Agency, USA. [online document] [Accessed 3.10.2018] Available: https://www.poweredbywsi.com/_literature_157978/Chapter_12_-_Analytics

Meinert, M. (2018) GDPR. American Bankers Association. *ABA Banking Journal* May/June 2018, Vol.110 (3), p. 30-33

Muijs, D. 2011. *Doing quantitative research in education with SPSS*. 2nd ed. Los Angeles, [Calif.] ; London: SAGE.

Mullock, J. (2012) EU data privacy laws face big shake up. *Journal of Direct, Data and Digital Marketing Practice* (2012) 13, p. 369 – 371

O'Brien, R. (2016). Privacy and security: The new European data protection regulation and its data breach notification requirements. *Business Information Review*, 33(2), p. 81.

Oldwick (2017). *Best's Briefing Reviews: European Data Regulation*. *Best's Review* 5, p. 88.

O'Neill, E. (2018). Smart data saves lives data collection methods in the field. DMA. [online document] [Accessed 6.8.2018] Available: <https://dma.org.uk/article/smart-data-saves-lives-data-collection-methods-in-the-field>

O'Reilly, L. (2018). Advertising (A Special Report) --- The Future of Digital Marketing in a Data-Privacy World: Tougher regulations and rising distrust have companies scrambling to figure out how to create stronger ties with their customers. *Wall Street Journal*. Eastern edition; New York, N.Y. 19 June 2018

Pearse, J. (2012), The ePrivacy Directive presents an opportunity, not a threat, Centaur Communications Ltd, London.

Petkovic, M & Jonker, W. 2007. Security, Privacy and Trust in Modern Data Management. Springer Berlin Heidelberg New York.

Pingitore, G., Rao, V., Cavallaro, K. Dwivedi, K. (2017) To share or not to share. What consumers really think about sharing their personal information. Deloitte University Press. [inline document] [Accessed 1.12.2018] Available: https://www2.deloitte.com/content/dam/insights/us/articles/4020_To-share-or-not-to-share/DUP_To-share-or-not-to-share.pdf

Pook, C. (2015). Should situational data be the bedrock of your personalisation strategy. Econsultancy. [online document] [Accessed 24.9.2018] Available: <https://econsultancy.com/should-situational-data-be-the-bedrock-of-your-personalisation-strategy>

Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. Business Intelligence. Journal of Direct, Data and Digital Marketing Practice, Vol.17(1), p. 30-35.

Romanosky, S., Hoffman, D. and Acquisti, A., 2014. Empirical analysis of data breach litigation. Journal of Empirical Legal Studies, 11(1), pp.74-104.

Saxby, S. (2008) Published in Computer Law and Security Review: The International Journal of Technology and Practice 2008, Vol.24(5), pp.375-376

Schneck, B (2018) The latest in digital marketing. AgriMarketing. Henderson Communications LLC. St. Louis Vol. 56, Iss. 1, (Jan/Feb 2018): 16, p. 18-19

Schenker, J. 2004. Causal-comparative research designs. Journal of Vocational Rehabilitation, 21(3), p. 117-121.

Steel, E. & Fowler, G., 2010. Facebook in privacy breach. The Wall Street Journal, 18(1).

Tjepkema, L. (2018) What is Data-Driven Marketing. Emarsys. [online document] [Accessed 9.10.2018] Available: <https://www.emarsys.com/en/resources/blog/data-driven-marketing/>

Trick, G. (2018a). EU ePrivacy regulation: everything you need to know about ePR. DMA. [online document] [Accessed 22.8.2018] Available:

<https://dma.org.uk/article/eu-eprivacy-regulation-everything-you-need-to-know-about-epr>

Trick, G. (2018b). EU ePrivacy regulation: everything you need to know about ePR. Consentric. [online document] [Accessed 23.8.2018] Available: <https://consentric.io/eu-eprivacy-regulation-everything-you-need-to-know-about-epr/>

Uzialko, A. & Writer, S. (2018) How businesses are collecting data (and what they're doing with it) [online document] [Accessed 9.11.2018] Available: <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>

Van Eijk, N. 2012. Online tracking: Questioning the power of informed consent. info, 14(5), pp. 57-73.

Wei, L. & Zhu, H. & Cao, Z. & Dong, X., Weiwei, J. & Chen, Y. & Vasilakos, A. 2014. Security and privacy for storage and computation in cloud computing. Information Sciences, 258(C), pp. 371-386.

APPENDICES

APPENDIX 1: WEB-QUESTIONNAIRE

Tutkimuskysely kuluttajien asenteista suhteessa tietosuojaan/
Survey research on consumers' attitudes towards data privacy

1. Vastaajan ikä/Age of respondent

- a. Alle 18/Under 18
- b. 18-24
- c. 25-34
- d. 35-44
- e. 45-54
- f. 55-64
- g. 65 tai yli/65 or over
- h. En halua sanoa/Prefer not to say

2. Vastaajan sukupuoli/Gender of respondent

- a. Nainen/Female
- b. Mies/Male
- c. En halua sanoa/Prefer not to say

3. Vastaajan asuinmaa/Country of residence

- a. Suomi/Finland
- b. Muu, mikä/Other, what
- c. En halua sanoa/Prefer not to say

4. Kuinka tärkeitä seuraavat asiat ovat sinulle/

How important is each of the following for you?

(En ole varma/Not sure, Ei yhtään tärkeää/Not at all important, Ei kovin tärkeää/Not very important, Melko tärkeää/Fairly important, Todella tärkeää/Very important)

- a. Pääsy henkilökohtaisiin tietoihisi (esim. kuvat, kalenteri, yhteystiedot) tietokoneellasi, älypuhelimessasi tai tabletillasi on mahdollista vain sinun luvallasi/
Your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission

b. Sähköpostiesi ja pikaviestiesi yksityisyys on taattu/

The confidentiality of your emails and instant messages is guaranteed

c. Työkaluja, joilla monitoroidaan käyttäytymistäsi verkossa (kuten evästeet), on mahdollista käyttää vain kun olet antanut niihin luvan/

Tools for monitoring your activities online (such as cookies) can only be used with your permission

5. Vastaa asteikolla 1-10, kuinka huolissasi olet tietoturvallisuudesta tänä päivänä. (1 on "en lainkaan huolissani" ja 10 on "todella huolissani")/ On a scale from 1 to 10, how concerned are you about data privacy online these days. 1 is 'not at all concerned' and 10 is 'very concerned')

6. Kuinka samaa tai eri mieltä olet seuraavien väittämien kanssa?/

How much do you agree or disagree with the following statements?

(Täysin eri mieltä/Strongly disagree, Jokseenkin eri mieltä/Somewhat disagree, En samaa enkä eri mieltä/Neither agree nor disagree, Jokseenkin samaa mieltä/Somewhat agree, Täysin samaa mieltä/Strongly agree)

a. Tietojen ja henkilötietojen jakaminen verkossa on osa nykytaloutta./

Sharing data and personal information online is part of the modern economy.

b. Tietojenvaihto on välttämätöntä yhteiskunnan sujuvalle toiminnalle./

The exchange of personal information is essential for the smooth running of modern society.

c. Yleisesti ottaen olen tyytyväinen siihen kuinka paljon henkilötietojani jaan yrityksille./

On the whole I am happy with the amount of personal information I give to companies.

d. Tiedostan nykyään paremmin, mitä tietoja minusta kerätään ja mihin niitä käytetään./

Today, I feel more aware of how my data is used and collected than in the past.

e. Suhtaudun nykyään myönteisemmin tietojenvaihtoon yritysten kanssa kuin aikaisemmin./

Today, I feel more comfortable with the idea of exchanging some personal data with companies than I did previously.

f. Viimeaikojen uutisotsikot tietoturvallisuuden rikkomuksista ovat lisänneet tietoisuuttani omasta tietoturvastani./

Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy.

7. Vastaa asteikolla 1-10, kuinka suureksi koet vaikutusmahdollisuutesi seuraavissa asioissa.
(1 on "minulla ei ole lainkaan mahdollisuutta" ja 10 on "minulla on täysi mahdollisuus".)

On a scale from 1 to 10, how much control do you think you have over the following. (1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control'.)

- a. Estää yritystä keräämästä tietoja minusta/
Preventing companies from collecting information about me
- b. Estää yritystä jakamasta tietojani kolmansille osapuolille/
Preventing companies from sharing my information with 3rd parties
- c. Käskeä yritystä poistamaan minun tietoni/
Being able to compel a company to delete any information they have about me
- d. Varmistaa, että tietojani käytetään vain siihen tarkoitukseen mihin olen antanut luvan/
Ensuring brands use my data for the purpose I initially agreed to
- e. Päättää eduista ja palkinnoista, joita saan vastikkeeksi tietojeni jakamisesta/
Choosing the benefits or rewards I receive in return for sharing my data with companies
- f. Hallinnoida tietosuoja-asetuksiani, jotka määrittävät mitä tietoja itsestäni jaan/
Managing the privacy settings that allow me to choose how much data I choose to share

8. Oletko kuluneen vuoden aikana tehnyt jotain seuraavista suojellaksesi henkilötietojasi?
Valitse kaikki, jotka sopivat./

Within the past year, have you taken any of the following actions to protect your data?

Select all that apply.

- a. Muokannut oman puhelimeni tietosuoja-asetuksia
Adjusted privacy settings on my phone
- b. Muokannut sosiaalisen median palveluiden tietosuoja-asetuksia/
Adjusted privacy settings on social media
- c. Antanut valheellisia tietoja itsestäni yrityksille/
Provided fake information to companies
- d. Poistanut evästeet käytöstä/
Disabled cookies
- e. Kiinnittänyt erityistä huomiota yritysten sopimuksiin henkilötietojen käsittelyssä ja yksityisyyden suojasta/
Paid close attention to privacy agreements

- f. Poistanut tai jättänyt lataamatta tiettyjä sovelluksia/
Deleted or did not download specific apps
- g. Jättänyt vierailematta tai sulkenut tietyn sivuston/
Not visited or closed a specific website
- h. Jättänyt ostamatta tietyn tuotteen tai ostanut saman tuotteen toiselta tuotemerkiltä/
Did not buy a certain product, or purchased the same product from a different brand
- i. Hankkinut mainostenesto-ohjelman, joka estää näkemästä mainoksia verkossa/
Obtained ad-blocking software that prevents from seeing the online adverts
- j. Hankkinut ohjelman joka estää verkkokäyttäytymiseni seuraamisen/
Obtained software that prevents my online activities from being tracked
- k. En ole tehnyt mitään yllä mainituista/
I have not done any of the above

9. Mitä seuraavista asioista sallisit, yritysten analysoivan tietojärjestelmissään, jotta he voisivat lähettää sinulle kohdistettuja mainoksia tai tarjouksia?/

Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.

- a. Ostohistoriasi/
Your purchase history
- b. Demografiset tietosi (esim. Ikä, sijainti, sukupuoli)/
Your demographic information (e.g. age, location, gender)
- c. Selainhistoriasi/
Your online search history
- d. Sosiaalisen median julkaisusi/
Your social media postings
- e. Sähköpostiviestiesi sisältö/
The content of your emails
- f. Ei mitään yllä mainituista/
None of the above

10. Mitkä seuraavista lisäävät luottamustasi yrityksen tietoturvallisuuteen henkilötietojesi käsittelyssä asioidessasi verkossa? Valitse kaikki ne, jotka sopivat./

Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.

- a. Sinulla on valta päättää siitä, mitä tietoja sinusta saa tai ei saa kerätä, käyttää tai jakaa./
Control over what information can and cannot be accessed or shared
- b. Erillinen suostumus ja ilmoitus käyttötarkoituksesta aina, jos joudut luovuttamaan henkilötietojasi./
Clearly stating how consumer data will be used each time data is collected and asking for consent
- c. Pystyt helposti muuttamaan tietosuoja-asetuksiasi./
You can easily change your privacy settings
- d. Läpinäkyvät tietoturvatimet (esim. mitä ennaltaehkäiseviä toimia tehdään henkilötietojen suojelemiseksi)./
More transparent data security policies (e.g., the precautions taken to prevent someone from stealing personal information)
- e. Selkokieliset tietosuojakäytännöt (esim. Miten yritys käyttää ja jakaa henkilötietoja)./
More easily understandable privacy policies (e.g. the ways company uses and share personal information)
- f. Mikään yllä mainituista ei lisää luottamustani./
None of the above increases my trust.

11. Kuinka samaa tai eri mieltä olet seuraavien väittämien kanssa?/

How much do you agree or disagree with the following statements?

(Täysin eri mieltä/Strongly disagree, Jokseenkin eri mieltä/Somewhat disagree, En samaa enkä eri mieltä/Neither agree nor disagree, Jokseenkin samaa mieltä/Somewhat agree, Täysin samaa mieltä/Strongly agree)

- a. Ostan todennäköisemmin yrityksiltä, joiden uskon suojelevan henkilötietojani./
I am more likely to purchase from companies that I believe protect my personal information.
- b. Vältän ostamista yrityksiltä, joiden en usko suojelevan henkilötietojani./
I avoid purchasing from companies that I do not believe protect my personal information.
- c. Yrityksen yksittäinenkin tietosuojarikkomus vaikuttaisi kielteisesti siihen, kuinka todennäköisesti heiltä ostaisin jatkossa./
Even a single data breach would negatively impact my likelihood to buy from a company in the future.
- d. Olisin valmis antamaan anteeksi yritykselle, joka rikkoisi tietosuojavelvoitteita, mutta korjaisi asian välittömästi./

I would be forgiving of a company that had one single data breach of my personal data as long as they quickly addressed the issue.

e. Uskon, että useimmat yritykset suojelevat henkilötietojani riittävän hyvin./

I believe most companies are adequately protecting my personal information.

f. Tiedän, mitkä yritykset suojaavat parhaiten henkilötietoja./

I know which companies best protect my personal information.

12. Oletko tietoinen EU:n yleisestä tietosuoja-asetuksesta (GDPR), joka astui voimaan toukokuussa 2018?/Are you aware of the General Data Protection Regulation (GDPR) that entered into force in May 2018? *

a. Kyllä/Yes

b. En/No

c. En ole varma/Not sure

13. Oletko tietoinen EU:n ePrivacy-asetuksesta, joka todennäköisesti tulee voimaan vuonna 2019?/ Are you aware of the EU ePrivacy regulation that is likely to enter into force in 2019?

a. Kyllä/Yes

b. En/No

c. En ole varma/Not sure

APPENDIX 2: SURVEY RESULTS

Kyselyn nimi: Kuluttajien asenteet ja käyttäytyminen suhteessa tietosuojaan

Raportin otsikko: Tutkimuskysely kuluttajien asenteista suhteessa tietosuojaan/
Survey research on consumers' attitudes towards data privacy

Näytetään 116 vastaajaa kyselyn vastaajien kokonaismäärästä 120

1. Vastaajan ikä/ Age of respondent

| | Younger consumers | | Older consumers | | Yhteensä |
|----------------------------------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| Alle 18/Under 18 | 6 | 8,7% | 0 | 0% | 6 |
| 18-24 | 11 | 15,94% | 0 | 0% | 11 |
| 25-34 | 52 | 75,36% | 0 | 0% | 52 |
| 35-44 | 0 | 0% | 17 | 36,17% | 17 |
| 45-54 | 0 | 0% | 18 | 38,3% | 18 |
| 55-64 | 0 | 0% | 8 | 17,02% | 8 |
| 65 tai yli/65 or over | 0 | 0% | 4 | 8,51% | 4 |
| En halua sanoa/Prefer not to say | 0 | 0% | 0 | 0% | 0 |
| Yhteensä | 69 | | 47 | | 116 |

2. Vastaajan sukupuoli/ Gender of respondent

| | Younger consumers | | Older consumers | | Yhteensä |
|----------------------------------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| Nainen/Female | 55 | 79,71% | 43 | 91,49% | 98 |
| Mies/Male | 13 | 18,84% | 4 | 8,51% | 17 |
| En halua sanoa/Prefer not to say | 1 | 1,45% | 0 | 0% | 1 |
| Yhteensä | 69 | | 47 | | 116 |

3. Vastaajan asuinmaa/ Country of residence

| | Younger consumers | | Older consumers | | Yhteensä |
|---------------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| Suomi/Finland | 69 | 100% | 47 | 100% | 116 |

| | | | | | |
|----------------------------------|-----------|----|-----------|----|------------|
| Muu, mikä/Other, what | 0 | 0% | 0 | 0% | 0 |
| En halua sanoa/Prefer not to say | 0 | 0% | 0 | 0% | 0 |
| Yhteensä | 69 | | 47 | | 116 |

4. Kuinka tärkeitä seuraavat asiat ovat sinulle?/
How important is each of the following for you?

| Pääsy henkilökohtaisiin tietoihisi (esim. kuvat, kalenteri, yhteystiedot) tietokoneellasi, älypuhelimessasi tai tabletillasi on mahdollista vain sinun luvallasi/Your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission | En ole varma/Not sure | Ei yhtään tärkeää/Not at all important | Ei kovin tärkeää/Not very important | Melko tärkeää/Fairly important | Todella tärkeää/Very important | Yhteensä |
|---|-----------------------|--|-------------------------------------|--------------------------------|--------------------------------|------------|
| Younger consumers | 0 0 % | 0 0 % | 0 18,84% | 13 81,16% | 56 0 | 69 |
| Older consumers | 0 0 % | 0 0 % | 0 8,51% | 4 91,49% | 43 0 | 47 |
| Yhteensä | 0 | 0 | 0 | 17 | 99 | 116 |

| Sähköpostiesi ja pikaviestiesi yksityisyys on taattu/The confidentiality of your emails and instant messages is guaranteed | En ole varma/Not sure | Ei yhtään tärkeää/Not at all important | Ei kovin tärkeää/Not very important | Melko tärkeää/Fairly important | Todella tärkeää/Very important | Yhteensä |
|--|-----------------------|--|-------------------------------------|--------------------------------|--------------------------------|------------|
| Younger consumers | 0 0 % | 0 0 % | 0 4,35% | 3 95,65% | 66 0 | 69 |
| Older consumers | 0 0 % | 0 0 % | 0 6,38% | 3 93,62% | 44 0 | 47 |
| Yhteensä | 0 | 0 | 0 | 6 | 110 | 116 |

| Työkaluja, joilla monitoroidaan käyttäytymistäsi verkossa (kuten evästeet), on mahdollista käyttää vain kun olet antanut niihin luvan/Tools for monitoring your activities online (such as cookies) can only be used with your permission | En ole varma/Not sure | Ei yhtään tärkeää/Not at all important | Ei kovin tärkeää/Not very important | Melko tärkeää/Fairly important | Todella tärkeää/Very important | Yhteensä |
|---|-----------------------|--|-------------------------------------|--------------------------------|--------------------------------|----------|
| Younger consumers | 1 0 % | 0 10,15% | 7 37,68% | 26 50,72% | 35 0 | 69 |
| Older consumers | 0 0 % | 0 4,26% | 2 25,53% | 12 70,21% | 33 0 | 47 |
| Yhteensä | 1 | 0 | 9 | 38 | 68 | 116 |

5. Vastaa asteikolla 1-10, kuinka huolissasi olet tietoturvasuudesta tänä päivänä. 1 on "en lainkaan huolissani" ja 10 on "todella huolissani"./ On a scale from 1 to 10, how concerned are you about data privacy online these days. 1 is 'not at all concerned' and 10 is 'very concerned'.

| | Younger consumers | | Older consumers | | Yhteensä |
|----------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| 1 | 0 | 0% | 0 | 0% | 0 |
| 2 | 0 | 0% | 0 | 0% | 0 |
| 3 | 2 | 2,9% | 1 | 2,13% | 3 |
| 4 | 4 | 5,8% | 1 | 2,13% | 5 |
| 5 | 5 | 7,25% | 2 | 4,25% | 7 |
| 6 | 5 | 7,25% | 3 | 6,38% | 8 |
| 7 | 10 | 14,49% | 6 | 12,77% | 16 |
| 8 | 21 | 30,43% | 11 | 23,4% | 32 |
| 9 | 16 | 23,19% | 17 | 36,17% | 33 |
| 10 | 6 | 8,69% | 6 | 12,77% | 12 |
| Yhteensä | 69 | | 47 | | 116 |

6. Kuinka samaa tai eri mieltä olet seuraavien väittämien kanssa?/
How much do you agree or disagree with the following statements?

| | | | | | | |
|-------------------|--------|--------|--------|-------|---|-----|
| Younger consumers | 6 | 21 | 14 | 24 | 4 | 69 |
| | 30,43% | 20,29% | 34,78% | 5,8% | 0 | |
| Older consumers | 2 | 13 | 10 | 20 | 2 | 47 |
| | 27,66% | 21,28% | 42,55% | 4,26% | 0 | |
| Yhteensä | 8 | 34 | 24 | 44 | 6 | 116 |

| | | | | | | |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Tiedostan nykyään paremmin, mitä tietoja minusta kerätään ja mihin niitä käytetään./Today, I feel more aware of how my data is used and collected than in the past. | | | | | | |
| | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
| Younger consumers | 1 | 14 | 5 | 31 | 18 | 69 |
| | 20,29% | 7,24% | 44,93% | 26,09% | 0 | |
| Older consumers | 0 | 6 | 7 | 28 | 6 | 47 |
| | 12,77% | 14,89% | 59,57% | 12,77% | 0 | |
| Yhteensä | 1 | 20 | 12 | 59 | 24 | 116 |

| | | | | | | |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Suhtaudun nykyään myönteisemmin tietojenvaihtoon yritysten kanssa kuin aikaisemmin./Today, I feel more comfortable with the idea of exchanging some personal data with companies than I did previously. | | | | | | |
| | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
| Younger consumers | 5 | 22 | 18 | 19 | 5 | 69 |
| | 31,88% | 26,09% | 27,53% | 7,25% | 0 | |
| Older consumers | 1 | 18 | 18 | 8 | 2 | 47 |
| | 38,3% | 38,3% | 17,02% | 4,25% | 0 | |
| Yhteensä | 6 | 40 | 36 | 27 | 7 | 116 |

| Viimeaikojen uutisotsikot tietoturvallisuuden rikkomuksista ovat lisänneet tietoisuuttani omasta tietoturvastani./Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 1 13,04% | 9 15,94% | 11 44,93% | 31 24,64% | 17 0 | 69 |
| Older consumers | 0 6,38% | 3 8,51% | 4 59,58% | 28 25,53% | 12 0 | 47 |
| Yhteensä | 1 | 12 | 15 | 59 | 29 | 116 |

7. Vastaa asteikolla 1-10, kuinka suureksi koet vaikutusmahdollisuutesi seuraavissa asioissa. 1 on "minulla ei ole lainkaan mahdollisuutta" ja 10 on "minulla on täysi mahdollisuus"./
On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control'.

| Estää yritystä keräämästä tietoja minusta/Preventing companies from collecting information about me | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Yhteensä |
|---|-------------|-------------|--------------|-------------|-------------|------------|-------------|-------------|------------|--------|----------|
| Younger consumers | 5 11,59% | 8 17,39% | 12 15,94% | 11 5,8% | 4 13,04% | 9 7,25% | 5 14,49% | 10 4,35% | 3 2,9% | 2 0 | 69 |
| Older consumers | 5 14,89% | 7 12,77% | 6 12,77% | 6 14,89% | 7 8,51% | 4 4,25% | 2 12,77% | 6 2,13% | 1 6,38% | 3 0 | 47 |
| Yhteensä | 10 | 15 | 18 | 17 | 11 | 13 | 7 | 16 | 4 | 5 | 116 |

| | | | | | | | | | | | |
|-------------------|---------|---------|---------|---------|--------|---------|--------|--------|--------|---|-----|
| | 7 | 13 | 16 | 10 | 8 | 3 | 6 | 2 | 1 | 3 | 69 |
| Younger consumers | 18,84 % | 23,19 % | 14,49 % | 11,59 % | 4,35 % | 8,7% | 2,9% | 1,45 % | 4,35 % | 0 | |
| | 9 | 7 | 7 | 4 | 7 | 2 | 7 | 2 | 2 | 0 | 47 |
| Older consumers | 14,89 % | 14,89 % | 8,51% | 14,89 % | 4,26 % | 14,89 % | 4,26 % | 4,26 % | 0 % | 0 | |
| | | | | | | | | | | | |
| Yhteensä | 16 | 20 | 23 | 14 | 15 | 5 | 13 | 4 | 3 | 3 | 116 |

| | | | | | | | | | | | | |
|---|---------|---------|---------|---------|--------|--------|--------|--------|-----|---|---|----------|
| Päätää eduista ja palkinnoista, joita saan vastikkeeksi tietojeni jakamisesta/Choosing the benefits or rewards I receive in return for sharing my data with companies | | | | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 0 | Yhteensä |
| | 18 | 10 | 14 | 7 | 8 | 4 | 4 | 1 | 3 | 0 | 0 | 69 |
| Younger consumers | 14,49 % | 20,29 % | 10,14 % | 11,59 % | 5,8% | 5,8% | 1,45 % | 4,35 % | 0 % | 0 | 0 | |
| | 11 | 12 | 7 | 4 | 5 | 2 | 2 | 2 | 2 | 0 | 0 | 47 |
| Older consumers | 25,53 % | 14,89 % | 8,51% | 10,64 % | 4,25 % | 4,26 % | 4,26 % | 4,26 % | 0 % | 0 | 0 | |
| | | | | | | | | | | | | |
| Yhteensä | 29 | 22 | 21 | 11 | 13 | 6 | 6 | 3 | 5 | 0 | 0 | 116 |

| | | | | | | | | | | | | |
|---|--------|---------|---------|---------|---------|---------|---------|--------|--------|---|---|----------|
| Hallinnoida tietosuojasetuksiani, jotka määrittävät mitä tietoja itsestäni jaan/Managing the privacy settings that allow me to choose how much data I choose to share | | | | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 0 | Yhteensä |
| | 2 | 4 | 7 | 7 | 10 | 12 | 12 | 11 | 4 | 0 | 0 | 69 |
| Younger consumers | 5,8% | 10,15 % | 10,14 % | 14,49 % | 17,39 % | 17,39 % | 15,94 % | 5,8% | 0 % | 0 | 0 | |
| | 4 | 2 | 11 | 3 | 6 | 6 | 6 | 5 | 3 | 1 | 0 | 47 |
| Older consumers | 4,25 % | 23,4% | 6,38% | 12,77 % | 12,77 % | 12,77 % | 10,64 % | 6,38 % | 2,13 % | 0 | 0 | |
| | | | | | | | | | | | | |
| Yhteensä | 6 | 6 | 18 | 10 | 16 | 18 | 18 | 16 | 7 | 1 | 0 | 116 |

8. Oletko kuluneen vuoden aikana tehnyt jotain seuraavista suojellaksesi henkilötietojasi? Valitse kaikki, jotka sopivat./

Within the past year, have you taken any of the following actions to protect your data? Select all that apply.

| | Younger consumers | Older consumers | Yhteensä |
|--|-------------------|-----------------|----------|
| Muokannut oman puhelimeni tietosuojasetuksia/Adjusted privacy settings on my phone | 41 | 31 | 72 |
| Muokannut sosiaalisen median palveluiden tietosuojasetuksia/Adjusted privacy settings on social media | 59 | 36 | 95 |
| Antanut valheellisia tietoja itsestäni yrityksille/Provided fake information to companies | 24 | 11 | 35 |
| Poistanut evästeet käytöstä/Disabled cookies | 26 | 20 | 46 |
| Kiinnittänyt erityistä huomiota yritysten sopimuksiin henkilötietojen käsittelyssä ja yksityisyyden suojasta/Paid close attention to privacy agreements | 27 | 22 | 49 |
| Poistanut tai jättänyt lataamatta tiettyjä sovelluksia/Deleted or did not download specific apps | 41 | 40 | 81 |
| Jättänyt vierailematta tai sulkenut tietyn sivuston/Not visited or closed a specific website | 45 | 36 | 81 |
| Jättänyt ostamatta tietyn tuotteen tai ostanut saman tuotteen toiselta tuotemerkiltä/Did not buy a certain product, or purchased the same product from a different brand | 21 | 14 | 35 |
| Hankkinut mainostenesto-ohjelman, joka estää näkemästä mainoksia verkossa/Obtained ad-blocking software that prevents from seeing the online adverts | 12 | 0 | 12 |
| Hankkinut ohjelman joka estää verkkokäyttämiseni seuraamisen/Obtained software that prevents my online activities from being tracked | 15 | 2 | 17 |
| En ole tehnyt mitään yllä mainituista/I have not done any of the above | 2 | 0 | 2 |
| Yhteensä | 313 | 212 | 525 |

9. Mitä seuraavista asioista sallisit, yritysten analysoivan tietojärjestelmissään, jotta he voisivat lähettää sinulle kohdistettuja mainoksia tai tarjouksia?/

Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.

| | Younger consumers | Older consumers | Yhteensä |
|---|-------------------|-----------------|----------|
| Ostohistoriasi/Your purchase history | 30 | 27 | 57 |
| Demografiset tietosi (esim. ikä, sijainti, sukupuoli)/Your demographic information (e.g. age, location, gender) | 30 | 16 | 46 |
| Selainhistoriasi/Your online search history | 6 | 3 | 9 |
| Sosiaalisen median julkaisusi/Your social media postings | 8 | 2 | 10 |
| Sähköpostiviestiesi sisältö/The content of your emails | 0 | 0 | 0 |
| Ei mitään yllä mainituista/None of the above | 24 | 16 | 40 |
| Yhteensä | 98 | 64 | 162 |

10. Mitkä seuraavista lisäävät luottamustasi yrityksen tietoturvasuuteen henkilötietojesi käsittelyssä asioidessasi verkossa? Valitse kaikki ne, jotka sopivat./

Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.

| | Younger consumers | Older consumers | Yhteensä |
|---|-------------------|-----------------|------------|
| Sinulla on valta päättää siitä, mitä tietoja sinusta saa tai ei saa kerätä, käyttää tai jakaa./Control over what information can and cannot be accessed or shared | 58 | 45 | 103 |
| Erillinen suostumus ja ilmoitus käyttötarkoituksesta aina, jos joudut luovuttamaan henkilötietojasi./Clearly stating how consumer data will be used each time data is collected and asking for consent | 55 | 41 | 96 |
| Pystyt helposti muuttamaan tietosuojasetuksiasi./You can easily change your privacy settings | 61 | 36 | 97 |
| Läpinäkyvät tietoturvatimet (esim. mitä ennaltaehkäiseviä toimia tehdään henkilötietojen suojelemiseksi)./More transparent data security policies (e.g., the precautions taken to prevent someone from stealing personal information) | 40 | 25 | 65 |
| Selkokieliset tietosuojakäytännöt (esim. miten yritys käyttää ja jakaa henkilötietoja)./More easily understandable privacy policies (e.g., the ways companies use and share personal information). | 59 | 38 | 97 |
| Mikään yllä mainituista ei lisää luottamustani./None of the above increases my trust. | 2 | 0 | 2 |
| Yhteensä | 275 | 185 | 460 |

11. Kuinka samaa tai eri mieltä olet seuraavien väittämien kanssa?/
How much do you agree or disagree with the following statements?

| Ostan todennäköisemmin yrityksiltä, joiden uskon suojelevan henkilötietojani./ I am more likely to purchase from companies that I believe protect my personal information. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa eikä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|--|-------------------------------------|---|---|--|------------------------------------|------------|
| Younger consumers | 0 5,8% | 4 14,49% | 10 46,38% | 32 33,33% | 23 0 | 69 |
| Older consumers | 0 0 % | 0 14,9% | 7 42,55% | 20 42,55% | 20 0 | 47 |
| Yhteensä | 0 | 4 | 17 | 52 | 43 | 116 |

| Vältän ostamista yrityksiltä, joiden en usko suojelevan henkilötietojani./I avoid purchasing from companies that I do not believe protect my personal information. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|--|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 1 11,59% | 8 10,15% | 7 40,58% | 28 36,23% | 25 0 | 69 |
| Older consumers | 1 2,13% | 1 12,76% | 6 36,17% | 17 46,81% | 22 0 | 47 |
| Yhteensä | 2 | 9 | 13 | 45 | 47 | 116 |

| Yrityksen yksittäinenkin tietosuojarikko mus vaikuttaisi kielteisesti siihen, kuinka todennäköisesti heiltä ostaisin jatkossa./Even a single data breach would negatively impact my likelihood to buy from a company in the future. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 0 11,6% | 8 11,59% | 8 44,93% | 31 31,88% | 22 0 | 69 |
| Older consumers | 0 2,13% | 1 6,38% | 3 44,68% | 21 46,81% | 22 0 | 47 |
| Yhteensä | 0 | 9 | 11 | 52 | 44 | 116 |

| Olisin valmis antamaan anteeksi yritykselle, joka rikkoisi tietosuojavelvotteita, mutta korjaisi asian välittömästi./I would be forgiving of a company that had one single data breach of my personal data as long as they quickly addressed the issue. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 8 20,29% | 14 23,19% | 16 39,13% | 27 5,8% | 4 0 | 69 |
| Older consumers | 2 21,28% | 10 25,53% | 12 48,94% | 23 0 % | 0 0 | 47 |
| Yhteensä | 10 | 24 | 28 | 50 | 4 | 116 |

| Uskon, että useimmat yritykset suojelevat henkilötietojani riittävästi hyvin./I believe most companies are adequately protecting my personal information. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 8 30,44% | 21 17,39% | 12 36,23% | 25 4,35% | 3 0 | 69 |
| Older consumers | 4 27,66% | 13 34,04% | 16 27,66% | 13 2,13% | 1 0 | 47 |
| Yhteensä | 12 | 34 | 28 | 38 | 4 | 116 |

| Tiedän, mitkä yritykset suojaavat parhaiten henkilötietoja./ I know which companies best protect my personal information. | Täysin eri mieltä/Strongly disagree | Jokseenkin eri mieltä/Somewhat disagree | En samaa enkä eri mieltä/Neither agree nor disagree | Jokseenkin samaa mieltä/Somewhat agree | Täysin samaa mieltä/Strongly agree | Yhteensä |
|---|-------------------------------------|---|---|--|------------------------------------|----------|
| Younger consumers | 19 33,33% | 23 28,99% | 20 10,14% | 7 0 % | 0 0 | 69 |
| Older consumers | 13 23,4% | 11 31,92% | 15 17,02% | 8 0 % | 0 0 | 47 |
| Yhteensä | 32 | 34 | 35 | 15 | 0 | 116 |

12. Oletko tietoinen EU:n yleisestä tietosuojasetuksesta (GDPR), joka astui voimaan toukokuussa 2018?/
Are you aware of the General Data Protection Regulation (GDPR) that entered into force in May 2018?

| | Younger consumers | | Older consumers | | Yhteensä |
|-----------------------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| Kyllä/Yes | 56 | 81,16% | 41 | 87,24% | 97 |
| En/No | 6 | 8,7% | 3 | 6,38% | 9 |
| En ole varma/Not sure | 7 | 10,14% | 3 | 6,38% | 10 |
| Yhteensä | 69 | | 47 | | 116 |

13. Oletko tietoinen EU:n ePrivacy-asetuksesta, joka todennäköisesti tulee voimaan vuonna 2019?/
Are you aware of the EU ePrivacy regulation that is likely to enter into force in 2019?

| | Younger consumers | | Older consumers | | Yhteensä |
|-----------------------|-------------------|-----------|-----------------|-----------|----------|
| | n | Prosentti | n | Prosentti | |
| Kyllä/Yes | 15 | 21,74% | 7 | 14,89% | 22 |
| En/No | 43 | 62,32% | 26 | 55,32% | 69 |
| En ole varma/Not sure | 11 | 15,94% | 14 | 29,79% | 25 |
| Yhteensä | 69 | | 47 | | 116 |

APPENDIX 3: ANOVA ANALYSIS RESULTS

| Variables | F + P-value | Result |
|---|-------------------|--------|
| How important is each of the following for you?:Your personal information (e.g. photos, calendar, contacts) on your computer, smartphone or tablet can only be accessed with your permission | 2.39 (p=0.125) | > 0.05 |
| How important is each of the following for you?:The confidentiality of your emails and instant messages is guaranteed | 0.23 (p=0.631) | > 0.05 |
| How important is each of the following for you?:Tools for monitoring your activities online (such as cookies) can only used with your permission | 4.98 (p=0.028) | < 0.05 |
| On a scale from 1 to 10, how concerned are you about data privacy online these days. 1 is 'not at all concerned' and 10 is 'very concerned'. | 2.61 (p=0.109) | > 0.05 |
| How much do you agree or disagree with the following statements?:Sharing data and personal information online is part of the modern economy. | 4.84 (p=0.030) | < 0.05 |
| How much do you agree or disagree with the following statements?:The exchange of personal information is essential for the smooth running of modern society. | 1.31 (p=0.255) | > 0.05 |
| How much do you agree or disagree with the following statements?:On the whole I am happy with the amount of personal information I give to companies. | 0.64 (p=0.425) | > 0.05 |
| How much do you agree or disagree with the following statements?:Today, I feel more aware of how my data is used and collected than in the past. | 0.01 (p=0.935) | > 0.05 |
| How much do you agree or disagree with the following statements?:Today, I feel more comfortable with the idea of exchanging some personal data with companies than I did previously. | 0.44 (p=0.511) | > 0.05 |
| How much do you agree or disagree with the following statements?:Recent news headlines about data security breaches have heightened my awareness about my own personal data privacy. | 2.21 (p=0.140) | > 0.05 |
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control':Preventing companies from collecting information about me | 0.14 (p=0.709) | > 0.05 |
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control':Preventing companies from sharing my information with 3rd parties | 0 (p=0.999) | > 0.05 |
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control':Being able to compel a company to delete any information they have about me | 0.23 (p=0.636) | > 0.05 |
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control':Ensuring brands use my data for the purpose I initially agreed to | 0.01 (p=0.925) | > 0.05 |
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control':Choosing the benefits or rewards I receive in return for sharing my data with companies | 0.02 (p=0.879) | > 0.05 |

| | | |
|--|-------------------|--------|
| On a scale from 1 to 10, how much control do you think you have over the following. 1 is 'I don't feel I have any control at all' and 10 is 'I feel that I have complete control'.:Managing the privacy settings that allow me to choose how much data I choose to share | 1.83 (p=0.179) | > 0.05 |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Adjusted privacy settings on my phone | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Adjusted privacy settings on social media | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Provided fake information to companies | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Disabled cookies | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Paid close attention to privacy agreements | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Deleted or did not download specific apps | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Not visited or closed a specific website | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Did not buy a certain product, or purchased the same product from a different brand | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Obtained ad-blocking software that prevents from seeing the online adverts | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:Obtained software that prevents my online activities from being tracked | N/A | N/A |
| Within the past year, have you taken any of the following actions to protect your data? Select all that apply.:I have not done any of the above | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:Your purchase history | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:Your demographic information (e.g. age, location, gender) | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:Your online search history | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:Your social media postings | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:The content of your emails | N/A | N/A |
| Which of the following should companies be allowed to analyse using software programs in order to send targeted advertisements or coupons? Select all that apply.:None of the above | N/A | N/A |

| | | |
|---|-------------------|--------|
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:Control over what information can and cannot be accessed or shared | N/A | N/A |
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:Clearly stating how consumer data will be used each time data is collected and asking for consent | N/A | N/A |
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:You can easily change your privacy settings | N/A | N/A |
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:More transparent data security policies (e.g., the precautions taken to prevent someone from stealing personal information) | N/A | N/A |
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:More easily understandable privacy policies (e.g., the ways companies use and share personal information). | N/A | N/A |
| Which of the following increase your trust in companies in protecting your personal information when online? Select all that apply.:None of the above increases my trust. | N/A | N/A |
| How much do you agree or disagree with the following statements?:I am more likely to purchase from companies that I believe protect my personal information. | 1.84 (p=0.177) | > 0.05 |
| How much do you agree or disagree with the following statements?:I avoid purchasing from companies that I do not believe protect my personal information. | 1.77 (p=0.186) | > 0.05 |
| How much do you agree or disagree with the following statements?:Even a single data breach would negatively impact my likelihood to buy from a company in the future. | 5.74 (p=0.018) | < 0.05 |
| How much do you agree or disagree with the following statements?:I would be forgiving of a company that had one single data breach of my personal data as long as they quickly addressed the issue. | 0.35 (p=0.554) | > 0.05 |
| How much do you agree or disagree with the following statements?:I believe most companies are adequately protecting my personal information. | 0.04 (p=0.843) | > 0.05 |
| How much do you agree or disagree with the following statements?:I know which companies best protect my personal information. | 0.75 (p=0.389) | > 0.05 |
| Are you aware of the General Data Protection Regulation (GDPR) that entered into force in May 2018? | 0.74 (p=0.390) | > 0.05 |
| Are you aware of the EU ePrivacy regulation that is likely to enter into force in 2019? | 2.98 (p=0.087) | > 0.05 |