UNIVERSITY OF TWENTE.

Dutch Consumers' Perspective on Information Privacy in the Post-GDPR Era: An Exploratory Study

By

Shanna Hendrikx

A thesis submitted in partial fulfillment of the requirements for the degrees of:

Master of Science in Communication Science

Master of Science in Business Administration

July 2022

Supervised by:

Dr. Shenja van der Graaf

Drs. Mark Tempelman

Abstract

Objective – As of now it is still unclear whether consumers find that the GDPR has achieved its goal of improving information privacy. This study aims to explore consumers' online experiences with and perceptions of information transparency, information control, and information security in the post-GDPR era, thereby providing an initial understanding of consumers' view on the matter.

Method – A quantitative online survey research method was adopted. A survey was developed and distributed to a sample of 300 respondents via an online recruitment platform. Descriptive analyses and univariate analyses of variance were performed to examine the data.

Results – The results suggest that, generally, respondents perceive information transparency, control, and security to be low. They also show that individual characteristics (such as gender, age, educational level, privacy concern, internet skills, and internet self-efficacy) affect information privacy perceptions. Privacy concern and internet skills in particular were found to have significant effects. Specifically, as respondents' level of privacy concern increases, their perceptions of information transparency, control, and security decrease. The opposite pattern was found for internet skills.

Practical implications – Fostering positive privacy perceptions is key for anyone in business. As information privacy perceptions appear to vary depending on the type of person (e.g., male or female), companies will need to carefully consider who they are targeting and adjust their privacy communication strategies accordingly. Also, reducing privacy concerns should be a priority for all those involved with the GDPR and its execution and enforcement, including, for example, legislators, governmental authorities and organizations, and businesses.

Conclusion – Consumers' perceptions of the level of information transparency, control, and security provided by websites remain rather low. Some individual characteristics appear to affect consumers' information privacy perceptions, albeit to varying extents. This study's findings suggest that the GDPR's goals have not (yet) been achieved, at least not in the eyes of consumers.

Keywords Privacy law, General Data Protection Regulation (GDPR), Information privacy, Information transparency, Information control, Information security, Consumer perspective

Table of contents

1. INTRODUCTION

One of the most essential components, or drivers of the digital economy is data. The amount of available (consumer) data has increased tremendously and serious advances have been made in analytical methods over the past few decades (Wedel & Kannan, 2016). Innovations in technology (e.g., mobile applications, smart devices, internet of things) have provided companies with a wealth of information about consumers and customers. New ways of collecting, analyzing, and using personal data have helped companies gain a deeper and better understanding of consumers (Ackermann et al., 2021). This has been particularly valuable for marketers, who can now use advanced forms of (marketing) analytics to help inform their marketing decisions. By leveraging data, companies can provide their customers with more value and better experiences, increasing satisfaction and loyalty. Also, through data-driven decision-making, companies are said to achieve competitive advantages and extract more (financial) value (Wedel & Kannan, 2016).

However, with these data-driven practices an ever-growing increase in nontransparency can be detected, which, arguably, is of more concern. It has become more difficult for consumers to fully understand and be cognizant of how much of their data is collected and how it is used and combined to produce more information about them (Ackermann et al., 2021). As a result, consumers have become more concerned about when and in what way their data is being collected, stored and used (Ackermann et al., 2021). This has implications for consumers' privacy which consumers feel they are increasingly deprived of (Fernandes & Pereira, 2021). Recent years have shown a predominant regulatory approach to address the growing issues (Cumbley & Church, 2013; Fernandes & Pereira, 2021). Most notably, to tackle these and other issues, in 2018, the European Union (EU) implemented the General Data Protection Regulation (GDPR) across all its member states, a new law that concerns and applies to the processing practices and activities of all EU residents' personal data (Goddard, 2017; Albrecht, 2016). Privacy in this new law is considered and understood as a fundamental human right and data protection by design and default is central to it (Goddard, 2017). Information privacy is, and has been for some time now, a central issue facing business practice (Awad & Krishnan, 2006).

An important question to consider is whether and in what way consumers' information privacy experiences and perceptions may have changed since the introduction of the GDPR. More specifically, essential to the regulation are its aims of ensuring more information

transparency, information control, and information security. However, whether consumers' online experiences with and perceptions of (i.e. their understanding and sense-making of) these concepts are significantly different now compared to before the GDPR was introduced is not yet fully clear and still insufficiently addressed. This gap in the literature presents an opportunity for further exploration. The purpose of the study at hand thus is to explore consumers' online experiences with and perceptions of information transparency, control, and security in the post-GDPR era. This is done by means of quantitative survey research. Note that 'the post-GDPR era', a term commonly used in the existing literature, refers to a time frame that started in May 2018, when the GDPR came into force. As the GDPR still applies today, the present day is considered part of the post-GDPR era. To increase the contextuality of this study, focus is specifically on Dutch consumers' information privacy experiences and perceptions. This leads to the following research question: *What are Dutch consumers' online experiences with and perceptions of information privacy in the post-GDPR era?*

Many of the existing studies on the GDPR have examined its legal ramifications, its technological and economic consequences, and its impact on privacy policies and data practices. Importantly, most of these studies focused on the business side of things. In comparison, fewer studies so far have considered consumers' experiences and perspective on the GDPR. This study aims to do exactly that. As of now it is still not yet fully clear whether the GDPR has achieved some of its main goals, namely providing more information transparency, control, and security. The question remains whether consumers find that their online experiences with and perceptions of these information privacy concepts have improved since May 2018, keeping in mind all the changes the regulation has brought about in the privacy landscape. This study makes a first attempt at exploring the answer to this question.

In addition to contributing to this stream in privacy and information research, this study also holds practical relevance for EU legislators and business and marketing managers. The GDPR is a regulation "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (European Union, 2016, p. 1). Hence, legislators will be interested in how consumers experience and perceive this protection of their data four years after the GDPR came into force. Also, collecting and leveraging consumer data is crucial for many businesses in today's digital 'day and age'. It is therefore in businesses' best interest to know more about consumers' information privacy experiences and perceptions as these may affect how they feel about sharing their personal information and

otherwise behave and engage with websites online. Especially considering the restrictions the GDPR has imposed on data collection and the nearing demise of third-party cookies, marketing practitioners are becoming increasingly reliant on first-party data and consumers' explicit consent (Wiles, 2021). It is therefore important for them to be aware of consumers' perspective on information privacy and legislation. Also, previous research has shown that consumers' information privacy perceptions directly or indirectly affect other behavioral intentions that are important for businesses, such as (online) purchase intentions (e.g., Windiarti et al., 2020). This study helps inform professionals about consumers' perspective on these matters affected by the GDPR.

The structure of the remainder of this thesis is as follows: The next chapter covers the theoretical framework underlying this study. The chapter starts with a discussion of the contextual background. This includes an explanation of the GDPR's main principles and goals and a brief overview of (a selection of) previous studies that have examined the impact of the regulation. Next, three main information privacy concepts (information transparency, control, and security) are discussed in more detail and a number of research questions are proposed to further guide this study. The third chapter covers the methodology used to collect and analyze data. It includes a discussion of the research design, the target population and sample, the survey instrument, the validity and reliability of the measures, the study procedure, and the data analysis method. In the fourth chapter the most important results (and some additional results) from the data analyses are presented. Finally, the fifth and final chapter covers this study's findings and implications and includes a discussion of the research limitations, as well as a general conclusion.

2. THEORETICAL FRAMEWORK

2.1 Contextual background

The exploitation of personal data has been found to have a multitude of benefits. Not only for companies, but also for consumers. Marketeers can leverage this data to improve their customer relationships, for example, by personalizing their products and services, or even their entire marketing mix, or by otherwise offering more value and enhancing the customer experience (Wedel & Kannan, 2016). In any case, there are various ways for brands to extract the great economic value of personal data (Duan et al., 2020). Clearly, consumers may also benefit from some of these data-driven marketing decisions and practices, for example, when their online experience is enhanced by customized content and advertisements.

However, the collection and use of personal data and related marketing practices are not always considered beneficial by consumers, as they have the tendency to spark information privacy concerns (Duan et al., 2020). Consumers may then feel anxious about sharing their personal information and feel suspicious about what is done with that information (Duan et al., 2020). Personal data can be abused in alarming ways. It can be used for economic and social discriminatory practices, manipulation, or censorship, to name just a few (Acquisti et al., 2015). Companies might also share (or sell) their customers' data with third parties, such as business partners, and might experience data breaches which would potentially reveal personal information to unknown parties (Schudy & Utikal, 2017). Sharing more data then does not always lead to 'good things' per se, as it relates to the erosion of privacy and the consequences that that entails (Acquisti et al., 2015). Researchers have previously highlighted the significance of these developments. It has been argued that, "if this is the age of information, then privacy is the issue of our times" (Acquisti et al., 2015, p. 509). Or more specifically, the "collection and processing of data have made information privacy one of the most important ethical, legal, social, and political issues of the information age" (Ozdemir et al., 2017, p. 642).

In response to the widespread concerns over privacy several regulatory changes have been made in recent years. The following section focuses on one of the most notable regulatory changes, namely the EU's introduction of the General Data Protection Regulation (GDPR). The regulation's main principles are first discussed in more detail which serves to introduce the information privacy concepts that are central to this study.

GDPR

The GDPR came into force in May of 2018. This legislative framework involves bold rules for the protection of EU residents' personal data and harmonizes data protection laws across all member states (Dabrowski et al., 2019; Urban et al., 2020). It is considered "the Magna Carta of data protection" (Gal & Aviv, 2020, p. 349) and "a landmark in the evolution of the European privacy framework" (Goddard, 2017, p. 703) and is seen as one of the most prominent and strict regulatory frameworks for the protection of personal data on a global level (Dabrowski et al., 2019). The GDPR is meant to better protect individuals from unauthorized or misuse of their data, which might cause them harm or otherwise negatively affect them (e.g., being a victim of price or other forms of discrimination) (Gal & Aviv, 2020). Central to the GDPR is its aim to alter the power balance between data subjects on the one hand and data controllers on the other (Gal & Aviv, 2020). More specifically, it confers greater autonomy and leverage to data subjects (Almeida & Monteiro, 2021; Bauer et al., 2021). Another goal is to act as a reassurance to people that their data will not be handled in inappropriate or unreasonable ways and thereby strengthen people's trust in this regard (Gal & Aviv, 2020). Ever more people are now sharing their data with various services and data breaches are a common occurrence. With this legal framework, the EU is taking a firm stance on the issue of data protection and security (Wolford, n.d.).

Personal data is defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject')" (European Union, 2016, p. 33) and thus includes many types of data. The GDPR introduces strict rules for the ways and situations in which personal data can be collected, stored, used, and shared, thereby imposing several obligations and limitations with regards to data processing (Gal & Aviv, 2020; Dabrowski et al., 2019). The regulation is lengthy and extensive but revolves around a number of key points. For example, central to the GDPR are the principles relating to the processing of personal data. These include, for example, the principles of lawfulness, fairness, and transparency, purpose and storage limitation, and integrity and confidentiality (European Union, 2016). Also, the GDPR prescribes the kind of legal basis data controllers now require to process personal data (Dabrowski et al., 2019). Article 6 outlines six legal bases for lawful data processing. The first basis, and in the context of this study the most important basis, concerns a data subject's consent for processing their data (European Union, 2016). Importantly, the GDPR introduces

strict rules for what exactly constitutes such consent, how it may be requested and how it should be managed (Wolford, n.d.).

The GDPR also emphasizes the rather extensive list of privacy rights afforded to data subjects. They have the right to be informed, the right of access, right to rectification and erasure of personal data, to name a few (European Union, 2016). A key part of the GDPR thus is ensuring that data processing is fair and *transparent*, as well as enabling people to have (more) *control* over their own data. Also, data protection by design and default are other key principles of the regulation. Important in this regard is the "implement[ation of] appropriate technical and organisational measures" (European Union, 2016, p. 48). These measures should ensure that personal data are always handled safely and kept secure. Data (or information) *security* then is another key concept within the GDPR. Notably, the GDPR has increased the power of state institutions in terms of their ability to sanction those who violate the terms of the regulation, as organizations acting in violation of this law may now face hefty fines (Bauer et al., 2021).

Previous studies

The existing literature on the GDPR spans across various disciplines. From computer science to health science and business, studies have examined the impact of the GDPR in many different contexts. For example, previous research has discussed its legal ramifications (e.g., Morrissey, 2016) and economic consequences (e.g., Allen et al., 2019). It has also looked into how app privacy has changed since the implementation of the GDPR (Momen et al., 2019) and considered the regulation's impact on global technology development (Li et al., 2019), web privacy (Degeling et al., 2019), third party presence (Sørensen & Kosta, 2019), browser cookies usage (Dabrowski, 2019), data sharing in ad networks (Urban et al., 2020), trust in data collectors (Bauer et al., 2021), and the user experience (Almeida & Monteiro, 2021), to name a few. Notably, many of the existing studies focus on the implications for businesses or other organizations, governments, the economy, or society more generally. As was previously pointed out by Strycharz et al. (2020), studies focusing on individuals' perceptions of and perspective on the GDPR are scarce. This presents a gap in the literature that this study attempts to fill. The exact aim and main concepts of this study are discussed in detail in the following sections.

2.2 Main concepts of this study

The European Commission's key objectives for the GDPR concern the level of *transparency* provided to data subjects, the level of *control* they have over their own data, and the level of protection and *security* of (sensitive) personal data, among other things (Strycharz et al., 2020). Information transparency, control and security are central to the GDPR and thus represent three of its key themes, or goals. The question then is if, based on and measured from a consumer's perspective, these goals have been achieved? In other words, has the GDPR (so far) had the desired effect in terms of consumers' experiences with and perceptions of these key concepts?

As noted before, perceptions here involve not just how people see these concepts, but also how they understand them, how they make sense of them, and what they mean to them. More specifically, perception here is understood as "the process how people select, organize, and interpret information inputs to create a meaningful picture of the world", a process which "depends not only on physical stimuli, but also on the stimuli's relationship to the surrounding environment and conditions within each of us" (Gáti & Simay, 2020, p. 3). Because of the individual nature of perceptual processes, people may hold different perceptions about the same thing (Gáti & Simay, 2020).

This study aims to explore Dutch consumers' online experiences with and perceptions of information transparency, control, and security in this post-GDPR era. An additional aim is to examine how consumers' individual characteristics (e.g., demographic characteristics and individual capabilities) might influence their experiences and perceptions. Based on these aims, several research questions are developed and presented in the following sections.

<u>Information transparency</u>

It has been argued in previous studies that transparency (as a general concept) is both ethical and advantageous (Holland et al., 2018). According to Hauff et al. (2017), information transparency refers to "the extent to which an online firm provides features that allow customers to access the data collected about them as well as informs them on how and for what purposes the acquired information is going to be used" (p. 5007). The concept thus revolves around "the degree of information flow", not only within a company but also between the company and its customers (Foscht et al., 2018, p. 480). It is based on the voluntary and intentional sharing of high-quality information (Foscht et al., 2018). According

to Schnackenberg et al. (2021), transparency as a construct has three primary dimensions, namely perceived disclosure, clarity, and accuracy. Important attributes then include the (perception of) availability, accessibility, simplicity, understandability, comprehensibility, reliability, and correctness of information (Schnackenberg et al., 2021).

More consumers now want to be informed about what data and how much of their data is collected, how exactly it is stored, and whether or with whom it is shared (Dinev et al., 2013). In line with the GDPR, organizations should ensure full transparency by providing consumers with extensive information in a clear and accessible manner so that the information is easy to understand (Goddard, 2017). Transparency has been a feature of EU law for many years. By making it easier for people to understand the processes that affect them, transparency can help engender trust in these processes. Transparency as a concept is naturally closely linked to other concepts or principles that are important under the GDPR, namely fairness and accountability (Article 29 Data Protection Working Party, 2018). It is an obligation that applies to "the provision of information to data subjects related to fair processing; how data controllers communicate with data subjects in relation to their rights under the GDPR; and how data controllers facilitate the exercise by data subjects of their rights" (Article 29 Data Protection Working Party, 2018, p. 4). Transparency here is user-centric more so than legalistic and represents "a move away from legal tick-box compliance to a tailored, reflective and dynamic approach" (Goddard, 2017, p. 704), empowering data-subjects (Article 29 Data Protection Working Party, 2018).

According to findings from a previous study (Gáti & Simay, 2020), users clearly wish for companies to inform them about the collection and use of their personal information and for transparent disclosure of privacy directives. The concept of transparency and the GDPR's obligations and goal in this regard are clear. Findings from one study (Presthus & Sørum, 2019) have suggested that some improvements have been made in this regard, as it is concluded that "consumers gained significant knowledge about their information privacy from the GDPR" (p. 19). For example, in response to a question about cookies, almost half of all respondents checked the answer option "Companies have become much better at informing website visitors about cookies" (Presthus & Sørum, 2019, p. 24). Although this provides an indication, it is not yet fully clear if and how consumers' online experiences with and perceptions of information transparency have changed since the implementation of the

GDPR. The existing literature has not yet determined whether or to what extent this goal of the GDPR has been achieved. This leads to the following research question:

RQ1: What are Dutch consumers' online experiences with and perceptions of information transparency in the post-GDPR era?

Information control

It has previously been argued that the element of control is one of the main factors of privacy (Dinev et al., 2013). In line with a study by Taddei and Contena (2013), consumers' perceived control over information here refers to their perception "about the possibility of managing their own information" (p. 823) and thus concerns "the power of consumers to decide what is learned about them" (Taylor et al., 2009, p. 208). Central to the concept is the influence consumers have on the flow of their own data (Ifenthaler & Schumacher, 2016). Not only in terms of the initial information disclosure, that is, but also when it comes to the use of information once it is obtained (Dinev et al., 2013).

In line with the GDPR, organizations should give consumers control over their own data by requiring their informed consent to process data and enabling them to take decisions regarding the use of their data. As previously noted, enhancing individuals' control over personal information is one of the GDPR's main goals. Compared to previous EU regulations, the GDPR more explicitly highlights the importance of control and empowers individuals in this regard (van Ooijen & Vrabec, 2019). The GDPR contains multiple references to this concept of control in its provisions and recitals, such as in those on consent and the rights of data subjects (van Ooijen & Vrabec, 2019). While the GDPR is clear in its intentions, it is not yet entirely clear if consumers perceive their control over their personal data to have strengthened significantly since the implementation of the GDPR. As part of a survey conducted by Deloitte (2018), called 'A new era for privacy: GDPR six months on', a sample of consumers was asked whether the regulation increased the control they have over their personal data. Just over half of participants indicated to think so, at least to some extent (Deloitte, 2018). However, it is also concluded in the report that "most people do not feel that GDPR has done enough to increase the control they have over their data" (Deloitte, 2018, p. 5). In a Eurobarometer survey conducted in 2019 (European Commission, 2019), respondents were asked about their perceived control over personal data they provided online, a question

that produced almost the exact same result as it did four years earlier, in 2015. Whereas the report shows that perceived control over data has increased or decreased quite significantly in some European countries, perceptions appear to have been quite stable in the Netherlands and various other countries (European Commission, 2019). In a survey conducted by Presthus and Sørum (2019), Norwegian respondents were asked to what extent they find their personal information to exist in places they have no control over. Most respondents indicated they had partial control (46,79%) or no control at all (38,53%). However, these findings were not discussed in relation to the impact of the GDPR. Notably, all of these surveys were conducted within one year after the implementation of the GDPR. At this time, four years after the regulation came into force, it is still unclear if and how consumers' online experiences with and perceptions of information control have changed since the implementation of the GDPR. Hence, the following research question is proposed:

RQ2: What are Dutch consumers' online experiences with and perceptions of information control in the post-GDPR era?

Information security

Based on the international standard ISO/IEC 27000 (2018), information security can be understood as the "preservation of confidentiality, integrity and availability of information", noting that "other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved" (International Organization for Standardization, Terms and definitions). These information security 'properties', or objectives, as well as others, have also been noted by practitioners and academicians in previous literature (e.g., Ma et al., 2008). According to the SANS Institute, information security has to do with the "processes and methodologies which are designed and implemented to protect […] confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption" (n.d., n.p.). In line with the definition proposed by Chellappa and Pavlou (2002), perceived information security here is understood as "the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage or by inappropriate parties" (p. 359). Again, this is a subjective, personal perception rather than an objective measurement (Chellappa &

Pavlou, 2002). It is about an individual's *belief* about whether their data is or will be secure (Mohr & Walter, 2019).

In line with the GDPR, organizations should ensure the security of consumers' data by being accountable and being responsible in their handling of personal data, through data breaches monitoring and notification regimes, and by being proactive and setting up prevention plans (Goddard, 2017; Piras et al., 2019). The GDPR is thus not only concerned with ensuring that data are not compromised but is also about the way organizations deal with it and communicate about it if they are. Consumers' perceptions of security are important as they may form the basis for and affect various attitudes and behavioral intentions, such as trust or online purchase intention (Mohr & Walter, 2019). It seems then that organizations have strong incentives to provide this security. Interestingly, the GDPR Enforcement Tracker (n.d.) shows that the third most fined type of violation of the GDPR is 'Insufficient technical and organisational measures to ensure information security'. This suggests that non-compliance with the GDPR in this regard is an issue. As noted in a previous study on GDPR perceptions (Gáti & Simay, 2020), "it is worth analysing what actual changes the regulation caused in users' security-related perception" (p. 3). At this time, it is unclear how consumers' online experiences with and perceptions of information security have changed since the implementation of the GDPR. For this reason, the following research question is proposed:

RQ3: What are Dutch consumers' online experiences with and perceptions of information security in the post-GDPR era?

Individual characteristics

Previous studies have considered the influence of various demographic characteristics on privacy variables of interest. For example, several studies have examined gender differences in privacy concerns and behaviors on social networking sites. These studies have reported mixed findings (Tifferet, 2019). Other studies have looked into how people in different age groups differ in terms of, e.g., their privacy attitudes and privacy management behaviors (Kezer et al., 2016) and privacy concern and privacy protection (van den Broeck et al., 2015).

Privacy concern itself is also a factor that has been found to affect various types of (privacy) attitudes, behaviors, or perceptions. It has been conceptualized (and thus also operationalized) in different ways across studies. Although different in structure, many of the

developed measurement scales do have in common a few items or dimensions, such as those regarding the collection of information and the unauthorized use or access of that information (Li, 2011). (Online) privacy concern has been a central concept in many studies and has been linked to, e.g., privacy protection behaviors (Chen & Chen, 2015), trust in e-vendors (Kim, 2008), e-commerce use (Dinev et al., 2006), perceived uncertainty in online exchange relationships (Pavlou et al., 2007), willingness to provide information (Premazzi et al., 2010), willingness to buy (Faja & Trimi, 2006), and frequency of online transactions (Akhter, 2014).

Also prevalent in the privacy literature are concepts related to individuals' capabilities, or beliefs about their capabilities in the digital landscape. Concepts such as internet skills or internet literacy have been studied in relation to, e.g., privacy protection behaviors (Büchi et al, 2017), online privacy management (Hargittai & Litt, 2013), internet privacy concerns, and intention to transact online (Dinev & Hart, 2005). A related but distinct concept is internet self-efficacy, or "beliefs in one's ability to navigate the internet and accomplish different tasks" (Akhter, 2014, p. 119). Internet self-efficacy has previously been linked to, e.g., online technical protection privacy behavior (Lee et al., 2017), privacy concern, and the frequency of online transactions (Akhter, 2014).

It is clear from the discussion above that certain individual characteristics, including demographic characteristics such as gender, age, and educational level, but also individuals' level of privacy concern, internet skills, and internet self-efficacy may well influence other concepts related to privacy, such as the ones central in this study. The question then is what role these variables play in the formation of consumers' online experiences with and perceptions of information transparency, control, and security. Thus, the following question is proposed:

RQ4: How do individual characteristics affect Dutch consumers' online experiences with and perceptions of information transparency, information control, and information security?

3. METHODOLOGY

3.1 Research design

The questions guiding this study are exploratory. The purpose is to find out more about Dutch consumers' online experiences with and perceptions of the current privacy landscape in terms of information transparency, control, and security in this post-GDPR era. In order to achieve this purpose and answer the proposed questions an exploratory, quantitative online survey research method was adopted. A survey was developed and carefully pre-tested before being distributed to respondents online. There are some advantages to conducting online survey research that are particularly relevant for this study. For example, quantitative online surveys make it easy to reach certain groups (i.e. people with common characteristics) or populations in a relatively short amount of time, (generally) at a relatively low cost (Wright, 2005). A disadvantage is that there often is little opportunity for any potentially relevant side-tracking, follow up questions, or further elaboration. Online survey questions may thus not provide as detailed and nuanced responses as e.g., face-to-face interview questions. However, as this study is exploratory in nature and aims to provide an initial understanding of consumers' experiences and perceptions, subsequent research can build on this and employ complimentary research methods to produce more specific and nuanced findings.

3.2 Population and sample

The population of interest in this study is Dutch consumers. The sample that was drawn therefore consisted of Dutch consumers. Naturally, having the Dutch nationality was a prerequisite for participation in this study. Notably, the survey was conducted in Dutch, so a (near)native understanding of the Dutch language was also an important prerequisite. No other inclusion criteria for the sample applied.

An online recruitment platform was used to find a sample of respondents. This online data collection method was used because of the speed with which responses could be collected and the ease with which demographically diverse people from a specific population could be recruited. Prolific, the platform that was used, was launched in 2014 and mostly caters to researchers and startups (Peer et al., 2017). When compared to other platforms and panels such as MTurk, Qualtrics, and CloudResearch, Prolific was found to outperform the others in terms of its overall score on data quality (Peer et al., 2021). Prolific also has other important features, such as its many (free) pre-set filters to pre-screen and filter the audience.

In addition, Prolific has clear rules and guidelines for both researchers and participants and adheres to a minimum hourly reward for participants (Palan & Schitter, 2018).

Two pre-screening filters were used in the selection procedure for this study. The 'Nationality' filter was set to 'Netherlands' to ensure that all respondents were Dutch and the 'Fluent languages' filter was set to 'Dutch' to ensure that all respondents had a good understanding of the Dutch language. The sample size was set to 300 responses. Given that not all Dutch consumers (i.e. members of the target population) were equally likely to be invited to partake in the study, the sample is considered a nonprobability sample (Albert et al., 2010). More specifically, considering the nature of the sampling procedure in this study (i.e. participation was on a first-come, first-serve basis), the sample is a convenience sample. Note that the sample is not considered or claimed to be representative for the entire target population. Recruitment for this study took place between 17 and 20 May 2022.

Some basic demographic characteristics of the final sample are reported in Table 1. The age range of respondents was quite broad, as the youngest respondent was 19 years old and the oldest was 76 years old. Overall, however, this sample was relatively young, as the average age of respondents was a little under 32 (*M* = 31.64). As for the gender division, the sample was well balanced, as both males and females made up 48% of the sample. The sample was also reasonably balanced in terms of respondents' educational level. Those with a (relatively) low educational level (i.e., high school degree or secondary vocational education) made up 29% of the sample. Those with a high educational level (i.e., academic Bachelor's, Master's, or Doctoral degree) made up approximately 40% of the sample. Those in between (i.e., secondary vocational education) made up 31% of the sample. Overall, most respondents in this sample had obtained an additional degree after high school.

Table 1

Demographic statistics of the sample (frequency, percentage, mean, standard deviation, minimum and maximum)

Variable	Answer categories	*n*	*%*	*M*	*SD*	*Min/Max*
Age				31.64	10.81	19/76
Gender	Male	144	48			
	Female	145	48			
	Other	8	3			
	Prefer not to say	3	1			

Table 1 (continued)

Educational level	High school degree	60	20
	Secondary vocational education	26	9
	Higher vocational education	93	31
	Academic Bachelor's degree	50	17
	Academic Master's degree	62	21
	Doctoral degree	9	3

3.3 Survey instrument

Consumers' online experiences with and perceptions of information transparency, control, and security were measured using (adapted) items from existing scales as well as a number of new items. Specifically, *information transparency* was measured using five items, of which four were adapted from a scale used by Awad & Krishnan (2006) and one was a new item. An example item is 'Websites are transparent about what information they collect about me'. *Information control* was measured using five items, of which three were adapted from a scale used by Xu (2007). The remaining two items were adapted from surveys conducted by the European Commission (2019) and Presthus and Sørum (2019), respectively. An example item for this scale is 'I have control over the amount of information websites collect about me'. *Information security* was measured using five items, of which two were adapted from a scale used by Chellappa and Pavlou (2002) and three of which were new items. For example, an item included in this scale is 'Websites protect my information from misuse'. Consumers' *privacy concern* was measured using one new item (similar to single-items used in previous studies): 'How concerned are you about your privacy on the internet?'. The item thus directly asked consumers for their general level of concern regarding their privacy on the internet. Consumers' perception of their *internet skills* and *internet self-efficacy* were measured using one new item and three items which were adapted from a scale used by Kim et al. (2021), respectively. An example item for the latter scale is 'I am well able to use the internet for various tasks or activities'. All but one of these items were measured on a 5-point Likert scale, ranging from strongly disagree to strongly agree. The item measuring privacy concern was the only item of a categorical nature. The survey also included a few additional items, which are discussed in a later section. The final survey consisted of 32 items in total and is reported in Appendix 1. A table showing all *original* scale items alongside the adapted versions for the survey can be found in Appendix 2.

Pre-tests

The survey used in this study was pre-tested before its official distribution. The first pre-test was of a qualitative nature. Five Dutch consumers were asked to join the researcher for a short meeting and fill in the survey through a Qualtrics link. The think aloud method was used in these sessions. The purpose of this pre-test was to check whether there were any issues with the survey's instructions and scale items in terms of their comprehensibility. Respondents' comments helped determine which items or words could lead to confusion or misunderstanding. Based on these comments and feedback some minor changes were made. The second pre-test was of a quantitative nature. Prolific was used to recruit 25 responses. The purpose of this pre-test was to provide an indication of the reliability and validity of the scales and to check whether all technical aspects of the survey were working correctly. Based on these data a few items were deleted or adapted. The resulting final survey was then distributed to a large sample (N = 300) of eligible respondents to collect data for this study.

Validity and reliability of the measures

Factor analyses were performed to examine the validity of all multi-item constructs (i.e., information transparency, information control, information security, and internet self-efficacy). Principal axis factoring was used as the extraction method in these factor analyses. Direct Oblimin was used as the rotation method. Notably, a first factor analysis showed that the fifth item measuring information control had an extremely low communality (0.058). It also had very low factor loadings (< 0.138) and severe cross-loading issues. The item was deleted for these reasons.

A second factor analysis was performed, this time with one less item. The Kaiser-Meyer-Olkin test for sampling adequacy and Bartlett's test of sphericity confirmed the suitability of the data for this analysis (0.857 and $p < 0.001$, respectively). The pattern matrix showed that all items from each construct loaded on one specific factor, and one factor only. Communalities were satisfactory, as almost all items had a communality of well above 0.4. Four factors had eigenvalues greater than 1. Hence, based on Kaiser's criterion, four factors were extracted. Cumulatively these four factors explained around 64% of all variance.

Reliability analyses were also performed for each of the four multi-item constructs. The Cronbach's Alpha values indicated that the constructs had good levels of internal consistency. The Alpha values, eigenvalues and percentages of explained variance of each

construct are reported in Table 2 below, along with the (rotated) factor loadings of all items. More output from the factor analyses is reported in Appendix 3.

Table 2

Validity and reliability of the measures (factor loadings, eigenvalues, percentages of variance, and Cronbach's Alpha)

Items	Loading	Eigenv.	% Var.	α
Information transparency		1.66	9.76	0.83
Websites are transparent about what information they collect about me.	-0.64			
Websites are transparent about why or for what purpose they collect information about me.	-0.78			
Websites are transparent about how long they store my information.	-0.76			
Websites are transparent about how they use my information.	-0.68			
Websites are transparent about the rights I have regarding the processing of my information.	-0.51			
Information control		1.38	8.13	0.72
I have control over the amount of information websites collect about me.	0.74			
I have control over how websites use my information.	0.55			
I have control over who has access to my information.	0.58			
I have control over the information I provide to websites (e.g., by being able to correct, change, or delete that information).	0.52			
Information security		5.59	32.86	0.88
Websites take their responsibility to protect my information seriously.	0.8			
Websites protect the integrity of my information.	0.83			
Websites protect my information from misuse.	0.88			
Websites do not share my information with other parties.	0.6			
My information is not viewed, stored or manipulated by unauthorized parties.	0.66			
Internet self-efficacy		2.28	13.4	0.82
I easily learn new internet skills.	0.74			
I am well able to use the internet for various tasks or activities.	0.76			
I can solve problems on the internet by myself.	0.85			

3.4 Study procedure

As previously noted, the survey was conducted using an online recruitment platform. Taking into account the pre-screening filters (Dutch nationality and fluency in Dutch), Prolific distributed the survey to a random subset of eligible respondents. Participation in the survey was then on a first-come, first-serve basis. The survey automatically closed when 300 completed responses were recorded.

Given the involvement of a large number of people in this study, it was important that certain ethical principles were upheld. For this reason, this study was reviewed (and subsequently approved) by the BMS ethics committee of the University of Twente. With regards to the survey, transparency about the procedure and steps in the process was provided up front. First, respondents were made aware of the topic of the survey by providing them with a title and a short description, being careful not to give away too much at this point to avoid potential biases. Respondents were then assured of their anonymity, as well as the safety and confidentiality of their data. They were also asked to confirm that they wanted to participate in the survey by providing their consent.

The first question respondents were asked in the survey was whether they had ever heard of the GDPR. If their answer was 'yes', they were then asked to what extent they had knowledge of, or were familiar with, the content of the GDPR. If they indicated to have some knowledge or good knowledge of the content, they were then asked to what extent they understood this content. Note that if respondents declared not to have heard of the GDPR, they were not shown any of the latter two follow-up questions. Instead, they were provided with a brief explanation about the GDPR, which they could choose to read or not. If respondents indicated to have heard of the GDPR but not to have knowledge of its content, they were also rerouted to the brief explanation. Ultimately, a large majority of all respondents (87%) was shown the first follow-up question about their knowledge of the GDPR and most respondents ($\pm$ 70%) were also shown the second follow-up question about their understanding of the GDPR.

There were no more alternative routings after the first three questions, meaning that from that point on all respondents were presented with exactly the same questions. As noted previously, this included questions about (perceptions of) information transparency, control, and security, and privacy concern, internet skills, and self-efficacy. The survey also included a number of additional questions. Respondents were asked about their perceptions of the

impact of the GDPR, their satisfaction with it, and their opinion on the importance of the law. In addition, three questions asked respondents to compare their current information privacy experience to their experience four years ago. Finally, the survey included questions about respondents' gender, age, and educational level. Some of these questions were Likert scale questions, others were multiple choice or open questions. After answering all survey questions, respondents were kindly thanked for their participation. The full survey including the opening and closing statements is reported in Appendix 1.

3.5 Data analysis method

Several statistical analyses were performed using SPSS Statistics 27 to examine the 300 survey responses. Specifically, descriptive analyses were carried out mainly to determine how respondents (on average) scored on the variables of interest in this study (i.e., information transparency, control, and security). Also, analyses of variance (ANOVA) were conducted to determine if different groups of respondents had (significantly) different scores on these variables. These groups differed in terms of respondents' gender, age, educational level, privacy concern, internet skills, and internet self-efficacy. All of these variables were split into either two or three groups (e.g., low, middle, and high) for use in the analyses.

For example, age was split into two groups based on how old respondents were when the internet first became more readily accessible to the general public (early/mid 1990s). Those in the first age group (18-29 years old) were either very young or not even born yet at that time. Those in the second age group (30+) were children, teenagers, or already adults. The difference between the two groups is thus that most of those in the first group likely grew up with the internet and many of those in the second group likely did not. As a negative effect between age and technology acceptance has been found in previous studies (e.g., Hauk et al., 2018), people's age at the time of the internet's commercial introduction could affect their (current) use of the internet and in turn their perceptions of their information privacy on the internet. Educational level was split into three groups based on respondents' highest attained degree. Those with a high school degree and those with a degree from secondary vocational education represent the lowest education group, those with a degree from higher vocational education represent the middle education group, and those with an academic degree represent the highest education group. Privacy concern was split into three equal groups (100 respondents each) based on scores ranking from lowest to highest. This resulted in 'low',

'middle', and 'high' groups for privacy concern. Similarly, internet skills and internet self-efficacy were split into two (rather than three) equal groups (150 respondents each) because there was a lack of low scores on these variables: (most of) the scores were relatively high and clustered on that (right) side of the spectrum. This resulted in only 'middle' and 'high' groups for internet skills and internet self-efficacy.

The mean scores and standard deviations for all groups are reported in Table 3 below. The results of three ANOVA tests comparing the mean scores of the groups are also reported in Table 3. These results (and the results of a post-hoc analysis for the privacy concern groups) showed that the mean scores of all groups on each variable differed significantly, which confirms the feasibility of using these groups for subsequent analyses.

Table 3

Descriptive statistics and ANOVA test results showing the differences between groups

Variable	Group	*M (SD)*	*df*	*F*	*p*	η^2
Privacy concern	Low (N = 100)	2.22 (0.56)	2	257.864	0.000*	0.635
	Middle (N = 100)	3 (0)				
	High (N = 100)	3.87 (0.69)				
Internet skills	Middle (N = 150)	3.78 (0.46)	1	332.595	0.000*	0.527
	High (N = 150)	4.73 (0.44)				
Internet self-efficacy	Middle (N = 150)	3.89 (0.32)	1	797.635	0.000*	0.728
	High (N = 150)	4.82 (0.25)				

** $p < 0.05$*

Note. Privacy concern was measured as a categorical variable with five categories ('not worried at all' – 'deeply worried'). Internet skills and internet self-efficacy were measured on a 5-point Likert scale (strongly disagree - strongly agree)

4. RESULTS

As previously noted, all items for information transparency, control, and security were measured on a 5-point Likert scale. Composite scores were calculated for each respondent for all three variables for use in analyses. The lowest score (1) should be interpreted as indicating very low levels of (perceived) information transparency, control, and security, and the highest score (5) should be interpreted as indicating very high levels. On average, respondents (N = 300) scored lowest on information control (M = 2.28), followed by information transparency (M = 2.34). They scored highest on information security (M = 2.4), although only by a small margin. One sample t-tests confirmed that these mean scores were all significantly lower than the (neutral) midpoint of the used scale. These scores thus suggest that, generally, respondents perceive information transparency, control, and security to be relatively low.

Several univariate analyses of variance were performed to gain a better understanding of respondents' perceptions of the information variables. Specifically, they were performed to test the effects of individual characteristics (gender, age, educational level, privacy concern, internet skills, and internet self-efficacy) on information transparency, control, and security. Descriptive statistics about these characteristics were reported in a previous section (Tables 1 and 3). The results of the analyses are discussed in the following sections.

4.1 RQ1: Information transparency

First, six variance analyses were performed using information transparency as the dependent variable. The mean scores, standard deviations and ANOVA test results are reported in Table 4 below. Females (n = 145), on average, scored higher (M = 2.41) on information transparency than males (n = 144, M = 2.28). The difference in mean scores was not significant, however (F(1, 287) = 2.209, p = 0.138). Also, the older age group (n = 138) had a noticeably lower mean score (M = 2.27) than the younger age group (n = 162, M = 2.41). Adhering to a cutoff of 0.05 for significance, the difference in mean scores again was not significant (F(1, 298) = 2.868, p = 0.091). As for educational level, those with a (relatively) low level of education (n = 86) had a higher score (M = 2.49) than those in the other education groups (n = 93, M = 2.26 and n = 121, M = 2.3). The difference was close to being significant (F(2, 297) = 2.515, p = 0.083). A clear pattern could also be detected in the mean scores of the three privacy concern groups. Those with a low level of privacy concern (n = 100) had the highest mean score (M = 2.52) and those with a high level of privacy concern (n = 100) had the lowest mean score (M = 2.19).

Notably, the ANOVA test result indicated that the difference between (at least two of) the mean scores was significant ($F(2, 297) = 5.144$, $p < 0.05$). The results of a post-hoc analysis showed that (only) the mean scores of those with a low level of privacy concern and those with a high level of privacy concern were significantly different. As for internet skills and self-efficacy, the mean scores increased as respondents' level of skills and self-efficacy increased as well ($n = 150$, $M = 2.2, 2.49$ and $n = 150$, $M = 2.28, 2.41$, respectively). Only the mean scores of the two internet skills groups differed significantly ($F(1, 298) = 11.572$, $p < 0.05$).

Table 4

Effects of individual characteristics on information transparency

Variable	Group	*M (SD)*	*df*	*F*	*p*	η^2
Gender	Male (N = 144)	2.28 (0.8)	1	2.209	0.138	0.008
	Female (N = 145)	2.41 (0.71)				
Age	18-29 (N = 162)	2.41 (0.72)	1	2.868	0.091	0.010
	30+ (N = 138)	2.27 (0.77)				
Educational level	Low (N = 86)	2.49 (0.83)	2	2.515	0.083	0.017
	Middle (N = 93)	2.26 (0.7)				
	High (N = 121)	2.3 (0.71)				
Privacy concern	Low (N = 100)	2.52 (0.76)	2	5.144	0.006*	0.033
	Middle (N = 100)	2.32 (0.61)				
	High (N = 100)	2.19 (0.82)				
Internet skills	Middle (N = 150)	2.2 (0.68)	1	11.572	0.001*	0.037
	High (N = 150)	2.49 (0.78)				
Internet self-efficacy	Middle (N = 150)	2.28 (0.66)	1	2.217	0.138	0.007
	High (N = 150)	2.41 (0.82)				

** $p < 0.05$*

Note. Information transparency was measured on a 5-point Likert scale (strongly disagree - strongly agree)

4.2 RQ2: Information control

Next, six variance analyses were performed using information control as the dependent variable (see Table 5 for the results). The mean scores follow the same pattern as discussed above. Again, females ($n = 145$) on average scored higher ($M = 2.34$) on information control than males ($n = 144$, $M = 2.22$). The older age group ($n = 138$) scored lower ($M = 2.25$) than the younger age group ($n = 162$, $M = 2.3$). Those with a (relatively) low level of education ($n =$

68) scored higher (*M* = 2.32) than those in the other education groups (*n* = 93, *M* = 2.19 and *n* = 121, *M* = 2.31). Those with a low level of privacy concern (*n* = 100) had the highest mean score (*M* = 2.4) and those with a high level of privacy concern (*n* = 100) had the lowest mean score (*M* = 2.11). Finally, the mean scores increased or remained the same as respondents' level of internet skills and self-efficacy increased as well (*n* = 150, *M* = 2.25, 2.31 and *n* = 150, *M* = 2.28, 2.28, respectively). Only the ANOVA comparing the mean scores of the three privacy concern groups returned a significant test result ($F(2, 297) = 5.091$, $p < 0.05$). The results of a post-hoc analysis showed that (only) the mean scores of those with a low level of privacy concern and those with a high level of privacy concern were significantly different.

Table 5

Effects of individual characteristics on information control

Variable	Group	*M (SD)*	*df*	*F*	*p*	η^2
Gender	Male (N = 144)	2.22 (0.7)	1	2.252	0.135	0.008
	Female (N = 145)	2.34 (0.69)				
Age	18-29 (N = 162)	2.3 (0.64)	1	0.404	0.525	0.001
	30+ (N = 138)	2.25 (0.74)				
Educational level	Low (N = 86)	2.32 (0.67)	2	1.133	0.324	0.008
	Middle (N = 93)	2.19 (0.7)				
	High (N = 121)	2.31 (0.7)				
Privacy concern	Low (N = 100)	2.4 (0.7)	2	5.091	0.007*	0.033
	Middle (N = 100)	2.33 (0.65)				
	High (N = 100)	2.11 (0.7)				
Internet skills	Middle (N = 150)	2.25 (0.65)	1	0.475	0.491	0.002
	High (N = 150)	2.31 (0.73)				
Internet self-efficacy	Middle (N = 150)	2.28 (0.67)	1	0.000	0.983	0.000
	High (N = 150)	2.28 (0.71)				

** $p < 0.05$*

Note. Information control was measured on a 5-point Likert scale (strongly disagree - strongly agree)

4.3 RQ3: Information security

Finally, six variance analyses were performed using information security as the dependent variable (see Table 6 for the results). Notably, these analyses produced more significant results. Females (*n* = 145) on average scored significantly higher (*M* = 2.49) on information

security than males (n = 144, M = 2.31) (F(1, 287) = 4.301, p < 0.05). The older age group (n = 138) scored lower (M = 2.37) than the younger age group (n = 162, M = 2.42), but these differences were not significant (F(1, 298) = 0.083, p = 0.92). The lower education group (n = 86) scored higher (M = 2.51) than the other education groups (n = 93, M = 2.26 and n = 121, M = 2.42). The corresponding ANOVA returned a result that was close to being significant (F(2, 297) = 2.892, p = 0.057). Those with a low level of privacy concern (n = 100) had the highest mean score (M = 2.56) and those with a high level of privacy concern (n = 100) had the lowest mean score (M = 2.18). The ANOVA test result again indicated that the difference between (at least two of) the mean scores was significant (F(2, 297) = 7.393, p < 0.05). The results of a post-hoc analysis showed that the mean score of those with a high level of privacy concern was significantly lower than those with low or medium levels of privacy concern. Also, those with a high level of internet skills (n = 150) scored significantly higher (M = 2.5) than those with a medium level of internet skills (n = 150, M = 2.3) (F(1, 298) = 5.776, p < 0.05). Finally, the mean score increased as respondents' level of internet self-efficacy increased as well (n = 150, M = 2.38, 2.41), but the difference between scores was not significant (F(1, 298) = 0.132, p = 0.717).

Table 6

Effects of individual characteristics on information security

Variable	Group	*M (SD)*	*df*	*F*	*p*	η^2
Gender	Male (N = 144)	2.31 (0.71)	1	4.301	0.039*	0.015
	Female (N = 145)	2.49 (0.75)				
Age	18-29 (N = 162)	2.42 (0.74)	1	0.386	0.535	0.001
	30+ (N = 138)	2.37 (0.72)				
Educational level	Low (N = 86)	2.51 (0.86)	2	2.892	0.057	0.019
	Middle (N = 93)	2.26 (0.67)				
	High (N = 121)	2.42 (0.66)				
Privacy concern	Low (N = 100)	2.56 (0.72)	2	7.393	0.001*	0.047
	Middle (N = 100)	2.45 (0.68)				
	High (N = 100)	2.18 (0.75)				
Internet skills	Middle (N = 150)	2.3 (0.72)	1	5.776	0.017*	0.019
	High (N = 150)	2.5 (0.74)				
Internet self-efficacy	Middle (N = 150)	2.38 (0.69)	1	0.132	0.717	0.000
	High (N = 150)	2.41 (0.78)				

** p < 0.05*

Note. Information security was measured on a 5-point Likert scale (strongly disagree - strongly agree)

4.4 Additional results

As noted in the previous chapter, the survey included a number of additional questions. First, respondents were asked about their awareness, knowledge, and understanding of the GDPR. As previously explained, not all respondents were shown all three of these questions. Whereas 300 respondents filled in the question about their awareness of the GDPR, only 261 respondents (87%) were shown the first follow-up question about their knowledge of the GDPR, and only 209 (± 70%) were shown the second follow-up question about their understanding of the GDPR.

The results of a descriptive analysis of the scores (reported in Appendix 4) showed that the majority of respondents (87 percent) was aware of the GDPR. Most of those who were aware had some knowledge of the content of the GDPR (± 66 percent), rather than having no knowledge (± 20 percent) or good knowledge (± 15 percent) of it. Most of those who had some or good knowledge of the content had some understanding of it (± 71 percent), others had a good understanding of it (± 27 percent), and only few had no understanding of it at all (± 2 percent). Overall, it is clear from these results that most respondents were familiar (to varying extents) with the GDPR prior to taking part in this study

The survey also included three questions that asked respondents about their perceptions of the impact of the GDPR, their satisfaction with it, and their opinion on the importance of the law. The mean score and standard deviation for each of these variables are reported in Appendix 4. Note that these items were measured on a 5-point Likert scale. The lowest score (1) should be interpreted as indicating very low levels of (perceived) GDPR impact, satisfaction, and importance, and the highest score (5) should be interpreted as indicating very high levels. The mean scores suggest that, on average, respondents (N = 300) had a slightly positive perception of the impact of the GDPR (M = 3.35) and that they were slightly dissatisfied with the GDPR in its current form (M = 2.88). Notably, despite this (slight) dissatisfaction, respondents generally did quite strongly agree that the GDPR is an important law (M = 4.29). Note that one sample t-tests confirmed that all three of these mean scores were significantly higher or lower than the (neutral) midpoint of the used scale.

Respondents were also asked whether their perception of information transparency, control, and security had changed since the implementation of the GDPR in May 2018. Notably, the responses to these questions appear to be quite neutral. Based on the mean scores, respondents felt that information transparency had improved the most (M = 3.41),

compared to information control (*M* = 3.04) and security (*M* = 3.03). Unsurprisingly, three one sample t-tests showed that only the first of these scores (*M* = 3.41) was significantly higher than the (neutral) midpoint of the used scale. On average, respondents thus neither disagreed nor strongly agreed with the idea that information transparency, control, and security have improved since 2018. This indicates that either not much has changed for respondents since pre-GDPR, or they simply do not remember enough about that time to make such specific comparisons. Note that all mean scores and standard deviations are reported in Appendix 4.

5. DISCUSSION

5.1 Discussion of the results

The main research question of this study was first proposed in the introduction of this study: *What are Dutch consumers' online experiences with and perceptions of information privacy in the post-GDPR era?* The aim of this study was to provide insights into consumers' perspective on information privacy by specifically focusing on their views on *information transparency*, *information control*, and *information security*. Another aim was to examine the effects of *individual characteristics* on these views. Four questions centering around these concepts were developed and presented to guide this study. The findings in relation to these questions are discussed in the following sections.

Information privacy: transparency, control, and security

It was noted earlier that users have a clear need for transparent disclosure of privacy directives (Gáti & Simay, 2020). Based on the analysis of the data collected for this study, it appears that Dutch consumers generally find that the level of information transparency on websites is rather low, suggesting that their need for transparent disclosure is not yet sufficiently satisfied by websites. Previous studies have confirmed that websites generally have become more transparent, or at least more informative about their privacy policies and practices since the implementation of the GDPR (e.g., Kretschmer et al., 2021; Degeling et al., 2019). However, the results of this study imply that Dutch consumers' do not really (or at least not very strongly) perceive this to be the case. In line with previous research, one plausible explanation for this is that while websites may technically be sharing more information about their policies and practices, they do not do so in an accessible and understandable way. For example, one study (Kretschmer et al., 2021) found that information about privacy related practices is often still shared in a non-user-friendly way, thereby limiting its usefulness to consumers. To some extent, this may even be done on purpose, as "providers are aware of the discrepancy between what is legally required and what provides a practical benefit to the user", but "feel as if informing users […] beyond what is minimally legally required is not in their interest" (Kretschmer et al., 2021, p. 29). As a result, consumers may feel that transparency is often times not *truly* provided.

As was also discussed earlier, respondents of a Eurobarometer survey (European commission, 2019) were asked about their perceived control over personal data they provided online. Overall, close to two thirds of respondents indicated that they felt at least some control (specifically, most claimed to feel partial (rather than complete) control). In comparison, the results of this study suggest that Dutch consumers generally have a slightly more negative view on the level of control provided by websites. This may (in part) be due to differences in the response scales that were used, as consumers in this survey were not able to specifically specify whether they feel partial control, or maybe only feel control in some cases. In any case, the results are in line with the finding from a previous study (Kretschmer et al., 2021) that "the necessary control over personal data is [still] rarely provided to users" (p. 21). In another survey (Deloitte, 2018), just over half of all participants indicated to think that the GDPR has increased their control, albeit to varying extents. Notably, almost one third of respondents took a neutral stance. The results from this study are most in line with this latter finding, as respondents in this study (on average) felt rather neutral about the impact of the GDPR in this regard. This may be due to it (potentially) being difficult for respondents to remember exactly what they experienced and how they felt about this topic four years ago. Alternatively, as was suggested in the Deloitte report (2018), this neutral stance could also be because they are unaware of the control they could now have, in theory at least. In practice, however, it seems that some websites make it difficult for consumers to actually exercise this control. For example, although "online services more often provide means for their users to opt out of data processing, [they] regularly obstruct convenient access to such means through unnecessarily complex and sometimes illegitimate interface design" (Kretschmer et al., 2021, p. 1). As a result, it is not surprising that consumers may still experience very limited control.

Finally, as was also previously noted, data from the GDPR Enforcement Tracker (n.d.) indicated that not all organizations seem to take or establish sufficient measures to provide security and protect data. The results of this study, which suggest that the level of information security provided by websites is still perceived to be (somewhat) low, are not entirely surprising then. It was concluded in a previous study (Zaeem & Barber, 2020) that "the GDPR has made progress in protecting user data, but more progress is necessary" (p. 1). The results from this study seem to be most in line with the latter point, as respondents neither particularly disagreed nor agreed with the statement that their information is better protected since the implementation of the GDPR. It could be that still too many organizations

are not (yet) capable of providing, or do not know how to provide the kind of protection that is prescribed by the GDPR. Some may simply not be willing to. Alternatively, it may also be that these organizations are in fact providing a decent level of security, but do not communicate about it clearly enough. This is in line with the finding from Zaeem and Barber (2020) that "when there is non-compliance with the GDPR, it is often in the form of failing to explicitly indicate compliance" (p. 1). Consumers may then not *perceive* a high(er) level of information security because they have not seen or been told something that would make such a perception warranted.

Individual characteristics

The results of this study suggest that certain individual characteristics do affect perceptions of information transparency, control, and security. The most notable finding is that consumers' level of privacy concern clearly affects their perceptions on all three privacy variables. Specifically, it appears that the more concerned consumers are about their privacy, the less likely they are to agree that websites are transparent about the use and processing of their information, that websites give them sufficient control over their information, and that websites protect their data adequately. As noted previously, privacy concern has been studied in relation to many different variables (e.g., attitudes, behavioral intentions, etc.). Studies have, for example, found a negative relationship between privacy concern and trust in e-vendors (Kim, 2008) and a positive relationship between (information) privacy concern and perceived uncertainty in online exchange relationships (Pavlou et al., 2007). The results of this study seem to be in line with such findings, suggesting that privacy concerns seriously hinder websites in building trusting relationships with consumers and stimulating positive (privacy) perceptions. Reducing privacy concern is thus of key importance. Interestingly, it appears that people with a low, medium, or high level of privacy concern are not characterized by a specific set of individual characteristics. For example, all three privacy concern groups in this study were made up of an almost equal number of males and females and included people of many different ages, with different educational levels, and different levels of internet skills and self-efficacy. It might therefore be difficult for companies to try and identify (and for example target with a communication campaign) consumers who are very concerned, or not concerned at all.

Another interesting finding from this study concerns the effect of internet skills. Those with a high level of internet skills scored higher (although not always *significantly* higher) on all three privacy variables than those with a lower level. Previous studies have shown that internet literacy and self-efficacy are negatively related to privacy concern and positively related to the intention to transact online or the frequency of those transactions (Dinev & Hart, 2005; Akhter, 2014). It seems then that better internet capabilities might lead to more positive attitudes towards privacy and use of the internet. As was pointed out in a previous study (Dinev & Hart, 2005), "savvy and literate Internet users are more likely to be able to deal with privacy-invasive technologies, customize their browsers or Internet applications, […] and keep up with the latest antivirus, antispam applications" (p. 17, 19). As a result, they may be more aware of potential risks and problems and feel more capable of dealing with these issues, making them less concerned and less negative about their privacy. This is supported by the fact that the higher internet skills group in this study included noticeably more people with a low level of privacy concern and less people with a high level of privacy concern than the lower internet skills group.

Regarding the effect of gender, this study's results appear to confirm that males and females have different information privacy perceptions, as females on average had relatively more positive (or less negative) privacy perceptions than males in this study (although the difference was not always significant). This is in line with findings from previous studies that males and females differ in their privacy tendencies. These findings have been mixed, however, in terms of who they point to for having stronger privacy tendencies (Tifferet, 2019). Findings on this matter thus remain somewhat inconclusive.

As for age, the results are again in line with previous research. Those in the older age group (many of whom likely did not grow up with the internet) appeared to have more negative information privacy perceptions than those in the younger age group. As was noted in a previous study (Blank & Dutton, 2012), effects of age are often found in research about the internet. In line with a suggestion made in a study that considered the relationship between age and trust in the internet (Blank & Dutton, 2012), it may be the case that older individuals often have more negative information privacy perceptions due to "the degree to which older individuals tend to have less experience with the Internet and more scepticism about the role of technology in society" (p. 135). This effect appears minimal in this study, however, as the differences between the mean scores of the two age groups are generally

quite small. Given the omnipresence of the internet today, it may be that even those who did not grow up with the internet are experienced, knowledgeable, and comfortable with using the internet. Their online privacy experiences and perceptions then need not differ much from younger individuals, at least not on account of their age.

Finally, a consistent pattern is evident in the mean scores of those with a (relatively) low level of education, as this group scored higher on all variables than the other education groups. However, none of these differences are significant (although close). In line with the idea that educational background (and hence internet knowledge) may affect people's privacy (risk) perceptions (Kang et al., 2015), it could be that those with a lower level of education simply do not perceive as many privacy risks or problems as those with a high level of education and as a result have less concerns and negative information privacy perceptions. This is supported by the fact that the lowest education group in this study included noticeably more people with a low level of privacy concern and less people with a high level of privacy concern than the other education groups.

5.2 Practical implications

The results from this exploratory study indicate that the GDPR has not yet fully achieved its goals at this time. At least not from a consumers' perspective, that is. The results paint a somewhat negative and worrisome picture of how consumers view the current (information) privacy landscape and the role of the GDPR in it. Such negative views may have quite far-reaching consequences, as they can affect consumers' attitudes and behaviors in multiple ways. For example, some consumers may refrain from transacting or connecting and establishing any kind of (customer)relationship with organizations online. Others may simply refuse to engage in any type of activity online all together. Negative views of information privacy and the effectiveness of the GDPR in particular may perhaps also lead to a lack of trust or faith in the government, or the EU specifically. More research is required to determine exactly what effects these kind of (negative) privacy experiences and perceptions have.

In any case, those in business (and other organizations) have a clear interest in consumers' information privacy perceptions and would do well to take them seriously. More positive privacy perceptions could potentially greatly benefit them. For example, previous research has shown that companies' privacy practices have an effect on people's willingness to share information (e.g., Leon et al., 2013), which, considering the importance of data

(especially first party data these days), is important. However, fostering positive privacy perceptions may not always be easy. Changing policies and practices may be done relatively quickly but changing perceptions of those policies and practices may take a long time. Communication here is pivotal. Based on this study's findings that privacy perceptions are affected by individual characteristics, companies will need to carefully consider who they are targeting and communicating and adjust their privacy communication strategies accordingly.

This study's findings also particularly highlight how impactful privacy concerns still are. Reducing these concerns should be a priority for all those involved with the GDPR and its execution and enforcement, including, for example, legislators, governmental authorities and organizations, and businesses. This is not an easy task, however, as consumers have proven themselves to be hard to convince. For example, websites have tried to address concerns by creating more informative privacy policies (Malaga, 2014). However, studies have found that website visitors hardly ever click to read these privacy policies (e.g., Malaga, 2014). As stated in a previous study, "the disconnect between users' stated privacy concerns and their willingness to read privacy policies [and thus make an effort to inform themselves] requires a new approach to informing users about the privacy practices of the Websites they visit" (Malaga, 2014, p. 98). Essentially, businesses and other relevant parties need to get creative with their privacy communication strategies.

Another potential way to positivize consumers' information privacy perceptions is to increase their knowledge and understanding of the GDPR and the rights provided by it. This study's results suggest that a large majority of Dutch consumers is aware of the GDPR, but that most only have some knowledge and a somewhat limited understanding of its content. These findings are in line with a previous study that was also conducted using a Dutch sample (Strycharz et al., 2020). Increasing consumers' knowledge and understanding of the content of the regulation could help make their perceptions of information privacy more positive. Perhaps if more consumers were aware of all the rights afforded to them by the GDPR they would perceive and experience more control. It could also help clear up any misconceptions people might still have regarding their information privacy. As noted by Strycharz et al. (2020), "while experts would agree that some of the frustrations [about the GDPR] identified in this study are often unwarranted, this is not clear to the general public" (p. 420-421) and "these frustrations are in fact a clear signal that there is still much to be done on informing the public" (p. 421). The media in particular may have an important role in this (Strycharz et al., 2020). In

any case, improving communications is a key task for all parties involved. Despite being slightly dissatisfied with the GDPR in its current form, consumers do consider the GDPR to be an important law. Any efforts made to improve the law or knowledge about it will therefore likely be appreciated.

5.3 Limitations and future research

As any study, this study also has its limitations that should be considered. These limitations in turn lead to suggestions for future research. First, this study could have benefitted from a different sampling method. The sampling method used produced a sample that was not entirely optimal. Building a convenience sample via an online recruitment platform has clear benefits (as discussed previously) but it also has drawbacks. For example, the sample used in this study is not representative of the entire target population, which limits the generalizability of the findings. Not all age groups are represented equally (the sample is relatively young), making it more difficult to draw a comparison between these groups. In the same vein, a large majority of respondents had a high level of internet skills and self-efficacy, meaning that those with a low level of skills and self-efficacy were not well represented. For future research, researchers should consider using probability sampling (rather than nonprobability sampling, as was the case in this study) to recruit a representative sample.

Another limitation of this study is that data were only collected *after* the implementation of the GDPR and thus did not include any longitudinal or repeated measures data. This has made it difficult to draw any definite conclusions about the difference (if any) between consumers' perceptions and experiences pre- and post-GDPR. The findings presented in this study therefore only provide an indication of how this difference is perceived and experienced. Although it may be unlikely that future studies will be able to include data that was collected pre-GDPR, it could also be valuable to focus on two time points in the post-GDPR era. The GDPR and the privacy landscape will likely only continue to evolve over the next years, so measuring information privacy perceptions and experiences, say, five years apart could still produce interesting findings and highlight certain trends or patterns.

There is another limitation concerning the research method of this study. An online survey consisting (almost entirely) of closed-ended questions was used to measure consumers' information privacy perceptions and experiences. Although there are many advantages to this type of research method, there are also some disadvantages. Most notably,

in a survey such as the one used in this study, it is difficult to pursue interesting side-tracks, ask relevant follow-up questions, and allow respondents to elaborate on their answer. As a result, the 'why' behind respondents' answers may be left unexplained. There are other research methods that can be used to produce more detailed and nuanced findings. Future studies on this topic could benefit from using other methods, such as interviews or focus groups. Such studies could then, for example, focus on different types of privacy communication strategies and examine why some of these may be considered effective while others are not. In any case, there are still many topics left for future studies to explore that would contribute to (consumers' side of) the privacy literature.

5.4 Conclusion

Improving information transparency, control and security are three of the GDPR's key goals. An important question is if, from a consumer's perspective, these goals have been achieved. The purpose of this study was therefore to explore Dutch consumers' online experiences with and perceptions of information transparency, control, and security in the post-GDPR era. The results indicate that consumers are generally not (yet) impressed. It appears that in the perception of Dutch consumers, websites still are not transparent enough about the use and processing of data, consumers still do not have sufficient control over data provided to and collected by websites, and websites still do not adequately protect and secure data. What is more, it seems that these consumers have not experienced a significant improvement in information transparency, control, and security since the implementation of the GDPR in May 2018. A notable finding is that certain individual characteristics (gender, age, educational level, privacy concern, internet skills, and internet self-efficacy) appear to affect consumers' information privacy perceptions and experiences, albeit to varying extents. Privacy concern in particular seems to have the most noticeable effect. Overall, this study's findings suggest that the GDPR's goals have not yet been achieved, at least not in the eyes of consumers.

References

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., & Bearth, A. (2021). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour*, 1-12.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Akhter, S. H. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, *31*(2), 118-125.

Albert, B., Tullis, T., & Tedesco, D. (2010). *Beyond the Usability Lab: Conducting Large-scale Online User Experience Studies*. Morgan Kaufman.

Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, *2*, 287-289.

Allen, D. W., Berg, A., Berg, C., Markey-Towler, B., & Potts, J. (2019). Some economic consequences of the GDPR*, Economics Bulletin*, *39*(2), 785-797.

Almeida, F., & Monteiro, J. A. (2021). Exploring the Effects of GDPR on the User Experience. *Journal of Information Systems Engineering and Management*, *6*(3), em0140.

Article 29 Data Protection Working Party. 2018. "Guidelines on Transparency under Regulation 2016/679." 17/EN, WP260 rev.01 https://ec.europa.eu/newsroom/article29/redirection/document/51025

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Bauer, P. C., Gerdon, F., Keusch, F., Kreuter, F., & Vannette, D. (2021). Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Information, Communication & Society*, 1-21.

Blank, G., & Dutton, W. H. (2012). Age and trust in the Internet: The centrality of experience and attitudes toward technology in Britain. *Social Science Computer Review*, *30*(2), 135-151.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261-1278.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368.

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13-19.

Cumbley, R., & Church, P. (2013). Is "big data" creepy?. *Computer Law & Security Review*, *29*(5), 601-609.

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019, March). Measuring cookies and web privacy in a post-gdpr world. In *International Conference on Passive and Active Network Measurement* (pp. 258-270). Springer, Cham.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings of the 2019 Symposium on Network and Distributed System Security* (NDSS '19). Internet Society, San Diego, USA.

Deloitte. (2018). "A New Era for Privacy: GDPR Six Months On." https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7-29.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Duan, Y., Ge, Y., & Feng, Y. (2020). Pricing and personal data collection strategies of online platforms in the face of privacy concerns. *Electronic Commerce Research*, 1-21.

European Commission. (2019). “Special Eurobarometer 487a – March 2019: The General Data Protection Regulation.” Kantar Public [producer]. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=69701

European Union. (2016). “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.” (*General Data Protection Regulation*), OJ L 119. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the association for information Systems*, *17*(27).

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online?. *Telematics and Informatics*, *65*, 101717.

Foscht, T., Lin, Y., & Eisingerich, A. B. (2018). Blinds up or down? The influence of transparency, future orientation, and CSR on sustainable and responsible behavior. *European Journal of Marketing, 52*(3/4), 476-498.

Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, *16*(3), 349-391.

Gáti, M., & Simay, A. E. (2020). Perception of Privacy in the light of GDPR. In *Proceedings of the European Marketing Academy*, 11th, (85181).

GDPR Enforcement Tracker. (n.d.). *Statistics: Fines by type of violation*. Enforcement Tracker. https://www.enforcementtracker.com/?insights

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703-705.

Hargittai, E., & Litt, E. (2013). New strategies for employment? internet skills and online privacy practices during people's job search. *IEEE security & privacy*, *11*(3), 38-45.

Hauff, S., Dytynko, O., & Veit, D. (2017, January). The influence of privacy dispositions on perceptions of information transparency and personalization preferences. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 5006-5015.

Hauk, N., Hüffmeier, J., & Krumm, S. (2018). Ready to be a silver surfer? A meta-analysis on the relationship between chronological age and technology acceptance. *Computers in Human Behavior*, *84*, 304-319.

Holland, D., Krause, A., Provencher, J., & Seltzer, T. (2018). Transparency tested: The influence of message features on public perceptions of organizational transparency. *Public Relations Review*, *44*(2), 256-264.

Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, *64*(5), 923-938.

International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC Standard No. 27000). Retrieved from https://www.iso.org/standard/73906.html

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)* (pp. 39-52).

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1).

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)*, *15*(4), 1-42.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, *24*(4), 13-45.

Kim, M., Oh, J., & Kim, B. (2021). Experience of digital music services and digital self-efficacy among older adults: Enjoyment and anxiety as mediators. *Technology in Society*, *67*, 101773.

Lee, W. Y., Tan, C. S., & Siah, P. C. (2017). The role of online privacy concern as a mediator between internet self-efficacy and online technical protection privacy behavior. *Sains Humanika*, *9*(3-2), 37-43.

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., ... & Cranor, L. F. (2013, July). What matters to users? Factors that affect users' willingness to share information with online advertisers. In *Proceedings of theNninth Symposium on Usable Privacy and Security* (pp. 1-12).

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

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(28).

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, *16*(3), 251-270.

Malaga, R. A. (2014). Do web privacy policies still matter?. *Journal of Management Information and Decision Sciences*, *17*(1), 95-99.

Mohr, H., & Walter, Z. (2019). Formation of consumers' perceived information security: Examining the transfer of trust in online retailers. *Information Systems Frontiers*, *21*(6), 1231-1250.

Momen, N., Hatamian, M., & Fritsch, L. (2019). Did app privacy improve after the GDPR?. *IEEE Security & Privacy*, *17*(6), 10-20.

Morrissey, S. (2016). Take notice! The legal and commercial impact of the General Data Protection Regulation's rules on privacy notices. *Journal of Data Protection & Privacy*, *1*(1), 46-52.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642-660.

Palan, S., & Schitter, C. (2018). Prolific. ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, *17*, 22-27.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, *70*, 153-163.

Peer, E. P., Rothschild, D., Gordon, A., Evernden, Z., & Damer, E. (2021). Data quality of platforms and panels for online behavioral research. *Behavior Research Methods*, 1-20.

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Crespo, B. G. N., ... & Zorzino, G. G. (2019, August). DEFeND architecture: a privacy by design platform for GDPR compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 78-93). Springer, Cham.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., & Hofacker, C. F. (2010). Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal of Electronic Commerce*, *14*(3), 63-91.

Presthus, W., & Sørum, H. (2019). Consumer perspectives on information privacy following the implementation of the GDPR. *International Journal of Information Systems and Project Management*, *7*(3), 19-34.

SANS Institute. N.d. *Information Security Resources*. https://www.sans.org/information-security/

Schnackenberg, A. K., Tomlinson, E., & Coen, C. (2021). The dimensional structure of transparency: a construct validation of transparency as disclosure, clarity, and accuracy in organizations. *Human Relations*, *74*(10), 1628-1660.

Schudy, S., & Utikal, V. (2017). 'You must not know about me'—On the willingness to share personal data. *Journal of Economic Behavior & Organization*, *141*, 1-13.

Sørensen, J., & Kosta, S. (2019, May). Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites. In *Proceedings of the 2019 The World Wide Web Conference* (pp. 1590-1600).

Strycharz, J., Ausloos, J., & Helberger, N. (2020). Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. *European Data Protection Law Review*, *6*, 407.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in human behavior*, *29*(3), 821-826.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic commerce research*, *9*(3), 203-223.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1-12.

Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2020, October). Measuring the impact of the gdpr on data sharing in ad networks. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (pp. 222-235).

van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, *1*(2), 1-11.

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, *42*(1), 91-107.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing*, *80*(6), 97-121.

Wiles, Jackie. (2021, July 1). *Marketers Are Under a Digital Ad Siege and Must Now Convince Customers to Share Data*. Gartner. https://www.gartner.com/en/marketing/insights/articles/marketers-are-under-a-digital-ad-siege-and-must-now-convince-customers-to-share-data

Windiarti, S., Djajadikerta, H., & Setiawan, A. (2020). The Effect of Information Privacy Concern, Privacy Policy on Online Purchase Intention on Students in Bandung. *Psychology and Education Journal*, *57*(9), 5140-5145.

Wolford, Ben. (n.d.). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of computer-mediated communication*, *10*(3), JCMC1034.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. In *Proceedings of the 28th Annual International Conference on Information Systems (ICIS).* Montréal, Canada.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1), 1-20.

Appendix 1: Survey

Opening statement	Beste deelnemer, Hartelijk dank voor uw deelname aan dit onderzoek. Het doel van dit onderzoek is om inzicht te krijgen in hoe Nederlandse consumenten hun informatie privacy op het internet ervaren. In deze survey worden verschillende vragen gesteld over uw online privacy beleving. Het invullen van de survey zal ongeveer 6 minuten duren. Uw deelname aan dit onderzoek is volledig anoniem. Uw antwoorden zullen uitsluitend voor dit onderzoek gebruikt worden en vertrouwelijk behandeld en verwerkt worden. U kunt op ieder moment uw deelname aan dit onderzoek beëindigen en uw toestemming voor het gebruik van uw antwoorden intrekken. Door verder te gaan geeft u aan bovenstaande informatie begrepen te hebben en deel te willen nemen aan dit onderzoek en geeft u toestemming voor de verwerking van uw (geanonimiseerde) antwoorden. O Ik ga akkoord O Ik ga niet akkoord
GDPR awareness	Heeft u wel eens gehoord van de Algemene Verordening Gegevensbescherming (AVG)? *(Of in het Engels: General Data Protection Regulation (GDPR))?* O Ja O Nee
GDPR knowledge	In hoeverre bent u bekend met de inhoud van de Algemene Verordening Gegevensbescherming (AVG) (*GDPR*)? O Ik ben niet bekend met de inhoud van de AVG O Ik ben enigszins bekend met de inhoud van de AVG O Ik ben goed bekend met de inhoud van de AVG
GDPR understanding	In hoeverre begrijpt u de inhoud van de Algemene Verordening Gegevensbescherming (AVG) (*GDPR*)? O Ik begrijp de inhoud van de AVG niet O Ik begrijp de inhoud van de AVG enigszins O Ik begrijp de inhoud van de AVG goed

Brief explanation of the GDPR *Note: This text is only shown to those who indicated (above) not to have heard of the GDPR, not to have knowledge of its content, or not to understand its content.*	Voordat u doorgaat naar de volgende vragen kunt u hieronder een korte beschrijving van de AVG (*GDPR*) lezen. *[Button]*: Beschrijving AVG De AVG is een Europese privacywet die sinds 25 mei 2018 van toepassing is in de hele Europese Unie (EU). Het voornaamste doel van deze privacywetgeving is het beter beschermen van 'natuurlijke personen' (ofwel, elk individu dat in juridische zin rechten en verplichtingen heeft) als het gaat om de verwerking van hun persoonsgegevens. In de wet liggen de belangrijkste regels voor de verwerking van persoonsgegevens en de rechten van natuurlijke personen met betrekking tot deze verwerking vastgelegd. Centraal in de wet staan het afdwingen van meer transparantie over de verwerking van persoonsgegevens, het bieden van meer controle voor personen over deze verwerking van hun persoonsgegevens en het garanderen van meer veiligheid rondom de verwerking van deze gegevens.
Instructions	Hieronder ziet u een aantal uitspraken. Deze uitspraken hebben betrekking op uw privacy ervaring op het internet. Geef aan in hoeverre u het eens bent met elke uitspraak. Er zijn geen goede of foute antwoorden; het gaat hier om uw algemene ervaring en persoonlijke beleving.
Information transparency	Websites zijn transparant over welke informatie zij over mij verzamelen. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Websites zijn transparant over waarom of met welk doel zij informatie over mij verzamelen. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Websites zijn transparant over hoe lang zij mijn informatie bewaren.

	O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————— Websites zijn transparant over hoe zij mijn informatie gebruiken. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————— Websites zijn transparant over de rechten die ik heb met betrekking tot de verwerking van mijn informatie. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Comparison pre-GDPR information transparency	In mijn beleving zijn websites transparanter over de verzameling en verwerking van informatie sinds de AVG van toepassing is (mei 2018). O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Information control	Ik heb controle over de hoeveelheid informatie die websites over mij verzamelen. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*

	——————————————————————————— Ik heb controle over hoe websites mijn informatie gebruiken. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————————— Ik heb controle over wie er toegang heeft tot mijn informatie. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————————— Ik heb controle over de informatie die ik aan websites verstrek (bijvoorbeeld doordat ik deze informatie kan corrigeren, veranderen of verwijderen). O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————————— Mijn informatie staat op plekken waar ik geen controle over heb (bijvoorbeeld in databanken van andere bedrijven). O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Comparison pre-GDPR information control	In mijn beleving heb ik meer controle over mijn informatie sinds de AVG van toepassing is (mei 2018). O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens

	O Helemaal mee eens *[Likert scale]*
Information security	Websites nemen hun verantwoordelijkheid voor het beschermen van mijn informatie serieus. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Websites beschermen de integriteit van mijn informatie. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Websites beschermen mijn informatie tegen misbruik. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Websites delen mijn informatie niet met andere partijen. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ———————————————————————————— Mijn informatie wordt niet bekeken, opgeslagen of gemanipuleerd door onbevoegde partijen. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens

	O Helemaal mee eens *[Likert scale]*
Comparison pre-GDPR information security	In mijn beleving wordt mijn informatie beter beschermd sinds de AVG van toepassing is (mei 2018). O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Instructions	Hieronder ziet u een aantal uitspraken. Deze uitspraken gaan over de AVG. Geef aan in hoeverre u het eens bent met elke uitspraak. Er zijn geen goede of foute antwoorden; het gaat hier om uw algemene ervaring en persoonlijke beleving.
GDPR impact	De AVG heeft mijn informatie privacy verbeterd. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
GDPR satisfaction	Ik ben tevreden met de AVG in huidige vorm. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
GDPR importance	De AVG is een belangrijke wet. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Instructions	Hieronder ziet u een vraag over uw privacy zorgen. Kies het antwoord dat het beste bij uw algemene beleving past.

Privacy concern	Hoeveel zorgen maakt u zich over uw privacy op het internet? O Helemaal geen zorgen O Weinig zorgen O Enigszins zorgen O Veel zorgen O Zeer veel zorgen
Instructions	Hieronder ziet u een aantal uitspraken. Deze uitspraken gaan over uw vermogen om het internet te gebruiken (bijvoorbeeld het kunnen zoeken, verwerken en evalueren van informatie op het internet). Geef aan in hoeverre u het eens bent met elke uitspraak. Er zijn geen goede of foute antwoorden; het gaat hier om uw eigen perceptie van uw vaardigheden.
Internet skills	Ik heb sterke internetvaardigheden. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Internet self-efficacy	Ik leer gemakkelijk nieuwe internetvaardigheden. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————————— Ik ben goed in staat het internet te gebruiken voor verschillende taken of activiteiten. O Helemaal mee oneens O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]* ——————————————————————————— Ik kan problemen op het internet zelf oplossen. O Helemaal mee oneens

	O Mee oneens O Neutraal O Mee eens O Helemaal mee eens *[Likert scale]*
Gender	Wat is uw geslacht? O Man O Vrouw O Anders O Zeg ik liever niet
Age	Wat is uw leeftijd? _____
Educational level	Wat is uw opleidingsniveau (hoogste afgesloten niveau)? O Geen O Middelbare school O MBO O HBO O WO bachelordiploma O WO masterdiploma O Doctoraatsdiploma O Anders
Closing statement	Hartelijk dank voor het deelnemen aan dit onderzoek. Heeft u opmerkingen of vragen over (uw deelname aan) dit onderzoek? Dan kunt u een mail sturen naar: [*email address*] Klik nog eenmaal op het onderstaande pijltje om automatisch teruggeleid te worden naar Prolific en uw inzending te registreren.

Appendix 2: Survey constructs and items

Concept	Original items	(Adapted) items used in survey
GDPR awareness	N/A	1. Heeft u wel eens gehoord van de Algemene Verordening Gegevensbescherming (AVG)? *(Of in het Engels: General Data Protection Regulation (GDPR))?*
GDPR knowledge	N/A	1. In hoeverre bent u bekend met de inhoud van de Algemene Verordening Gegevensbescherming (AVG) (*GDPR*)?
GDPR understanding	N/A	1. In hoeverre begrijpt u de inhoud van de Algemene Verordening Gegevensbescherming (AVG) (*GDPR*)?
Information transparency	1. Importance of whether a company will allow me to find out what information about me they keep in their databases. 2. Importance of whether a site tells me how long they will retain information they collect from me. 3. Importance of the purpose for which the site wants to collect info from me. 4. Importance of whether a site is going to use the information they collect from me in a way that will identify me. (Awad & Krishnan, 2006)	1. Websites zijn transparant over welke informatie zij over mij verzamelen. 2. Websites zijn transparant over waarom of met welk doel zij informatie over mij verzamelen. 3. Websites zijn transparant over hoe lang zij mijn informatie bewaren. 4. Websites zijn transparant over hoe zij mijn informatie gebruiken. 5. Websites zijn transparant over de rechten die ik heb met betrekking tot de verwerking van mijn informatie.
Comparison pre-GDPR information transparency	N/A	1. In mijn beleving zijn websites transparanter over de verzameling en verwerking van informatie sinds de AVG van toepassing is (mei 2018).

Information control	1. How much control do you feel you have over the amount of your personal information collected by the company? 2. How much control do you feel you have over who can get access to your personal information? 3. How much control do you feel you have over how your personal information is being used by the company? (Xu, 2007) 1. How much control do you feel you have over the information you provide online, e.g. the ability to correct, change or delete this information? (European Commission, 2019) 1. To what extent do you find that your personal information exists in places that you do not have control over? (E.g., information stored in databases of different businesses) (Presthus & Sørum, 2019)	1. Ik heb controle over de hoeveelheid informatie die websites over mij verzamelen. 2. Ik heb controle over hoe websites mijn informatie gebruiken. 3. Ik heb controle over wie er toegang heeft tot mijn informatie. 4. Ik heb controle over de informatie die ik aan websites verstrek (bijvoorbeeld doordat ik deze informatie kan corrigeren, veranderen of verwijderen). 5. Mijn informatie staat op plekken waar ik geen controle over heb (bijvoorbeeld in databanken van andere bedrijven).
Comparison pre-GDPR information control	N/A	1. In mijn beleving heb ik meer controle over mijn informatie sinds de AVG van toepassing is (mei 2018).
Information security	1. The degree of confidence that inappropriate parties would neither view nor store consumer information.	1. Websites nemen hun verantwoordelijkheid voor het beschermen van mijn informatie serieus.

	2. The degree of confidence that the retailer will not expose consumer information to others. 3. Belief that inappropriate parties will not manipulate consumer information during a transaction. (Chellappa & Pavlou, 2002)	2. Websites beschermen de integriteit van mijn informatie. 3. Websites beschermen mijn informatie tegen misbruik. 4. Websites delen mijn informatie niet met andere partijen. 5. Mijn informatie wordt niet bekeken, opgeslagen of gemanipuleerd door onbevoegde partijen.
Comparison pre-GDPR information security	N/A	1. In mijn beleving wordt mijn informatie beter beschermd sinds de AVG van toepassing is (mei 2018).
GDPR impact	N/A	1. De AVG heeft mijn informatie privacy verbeterd.
GDPR satisfaction	N/A	1. Ik ben tevreden met de AVG in huidige vorm.
GDPR importance	N/A	1. De AVG is een belangrijke wet.
Privacy concern	N/A	1. Hoeveel zorgen maakt u zich over uw privacy op het internet?
Internet skills	N/A	1. Ik heb sterke internetvaardigheden.
Internet self-efficacy	1. I think I can easily learn how to use digital devices. 2. I believe I can use digital devices well. 3. I can solve problems with digital devices by myself. (Kim et al., 2021)	1. Ik leer gemakkelijk nieuwe internetvaardigheden. 2. Ik ben goed in staat het internet te gebruiken voor verschillende taken of activiteiten. 3. Ik kan problemen op het internet zelf oplossen.
Gender	N/A	1. Wat is uw geslacht?
Age	N/A	1. Wat is uw leeftijd?
Educational level	N/A	1. Wat is uw opleidingsniveau (hoogste afgesloten niveau)?

Appendix 3: Factor analyses

Discriminant validity: Iteration 1

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.852
Bartlett's Test of Sphericity	Approx. Chi-Square	2192.615
	df	153
	Sig.	0.000

	Communalities	
	Initial	Extraction
IT1	0.483	0.523
IT2	0.496	0.580
IT3	0.451	0.532
IT4	0.527	0.580
IT5	0.344	0.341
IC1	0.348	0.472
IC2	0.427	0.473
IC3	0.378	0.455
IC4	0.261	0.330
IC5 (rev.)	0.118	0.058
IS1	0.613	0.664
IS2	0.686	0.798
IS3	0.625	0.698
IS4	0.496	0.816
IS5	0.532	0.561
INT1	0.471	0.554
INT2	0.476	0.586
INT3	0.542	0.720

Extraction Method: Principal Axis Factoring.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation SS Load.
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %	Total
1	5.613	31.186	31.186	5.202	28.901	28.901	3.739
2	2.298	12.768	43.953	1.913	10.629	39.530	1.900
3	1.659	9.217	53.170	1.260	6.998	46.528	3.808
4	1.392	7.736	60.906	0.876	4.865	51.392	2.909
5	1.004	5.579	66.485	0.490	2.720	54.113	2.399
6	0.784	4.358	70.843				
7	0.676	3.758	74.601				
8	0.655	3.642	78.242				
9	0.605	3.362	81.604				
10	0.567	3.149	84.753				
11	0.463	2.573	87.326				
12	0.432	2.401	89.727				
13	0.383	2.125	91.852				
14	0.368	2.042	93.895				
15	0.312	1.734	95.628				
16	0.299	1.662	97.290				
17	0.272	1.512	98.802				
18	0.216	1.198	100.000				

Extraction Method: Principal Axis Factoring.

Pattern Matrix					
	Factor				
	1	2	3	4	5
IT1			0.645		
IT2			0.782		
IT3			0.757		
IT4			0.685		
IT5			0.516		
IC1				0.698	
IC2				0.555	
IC3				0.579	
IC4				0.543	
IC5 (rev.)					
IS1	0.765				
IS2	0.833				
IS3	0.760				
IS4					0.816
IS5	0.374				0.448
INT1		0.741			
INT2		0.766			
INT3		0.852			

Extraction method: Principal Axis Factoring

Rotation method: Oblimin with Kaiser Normalization

Note: small coefficients (< 0.3) were suppressed.

Factor Correlation Matrix					
Factor	1	2	3	4	5
1	1.000	0.045	0.437	0.389	0.430
2	0.045	1.000	0.021	-0.070	-0.108
3	0.437	0.021	1.000	0.418	0.320
4	0.389	-0.070	0.418	1.000	0.405
5	0.430	-0.108	0.320	0.405	1.000

Extraction method: Principal Axis Factoring

Rotation method: Oblimin with Kaiser Normalization

Discriminant validity: Iteration 2

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.857
Bartlett's Test of Sphericity	Approx. Chi-Square	2158,487
	df	136
	Sig.	0.000

	Communalities	
	Initial	Extraction
IT1	0.479	0.517
IT2	0.495	0.581
IT3	0.450	0.536
IT4	0.524	0.573
IT5	0.344	0.337
IC1	0.345	0.500
IC2	0.416	0.462
IC3	0.378	0.446
IC4	0.261	0.314
IS1	0.600	0.627
IS2	0.684	0.720
IS3	0.624	0.706
IS4	0.485	0.433
IS5	0.531	0.508
INT1	0.470	0.558
INT2	0.472	0.576
INT3	0.541	0.720

Extraction Method: Principal Axis Factoring.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation SS Load.
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %	Total
1	5.586	32.857	32.857	5.131	30.180	30.180	4.265
2	2.278	13.400	46.257	1.897	11.156	41.336	1.891
3	1.659	9.758	56.015	1.224	7.198	48.534	3.794
4	1.383	8.134	64.149	0.864	5.082	53.616	2.958
5	0.789	4.639	68.788				
6	0.679	3.996	72.784				
7	0.660	3.885	76.669				
8	0.613	3.603	80.272				
9	0.569	3.345	83.617				
10	0.468	2.753	86.370				
11	0.438	2.578	88.948				
12	0.394	2.316	91.264				
13	0.368	2.163	93.427				
14	0.323	1.901	95.328				
15	0.299	1.761	97.089				
16	0.277	1.627	98.716				
17	0.218	1.284	100.000				

Extraction Method: Principal Axis Factoring.

Pattern Matrix				
	Factor			
	1	2	3	4
IT1			-0.637	
IT2			-0.784	
IT3			-0.762	
IT4			-0.681	
IT5			-0.505	
IC1				0.742
IC2				0.545
IC3				0.578
IC4				0.515
IS1	0.797			
IS2	0.827			
IS3	0.880			
IS4	0.600			
IS5	0.658			
INT1		0.744		
INT2		0.755		
INT3		0.849		

Extraction method: Principal Axis Factoring

Rotation method: Oblimin with Kaiser Normalization

Note: small coefficients (< 0.3) were suppressed.

Factor Correlation Matrix				
Factor	1	2	3	4
1	1.000	0.019	-0.507	0.515
2	0.019	1.000	-0.054	-0.010
3	-0.507	-0.054	1.000	-0.413
4	0.515	-0.010	-0.413	1.000

Extraction method: Principal Axis Factoring

Rotation method: Oblimin with Kaiser Normalization

Convergent validity: Information transparency

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.835
Bartlett's Test of Sphericity	Approx. Chi-Square	516.163
	df	10
	Sig.	0.000

Communalities		
	Initial	Extraction
IT1	0.429	0.521
IT2	0.480	0.572
IT3	0.416	0.508
IT4	0.451	0.553
IT5	0.304	0.340

Extraction Method: Principal Axis Factoring.

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %
1	2.984	59.673	59.673	2.494	49.871	49.871
2	0.670	13.408	73.081			
3	0.530	10.596	83.677			
4	0.440	8.805	92.482			
5	0.376	7.518	100.000			

Extraction Method: Principal Axis Factoring.

Factor Matrix	
	Factor
	1
IT1	0.722
IT2	0.756
IT3	0.713
IT4	0.744
IT5	0.583

Extraction Method: Principal Axis Factoring.

Convergent validity: Information control

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.750
Bartlett's Test of Sphericity	Approx. Chi-Square	227.942
	df	6
	Sig.	0.000

Communalities		
	Initial	Extraction
IC1	0.279	0.412
IC2	0.305	0.448
IC3	0.297	0.442
IC4	0.220	0.309

Extraction Method: Principal Axis Factoring.

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %
1	2.202	55.059	55.059	1.611	40.273	40.273
2	0.681	17.036	72.095			
3	0.606	15.155	87.250			
4	0.510	12.750	100.000			

Extraction Method: Principal Axis Factoring.

Factor Matrix	
	Factor
	1
IC1	0.642
IC2	0.669
IC3	0.665
IC4	0.556

Extraction Method: Principal Axis Factoring.

Convergent validity: Information security

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.830
Bartlett's Test of Sphericity	Approx. Chi-Square	786.392
	df	10
	Sig.	0.000

Communalities		
	Initial	Extraction
IS1	0.585	0.625
IS2	0.647	0.698
IS3	0.593	0.675
IS4	0.456	0.437
IS5	0.504	0.513

Extraction Method: Principal Axis Factoring.

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %
1	3.346	66.912	66.912	2.949	58.972	58.972
2	0.715	14.306	81.218			
3	0.364	7.277	88.495			
4	0.330	6.594	95.089			
5	0.246	4.911	100.000			

Extraction Method: Principal Axis Factoring.

Factor Matrix	
	Factor
	1
IS1	0.791
IS2	0.835
IS3	0.821
IS4	0.661
IS5	0.717

Extraction Method: Principal Axis Factoring.

Convergent validity: Internet self-efficacy

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.713
Bartlett's Test of Sphericity	Approx. Chi-Square	331.280
	df	3
	Sig.	0.000

Communalities		
	Initial	Extraction
INT1	0.446	0.560
INT2	0.447	0.561
INT3	0.522	0.725

Extraction Method: Principal Axis Factoring.

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Var.	Cumul. %	Total	% of Var.	Cumul. %
1	2.225	74.166	74.166	1.847	61.561	61.561
2	0.440	14.666	88.832			
3	0.335	11.168	100.000			

Extraction Method: Principal Axis Factoring.

Factor Matrix	
	Factor
	1
INT1	0.749
INT2	0.749
INT3	0.851

Extraction Method: Principal Axis Factoring.

Appendix 4: Descriptive statistics

Descriptive statistics: Information transparency, control, and security

Variable	*M*	*SD*
Information transparency	2.34	0.75
Information control	2.28	0.7
Information security	2.4	0.73

Descriptive statistics: GDPR awareness, knowledge, and understanding.

Variable	*Answer categories*	*N*	*%*
GDPR awareness	Aware	261	87
	Not aware	39	13
	Total	300	100
GDPR knowledge	No knowledge	52	20
	Some knowledge	171	66
	Good knowledge	38	15
	Total	261	100 (87% of 300)
GDPR understanding	No understanding	5	2
	Some understanding	148	71
	Good understanding	56	27
	Total	209	100 (70% of 300)

Descriptive statistics: GDPR impact, satisfaction, and importance

Variable	*M*	*SD*
GDPR impact	3.35	0.8
GDPR satisfaction	2.88	0.84
GDPR importance	4.29	0.66

Descriptive statistics: Comparison information transparency, control, and security

Variable	*M*	*SD*
Comparison information transparency	3.41	0.98
Comparison information control	3.04	0.98
Comparison information security	3.03	0.95