International Journal of
Information Systems and Project Management
ISSN (print):2182-7796, ISSN (online):2182-7788, ISSN (cd-rom):2182-780X
Available online at ijispm.sciencesphere.org

Five years with the GDPR: an empirical study emphasising information privacy and the consumer

Wanda Presthus
Kristiania University College
Kirkegata 24-26, 0153 Oslo
Norway
wanda.presthus@kristiania.no

Hanne Sørum
Kristiania University College
Kirkegata 24-26, 0153 Oslo
Norway
hanne.sorum@kristiania.no

Abstract:
Consumers' privacy rights have been enshrined in law, long before information systems and the Internet was brought to life. In 2018, stricter regulations relating to information privacy came into force, named the General Data Protection Regulation (GDPR). Using elements of Roger's diffusion of innovations theory, we investigated the research question: How has five years of the GDPR influenced consumer's knowledge, attitude, and practice of their enhanced rights? We draw on empirical data collected in Norway through four online survey questionnaires over five years (N=1293). Quantitative (descriptive statistics) and qualitative analyses (manual cluster text mining) were performed to obtain a state-of-the-art mapping of insights on consumers and their information privacy. Our findings show that the respondents' answers remained similar over the years, and that the GDPR has not had a significant influence on the consumer. The respondents demonstrated a high degree of knowledge regarding both the regulation and technology, such as cookies. Their attitude was sceptical, as they valued their enhanced rights but questioned the feasibility. Regarding their practice, our findings reveal diversity. Some respondents took careful actions to protect their privacy, while most did not. The present paper should be interesting to both the industry (practitioners) and academia (researchers).

Keywords:
information privacy; General Data Protection Regulation (GDPR); consumers; diffusion of innovations theory; online survey.

DOI: 10.12821/ijispm120301

Manuscript received: 11 September 2023
Manuscript accepted: 26 February 2024

1. Introduction

With a combination of only three variables of data—postal code, birth date, and gender—what percentage of individuals did computer scientist Latanya Sweeney manage to identify? Answer: 87% [1]. Add to this the consumer's use of the internet, mobile phones, and the many other digital traces we leave in this high-tech society, and companies can feast on our personal data. On the positive side, for example, as consumers, we now get faster application processing at the bank, and better predictions of health issues [2]. However, there are also challenges. With the development of technology, more decisions are now made without the involvement of human actors. For example, a bank's machine algorithm can decide whether an applicant will get a mortgage. Such cases are not illegal, but consumers have the right to be informed if the decision was made automatically and without human involvement. A more questionable example, perhaps, is when the algorithm of a hotel chain matches your device's IP address with your country of resident and categorises it as wealthy or not. Residents of wealthy countries are shown higher prices for hotel rooms, a phenomenon called *price discrimination*.

Companies also know where we shop, what we are likely to buy in the future, and what our digital movements are like. Most people are probably not familiar with all the various digital traces they leave behind every day; but some individuals care more than others. However, there are laws and regulations to protect consumers so that their privacy is safeguarded in a fair and good way. In Norway, there have been strict rules related to privacy and the handling of personal data for many decades. Consumers' interests have been well looked after, and people usually do not think too much about this unless problems arise, such as the misuse of their personal data. In 2018, an even stricter regulation named the General Data Protection Regulation (GDPR) was enacted. The GDPR is a privacy law that affects all citizens who live in European Union (EU) or European Economic Area (EEA) countries and any company that does business with these citizens. A privacy law will normally address two parties: the consumer, who gets increased rights, and the company, who gets increased duties [1].

This study focuses on the consumer's increased rights [1] and the research question is: *How has five years of the GDPR influenced consumer's knowledge, attitude, and practice of their enhanced rights?* Drawing on our empirical data collected between 2018 and 2023, we offer a mapping of consumers' perspectives during these years. The aim is to explore how this regulation works in practice and how consumers are aware of and use their rights. We discuss our findings with the help of elements from the diffusion of innovations theory [3]. Thus, we contribute with mainly new insights to the industry, but also to academia due to our use of a well-known theory.

Our paper is divided into seven parts: In Section 2, we review relevant literature; in Section 3, we present our theoretical framework; and in Section 4, we describe the use of method and the data analysis performed in the present study. The findings are presented in Section 5, followed by a discussion in Section 6. The conclusion is provided in Section 7, along with suggestions for future research.

2. Related work of privacy and the GDPR in an information systems' context

The literature on privacy is extensive and interdisciplinary [4]. It includes definitions for philosophers, conceptual frameworks for academics, insights into the laws and regulations for legal professionals, business strategies for companies, and benefits and challenges for individuals, companies, and society. More recently, topics such as *algorithmic transparency* [5] and *responsible artificial intelligence* [6] have emerged.

The famous juridical definition of privacy as "*the right to be left alone*" was suggested in 1890 by lawyers Warren and Brandeis. As explained by Solove [7], the motivation behind this was the invention of a portable camera. Extant literature claims that we lack a common definition of privacy [8], however, in this study, we will focus on information privacy, which is a subset of privacy and often used in an information systems context [9].

Information systems are a young discipline [10], at least compared to privacy and jurisprudence. As suggested by Dahlbom, the evolution of information systems can be divided into four phases [11]:

> **Phase 1.** The first computing machines were automatic versions of the mechanical calculating machines used in offices and retail stores. The machines performed the same tasks as humans, only faster, cheaper, and more reliable.
>
> **Phase 2:** In the early 1960s, computers began to be used as information systems due to their capacity to handle large sets of data. Information systems were used by companies and government agencies to register and keep track of people, products, payments, and taxes.
>
> **Phase 3:** The personal computer became portable, and networks and client server technology were introduced in the late 1980s. This made it possible to distribute, sort, and cooperate with all the documents and spreadsheets produced in the PCs. Computer technology became a medium of communication for entertainment, education, news, and marketing.
>
> **Phase 4:** Today, we have witnessed the emergence of the Internet, infrastructures, interactive multimedia, cyberspace, networks, machine learning, artificial intelligence, and the Internet of Things.

From Dahlbom's [11] description of information systems, we note concepts such as *automatic*, *handling large sets of data*, and *keeping track of people*. Further, benefits such as *fast*, *cheap*, and *reliable* occur. A case from Norway illustrates the how fraud was revealed: The Driver and Vehicle Licensing Agency's database of people who had recently obtained their driver's licence was mapped with the social security office's database of people who also received welfare for being blind. Several matches were made [12].

Research has addressed the benefits and questionable consequences of using technology and analysing large amounts of data from multiple sources. Examples of benefits for the individual, organisation, and society include improved and tailored medical treatment, facilitated urban planning, catching more criminals, and thus creating a safer nation. These benefits also come with drawbacks such as *price discrimination*, tempting the consumer with targeted advertising, letting criminals know that you are away from home, and hacking companies' systems [2].

By browsing the Internet, a lot goes on behind the user's computer, and much is automated. For example, cookies are being traced, companies have an auction, and the highest bidder will place their ad on the user's screen [13]. Cookies have caught the attention of researchers considering the divide between EU/EAA citizens and non-EU/EAA citizens after the implementation of the GDPR. The GDPR rules of the former group are stricter, and EU/EAA users may experience a denial of access to, for example, US webpages [14].

The GDPR applies to any EU or EAA citizen. The GDPR is a central regulatory framework almost regardless of the industry or business sector [15]. The regulation replaced over 40 privacy laws in Europe, and one of the motivations behind the GDPR was the emergence of technology and analytical tools. The GDPR consists of 99 articles, 11 of which were found to influence how companies use information systems in particular [16]. For this study, the following articles apply:

> *Article 5: Principles relating to the processing of personal data*
> Consumers' personal data should be processed with fairness, lawfulness, and transparency and only collected for specified, legitimate, and explicit purposes.
>
> *Article 7: Conditions for consent*
> Consumers can withdraw their consent at any time and in an easy manner.
>
> *Article 15: Rights of access by the data subject*
> Consumers can obtain confirmation regarding whether personal data concerning them are being processed.

Article 17: Right to erasure ("right to be forgotten")
Consumers have the right to have their personal data erased from the organisation.

Article 20: Right to data portability
Consumers have the right to receive their personal data, and reuse them for their own purposes. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a secure way.

Article 22: Automated individual decision-making, including profiling
Consumers have the right not to be subject to a decision based solely on automated processing (without any human involvement).

Article 25: Data protection by design and by default
The organisation must ensure that only the consumers' personal data that are necessary for each specific purpose of the processing are processed.

The use of cookies is not directly mentioned in the 99 articles of the GDPR. The regulation (found here: https://gdpr-info.eu/) mentions cookies in recital number 30:

> *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".*

However, some researchers claim that other articles in the GDPR indirectly address how the owners of webpages use cookies, such as Article 6*: Lawfulness of processing* [17]. We also surmise that Articles 5 and 7, as listed above, are related to the use of cookies. The regulation poses challenges for organisations, and research shows that companies want to comply but struggle to understand their new duties [16, 18]. Failing to comply with the GDPR can result in sanctions from the country's data protection authority [19]. Another study by Dexe et al. [20] found that the translation of the GDPR wording differed in five countries. Companies struggle with the interpretation of the regulation, and the authors call for clarification from legislators.

If companies struggle to interpret the regulation, consumers most certainly will be puzzled. Before the GDPR, the privacy calculus model prevailed (see, e.g. Dinev et al. [21]), which involved people calculating which of their private data to give up in exchange for benefits when shopping online. Privacy in an online context has been a topic for many years, and several studies have explored consumers' concerns about the violation of their privacy, especially in e-commerce. Typically, consumers are concerned about misuse of personal information, monitoring, spam, hackers, viruses, and the risks associated with payment [8]. More recently, Momen et al. [22] investigated the effects of the GDPR on consumers' Android apps. Among others, the findings show that changes point to positive impacts of the implementation of GDPR regarding user's app behaviour and in user feedback. In general, the authors concluded that privacy in apps has moderately improved post-implementation of the new regulation. Previous studies [23] show that the GDPR has made progress in protecting user data. However, more progress is needed regarding giving users the right to edit and delete personal data. Recently, researchers have wondered whether consumers have any choice regarding their privacy, because they must give up personal data to exist in today's society [13, 24, 25].

3. Theoretical framing: the KAP model from Rogers' diffusion of innovations

In his well-known book on the diffusion of innovations, Roger's described a model called KAP: *knowledge, attitude, practice* [3, p. 176]. The author used cigarette smoking to exemplify KAP as follows: First, an individual needs to know that smoking is dangerous. Then, the smoker needs to want to give up smoking. Finally, the person must act and stop smoking, and remain a non-smoker.

In other words, there is a process: knowing → wanting → acting. The problem, as discussed by Rogers, is the *KAP gap*, which indicates the discrepancy between knowledge, attitude, and action. Knowing that fast food has many calories, and wanting to lose weight, an individual may still continue to eat hamburgers and deep-fried food. Sometimes, an individual may need a *cue-to-action* to change behaviour or adopt an innovation. A cue-to-action is *"... an event occurring at a time that crystallizes a favourable attitude into overt behavioural change"* [3, p. 176]. A cue-to-action may occur naturally; for example, in our context, a bank customer may experience being denied a mortgage, thus motivating the customer to exercise their *right to access* (Article 15). Another example can be triggered by rock stars, as discussed later in the article.

In the information privacy literature, the discrepancy between what people claim they do, and what they actually do is called the *privacy paradox* [26]. Consumers claim to care about their privacy, but their actions do not correspond. For example, they will willingly give up personal information to gain benefits, such as discounted prices, when shopping. Recently, the privacy paradox has been criticised, and some researchers, such as Knijnenburg et al. [24] and Solove [25], claim that consumers do not really have a choice.

In our study, *knowledge* refers to the information possessed by consumers, such as their awareness of information privacy and the GDPR. *Attitude* deals with the willingness to change one's behaviour. In our study, one example is choosing to care about one's privacy, or, as some do, simply give up the fight and hope for the best. *Practice* is about acting and making use of the enhanced rights offered by regulations such as the GDPR, including data portability, the right to be forgotten, insight, and rejecting cookies on websites. Our questionnaire and discussion were constructed based on the KAP concept [3] and is summarised in Table 1.

Table 1. Attributes regarding information privacy and the GDPR investigated in the present study.

Information privacy and the GDPR		
Knowledge	**Attitude**	**Practice**
Consumers must possess information about technology and be aware of their enhanced rights	Consumers must care about their privacy and be willing to change their behaviour, such as rejecting cookies on websites and start reading terms & conditions	Consumers must make use of the enhanced rights. The GDPR provides several articles: Article 15: right to insights Article 17: right to be forgotten Article 20: right to data portability Articles 5/6/7: consent

4. Methods

We drew on empirical data collected through four different online surveys. In this paper, we present our quantitative findings, in addition to a thorough qualitative analysis of the quotes from the respondents, to provide a richer and more descriptive picture of our findings. We start by presenting the most recent survey from 2023, followed by those from 2018 [27], 2019 [28], and 2020 [29].

4.1 Data collection

The survey from 2023 was designed by utilising the online tool *Nettskjema* (www.nettskjema.no). This tool was developed by the University of Oslo (Norway) and meets the requirements for privacy and research ethics. After the survey was designed using *Nettskjema*, a link (web address) was generated, and the respondents used the link to access the survey. Before data collection took place, we carried out a pilot test with four respondents. The purpose was to test that the questions were understandable; that there was a logical connection between question-and-answer alternatives; checking typographical errors; and that the link worked. We received a few comments that were implemented in the survey, mainly about improving the answer alternatives on some of the questions. This was useful and valuable feedback.

The data collection took place from February to the end of June 2023. Since privacy and the GDPR concern all people, we wanted answers from a broad target group. The link to the survey was therefore distributed through various channels. The link was posted on Facebook, sent to our contact network (private and work), and we recruited respondents who are students at a university in Norway. These students were from various fields of study and therefore had different backgrounds and interests. On the first page of the survey (start page), participants were informed of the topic of the survey, that participation was voluntary, and that all responses were anonymous. In addition, we included contact information for the research team. The survey was completed in June 2023 with 306 respondents.

By using the online tool for surveys *Nettskjema*, we only had access to respondents who filled in all the questions in the survey (and not those who dropped out before completing the questionnaire). Moreover, due to this method of posting a survey link on social media among networks and students who were physically present at school, we cannot report on the response rate. We closed the survey when we had a scientifically acceptable number of respondents, and we detected clear patterns in the responses.

The surveys from 2018, 2019, and 2020 were conducted using SurveyMonkey®. The main structures of the survey were similar. They all had an introduction consisting of a description of the topic, contact information of the research team, and information about research ethics, such as anonymity. All questionnaires contained questions that generated both qualitative and quantitative data. However, the surveys have been somewhat altered and improved based on the comments that we received in the open-ended questions. In the 2018 survey, 10 respondents stated that the survey was too long and cumbersome, with long sentences in our questions. They also claimed that the survey had either too many alternatives or that none of the alternatives suited them. We interpreted these comments as genuine interest in the topic. Based on this valuable feedback, we made some changes to our survey every year. For example, when we conducted the first explorative survey in 2018, the GDPR was yet to be implemented; thus, we had to provide descriptions of the articles in the survey questions. Over the years, the topic has become more known, and we have reduced the explanatory text in the questions.

Based on feedback from the previous participants, and pilot tests in 2023, we changed the last sentence "*What do you think about this*?" to "*Which answer option suits you best*?" to provide more flexibility to the participants. Moreover, it was necessary to change the verb tense from "I *may want to execute* this new right" prior to the implementation of the GDPR in 2018 to "I *have executed* this new right" in 2019 and onward. We acknowledge that altering the questions poses some challenges in comparing the results, but we will address this issue in the next sections.

4.2 Respondents

As mentioned above, we did not have a specific target group. Table 2 shows the detailed gender of all respondents between 2018 and 2023. We had a total of 1293 respondents, of which 652 were men, 633 were women, 2 indicated 'other', and 6 did not answer the gender question.

Table 2. Number of respondents in the four surveys conducted between 2018–2023.

	2018	**2019**	**2020**	**2023**
Men	137 (63.43%)	178 (54.43%)	166 (37.39%)	171 (55.9%)
Women	79 (36.57%)	146 (44.65%)	274 (61.71%)	134 (43.8%)
Other	-	-	1 (0.23%)	1 (0.30%)
Do not want to answer	-	3 (0.92%)	3 (0.68%)	-
SUM number of respondents	**216**	**327**	**444**	**306**

The distribution of the respondents for the survey conducted in 2023 is shown in Table 3.

Regarding the respondents who took part in the previous surveys, the following findings are highlighted: In 2018, more males participated in the survey (63%) than females (37%). Most of the respondents were 21–25 years old, followed by the 26–30-year-old group. In 2019, 54% of the respondents were men, and 45% were female. The rest did not want to give up their gender. Most respondents were 21–25 years old, followed by the 26–30-year-old group. In 2020, the typical respondent was female in the age group of 18–25 years. In all the surveys conducted, there was a dominance of younger people enrolled in a higher educational programme (typically a bachelor's degree).

Table 3. Overview of the respondent's characteristics in 2023.

Age	18–25 years: 148 (48.4%)
	26–30 years: 41 (13.4%)
	31–40 years: 37 (12.1%)
	41–50 years: 32 (10.5%)
	51–60 years: 34 (11.1%)
	Over 60 years: 14 (4.6%)
	Don't want to give up: 0
Level of education	Primary school: 0
	Upper secondary school: 22 (7.2%)
	Vocational school or equivalent: 20 (6.5%)
	Education at bachelor's level: 194 (63.4%)
	Master's level or higher: 68 (22.2%)
	Other: 2 (0.7%)
Main occupation	Income–generating work: 124 (40.5%)
	Student: 176 (57.5%)
	Other (for example, stay-at-home, retired): 6 (2%)

4.3 Data analysis

Our survey provided us with quantitative and qualitative data. Regarding the quantitative data, we first carried out descriptive analyses, looking for patterns and trends in the results. We used Microsoft Excel® to create tables and visual graphs. In this paper, we present descriptive data on how the answers were distributed on the measurement scale. This provided us with an understanding of how consumers viewed the GDPR over time.

In addition to quantitative data, our survey from 2023 included one open-ended question (see the Appendix), to which 36 respondents provided answers. The length of the answers was mostly one or two sentences, but some wrote a whole paragraph. Drawing on techniques for analysing qualitative data [30] we created a matrix in Microsoft Excel® and looked for clusters, or common topics, in the answers. The "search-and-mark-all" function in Microsoft Excel® allowed us to perform *stemming*, a text-mining term. Stemming is the process of reducing words to their roots. For example, stemmer, stemming, and stemmed are all from the root 'stem' [31]. We coded the most frequent words or topics and added up the occurrences. Due to the limited quantity of text, it was manageable to conduct the text analysis manually. The benefit of manual text analysis is that we can detect emotions, irony, and spelling errors.

As previously mentioned, our survey has been altered over the years. In 2018, we had six open-ended questions, and we received 69 answers in total. In 2019, we increased the open-ended questions to 11, and we received 160 answers. In 2020, we still had 11 open questions, and we received 101 answers in total. Typically, the respondents wrote one or two sentences, but a few wrote a small section. In summary, we obtained 366 different text answers from respondents from four surveys, as shown in Table 4.

Table 4. Number of qualitative comments in each of the four surveys conducted.

Survey year	2018	2019	2020	2023	**SUM**
Qualitative answers	69	160	101	36	**366**

4.4 Strengths and weaknesses of our method

The strengths of our method are that we have respondents of different ages and backgrounds, and we could repeat our survey multiple times and compare the results over time. A link to the survey was distributed in various networks, and the research team worked actively to get respondents who did not primarily reflect a given group in the society. Nevertheless, we acknowledge that most of our respondents were students in their twenties.

As mentioned, despite our pilot tests before collecting data, the survey had to be altered and improved over the years. For example, a few respondents in 2018 indicated that some questions were too leading, or, that there were not enough alternatives to choose from. In response to this, we included more open-ended questions in 2019 and 2020. Although we received more qualitative replies, we noted that there were many repetitive answers. In addition, some participants in

2019 claimed that the survey was too long and cumbersome. For these reasons, we only had one open-ended question at the end of the survey in 2023 (see the Appendix).

5. Findings

The following section is divided into two parts: Section 5.1 provides the quantitative findings, and Section 5.2 presents the qualitative findings from the open-ended questions in our study.

5.1 Quantitative findings

At the beginning of the survey, the respondents were asked questions about their knowledge of the GDPR. Table 5 shows how the answers are distributed, and Figure 1 shows a visual impression of the data in Table 5.

Table 5. Knowledge of the GDPR over the years (actual numbers in percentages).

	Knowledge of the GDPR			
	2018 (n = 216)	2019 (n = 327)	2020 (n = 444)	2023 (n = 306)
Yes, and I know what it means	46.76%	61.77%	26.13%	46.7%
Yes, I know a little, but not enough about what it means	26.39%	30.58%	26.80%	26.1%
Yes, but I do not know what it means	5.56%	3.06%	12.39%	8.8%
I have never heard of that	21.30%	4.59%	34.68%	18.3%

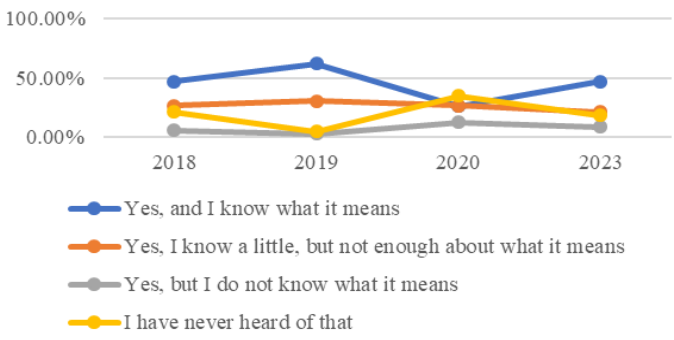


Fig. 1. Visualisation of the distribution of knowledge of the GDPR from 2018–2023.

Regarding the knowledge of the GDPR, there have been changes over the years, and most people had heard of the regulation and knew what it meant by 2019. This knowledge seemed to decline in 2020, but it increased in 2023. The number of respondents who had "never heard of the GDPR" was very few in 2018 and 2019, whereas in 2020, this represented approximately 35% of the respondents. In the survey from 2023, this number dropped to less than 20% among the respondents. Furthermore, the respondents were asked about their attitudes towards the GDPR and whether they were generally concerned as a consumer. The results are shown in Table 6 and a visual impression of the numbers is shown in Figure 2.

Table 6. Attitude of the GDPR over the years.

	Attitude of the GDPR			
	2018 (n = 220)	**2019 (n = 327)**	**2020 (n = 444)**	**2023 (n = 306)**
Not at all	1%	1%	2%	0.3%
Low	10%	12%	12%	11.1%
Medium	55%	56%	54%	50.7%
High	34%	31%	30%	37.9%
I do not know	1%	1%	3%	0

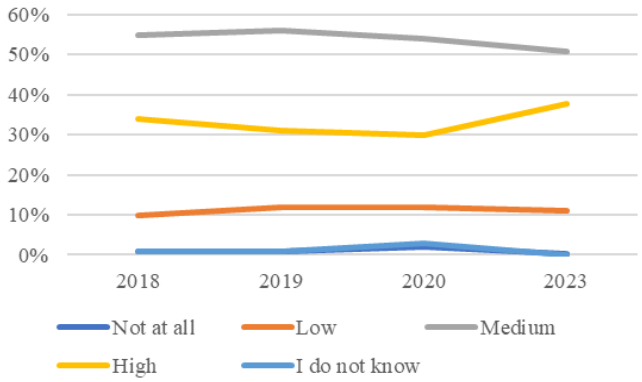


Fig. 2. Visualisation of the distribution on attitude pertaining to the GDPR from 2018–2023.

The findings show that the answers to this question have been relatively stable over the years, with one exception. We observe that the graph depicting high concern increased somewhat in 2023 (just below 40%).

In the following graphs we have omitted the results from 2018 due to the differences in the verb tenses in the questions, as explained earlier. We focus on comparing the actual practices of the respondents. However, we describe the results of the 2018 survey under each graph.

Our description of Data portability (Article 20) for the present study reads: Consumers have the right to receive their personal data and reuse it for their own purposes. They can move, copy, or transfer personal data easily from one IT environment to another in a secure way.

Regarding data portability, the analysis showed that the patters have been relatively stable from 2019-2023. However, inn 2023, even more respondents answered that they "might execute this right". The size of "I do not know" group had decreased.

In 2018 (prior to the implementation of the GDPR and not included in Figure 3), 17% of the 203 respondents believed they would make more use of the right to transfer personal data. More than half of the respondents (53%) stated that they might want to use the right, 20% indicated that they most likely would not, 3% did not care, and 7% did not know.

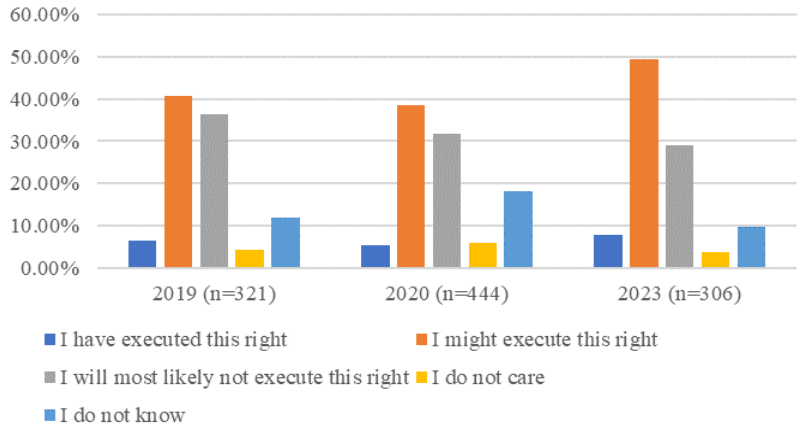


Fig. 3. Visualisation of answers pertaining to data portability from 2019–2023.

Our description of the Right to be forgotten/Erasure (Article 17) for the present study reads: Consumers have the right to have some of their personal data erased from the organisation.

Regarding the right to be forgotten, the answers were almost equal regarding distribution on the measurement scale. Over the years, most respondents answered that they might execute this right. Few responded that they did not care. Moreover, the findings show that surprisingly few respondents had executed this right over the years (above 10%).

Numbers from 2018 (not included in Figure 4) showed that 39% indicated that they would make use of this right, while 49% stated that they might take advantage of this right. Moreover, 9% answered that it was a right they most likely would not make use of, 1% of the respondents did not care, and 2% did not know.

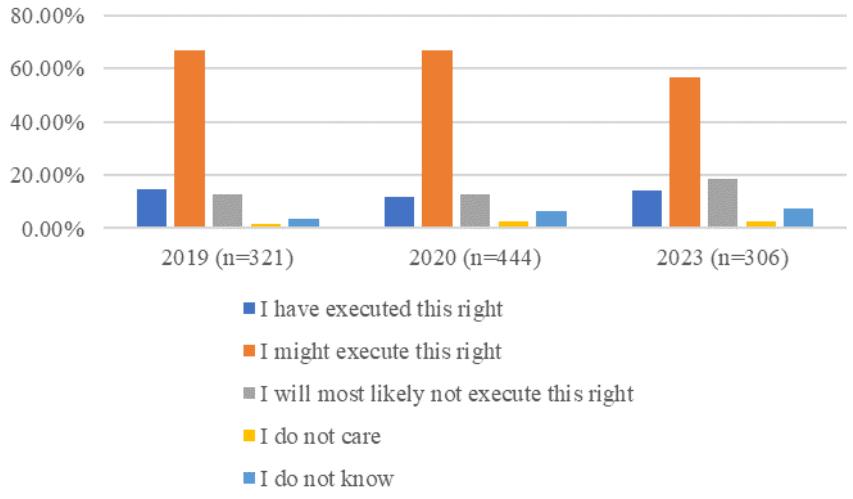


Fig. 4. Visualisation of answers pertaining to right to be forgotten from 2019–2023.

Our description of Right to access (Article 15) for the present study reads: Consumers can obtain confirmation of whether or not personal data concerning them are being processed. They have the right to insight and to rectify potential wrong information.

Regarding the right to access, there was a small variation in relation to what the respondents answered over the years. In 2020, 6% answered that they had exercised this right, and in 2019 and 2023, the affirmative response was also below 10%. Most of the respondents said that they would possibly make use of this right to access personal data. Very few of the respondents said they did not care.

According to the 2018 survey (not included in Figure 5), 17% of the respondents answered that they had wanted this opportunity for a long time, 9% indicated that it did not matter, 20% believed they would surely make use of it, and 53% stated that they could possibly use it. Furthermore, 13% stated that this was most likely a right they would not exercise, and 39% believed that this would create challenges for many companies.

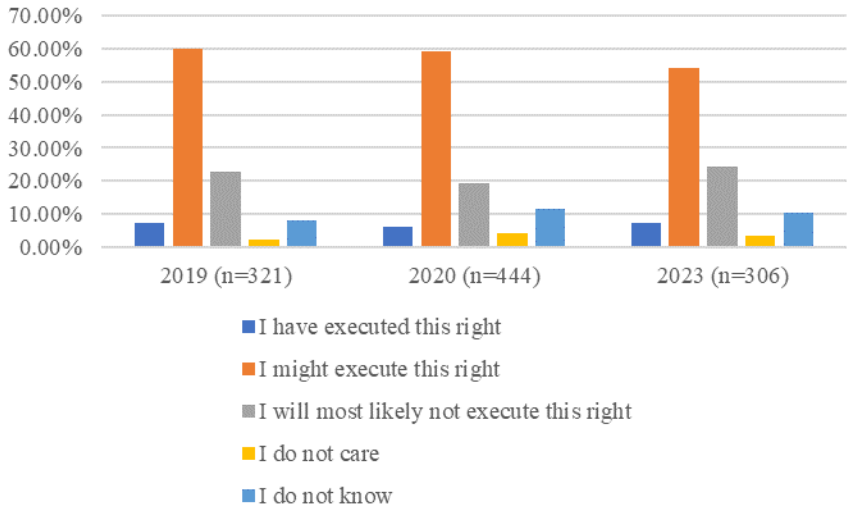


Fig. 5. Visualisation of answers pertaining to right to access from 2019–2023.

Our description of Cookies (Articles 5/6/7) for the present study reads: Consumers' personal data shall be processed with fairness, lawfulness, and transparency and only collected for specified, legitimate, and explicit purposes.

We need to mention that the numbers (percentage) in Figure 6 are more than 100% for some answers, as it was possible to check off more than one answer option in this question. However, the findings showed that the respondents generally experienced that companies had become better at informing about cookies after the GDPR was introduced. The responses from 2023 (compared to 2019 and 2020) show a clear increase in users' perceived opportunities to opt out of cookies or whether they want to accept all of them. At the same time, the findings also show that there is uncertainty associated with companies' use of cookies. A few people answered that they did not care and/or know what cookies were.

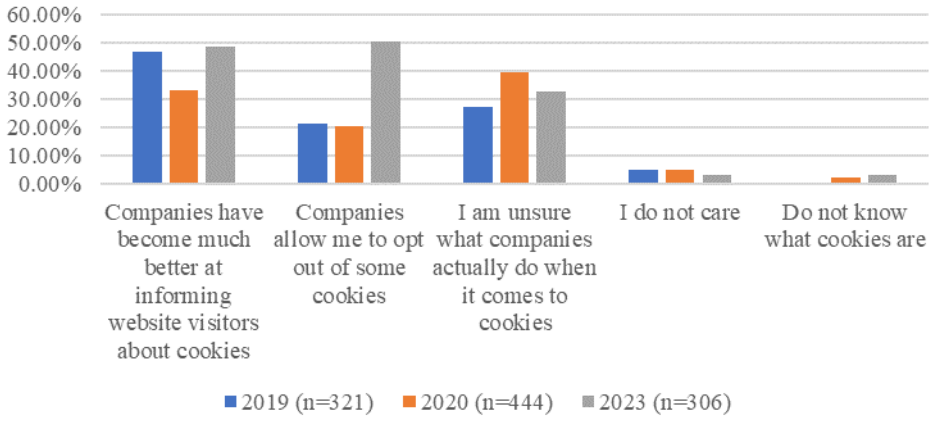


Fig. 6. Visualisation of answers pertaining to cookies from 2019–2023.

Regarding the 2018 data (not included in Figure 6), 63% of the respondents were positive about the expected enhanced rights enforced by the GDPR regarding cookies, 38% had no faith that all businesses would follow the new regulation, 29% were unsure of how this would work in practice, 7% did not care, and 2% of the respondents did not know what cookies were. Table 7 summarises the trends and patterns that emerged from the quantitative findings.

Table 7. An overview of the findings of the present study.

	2018	2019	2020	2023
Knowledge and attitude				
Knowledge of the GDPR	Yes, and I know what is means	Yes, and I know what is means	I have never heard of that	Yes, and I know what is means
Attitude/level of concern for privacy	Medium	Medium	Medium	Medium
Practice				
Right to data portability	May use	Might use	Might use	Might use
Right to data erasure	May use	Might use	Might use	Might use
Right to personal data access	May use	Might use	Might use	Might use
Consent/cookies	Positive to the expected enhanced rights	Companies better at informing about cookies	I am unsure what companies do about cookies	Companies allow me to opt out of some cookies

5.2 Qualitative findings

The text analysis revealed insights and more details within knowledge, attitude, and practice. This section starts by presenting the findings from 2023, followed by the main findings from 2018, 2019, and 2020.

The text analysis in 2023 resulted in four clusters:

Cluster 1: Dislike of cookie warnings on websites (mentioned by 19 participants)
Cluster 2: Expressing concerns pertaining to privacy (mentioned by 18 participants)
Cluster 3: Positive to new rights (mentioned by 5 participants)
Cluster 4: Sceptical to new rights; they do not work as intended (mentioned by 18 participants)

Regarding the largest cluster, cookies, the comments were exclusively negative. All the participants had versions of this quote: *"It is incredibly annoying to have to deal with a pop-up about GDPR every time you access a website. Many companies make it extremely difficult to limit cookies and super easy to accept everything".*

The text analysis also revealed that some participants had mixed emotions. For example, one participant shared: *"I have sent several "data erasure requests" over the past few years, many of which were positively addressed by the companies. I believe that the GDPR has increased businesses' awareness of data ownership and responsibility. However, I cannot be entirely certain that the data has not been misused".*

Thus, the comments indicated the respondents' annoyance towards cookies on websites and clear evidence of concerns about their information privacy in general. However, only 36 out of 306 participants chose to answer this open-ended question. However, the comments were similar to the results from previous surveys.

In 2018, our analysis revealed that the respondents had some, or good, knowledge, and interest about privacy and GDPR, and they demonstrated reflection. Their attitude was that the GDPR did not necessarily improve their rights. Regarding practice, the majority stated that they *might* execute their new rights (access, data portability, right to delete). This was before the implementation of the GDPR. Typical quotes:

"I am unsure to what extent this is actually prioritised by the businesses and how one can alone demand this".

"In general, I think that in a large and complicated society, it is more appropriate to have strict, clear GENERAL LAWS AND RULES related to privacy and data collection, rather than to set up for us to have detailed control over

how information about us is used. And in the continuation: that companies MUST comply with clear laws and regulations, but not spend large resources on answers to individual consumers. But, I could be wrong".

"To date, I have not come across a long "terms and conditions" that is readable by most people, so if the text is longer than what fits on one page, it is unlikely to be understandable. At the same time, most such texts are quite similar, so if you are familiar with one, you usually know the main points in most of them".

In the following study of 2019, the respondents demonstrated high knowledge about the regulation and technology, as shown by one of the quotes: *"one cannot have webpages without cookies"*. Regarding attitude, the respondents stated that they were positive about the new rights and articles in theory; however, they did not all think that their rights had improved in everyday life. Regarding practice, they were aware of, for example, cookies and the long "terms and conditions" when downloading an app, but they clicked "I agree" nonetheless. Two reflections read:

"Some companies make it cumbersome and difficult to find out the consequences of where the data ends up, and suggest that you accept the companies' terms that they want you to accept as much data as possible for them", and:

"This is completely idiotic. You cannot have websites without cookies. That they should inform me about cookies and that I must approve every time I access a website is just nonsense. Tracking, on the other hand, should rather be disclosed (which in that case is misuse of cookies)".

Most of the respondents were positive about the idea of the GDPR but unsure about its feasibility. There were a few outliers that were against the whole regulation: *"I would like to add that I am personally completely against the entire GDPR. 'The Right to be Forgotten' conflicts with principles of how the Internet should exist; this should be single-function pages and companies can choose to use, otherwise inform consumers that they do not enforce the right. […] GDPR is an encroachment on the private sphere by a state that should not exist, and people should react to it as such".*

In 2020, our analysis indicated the same conclusions as in previous years: the respondents were clearly concerned about their privacy and were in favour of the new articles. Regarding their practices, we detected some incoherence, as some respondents took more action than others.

To summarise the text analysis, our conclusion from the four surveys is that the respondents claimed extended knowledge about their privacy and the GDPR; they were positive towards their new or enhanced rights, but they had a sceptical attitude towards the feasibility, and their practices were incoherent.

6. Discussion

In response to our research question — *How has five years of the GDPR influenced consumer's knowledge, attitude, and practice of their enhanced rights?* — we structure our discussion according to the KAP (knowledge, attitude, and practice) framework [3] in Section 6.1. We then zoom out to discuss the topic by considering more elements of the diffusion of innovations theory in Section 6.2.

6.1 Knowledge, attitude, and practice

In our study, *knowledge* embraced the GDPR in general, and whether the respondents had heard about cookies. From the quantitative data visualised in Figure 1, we observe that knowledge about the GDPR has fluctuated over the years. It is difficult to see any patterns or make any forecasts regarding whether knowledge has improved over the years. Regarding cookies, however, a few respondents stated that they did not know what cookies were in 2018. No participants ticked off for "Do not know what cookies are" in 2019, but in 2020 and 2023, a few participants stated that they had no knowledge about cookies. From the answers provided in the open-ended questions, it seemed that most of our respondents possessed good knowledge throughout the years, and they seemed to be concerned about the same topics, such as protecting their personal data. One comment read: *"My e-mail was just sold to someone that spams my e-mail with topics like consumer loans".*

The overall *attitude* towards the GDPR has only slightly changed. As visualised in Figure 2, we observe that the "medium" is decreasing, while the "high" is increasing in 2023. Most of our respondents claim that their rights following the GDPR have improved. For every question about enhanced rights, we included the option to choose "I do not care at all". Very few, about 1–2%, ticked off this alternative. Our first study on privacy and the GDPR was published in 2018, just before the GDPR was enforced. The findings showed that prior to the implementation of the GDPR, consumers were more interested in the anticipated enhanced rights than proved to be the case in our survey after 2018. This can be due to several reasons. Just before and at the time when the GDPR was first introduced, there was a lot of focus on the regulation in the media and in various workplaces. The attention on the regulation decreased after the implementation, resulting in less awareness among consumers.

According to our qualitative data, the attitude towards cookies was clearly negative. Some participants went as far as to claim that companies made the information and possibility of opting out difficult and cumbersome on purpose. This negative attitude remained similar in the four surveys. The same observation was made regarding the attitude towards the GDPR. As indicated earlier, a few participants claimed that they were against regulation, but the majority found it useful and interesting. However, they questioned the feasibility, and very few stated that they had executed their enhanced rights.

In our study, *practice* pertains to the use of the right to data portability, insight, and deletion. Our data from the four surveys revealed a status quo, with a small dip compared to our first study in 2018. As previously described, cookies were a recurring topic for many of our respondents in the open-ended question. This may be because consumers encounter this issue almost every time they visit a website. As pointed out by many respondents, if they do not accept the website's use of (at least the necessary) cookies, access is denied and/or limited to a greater extent. Nevertheless, the findings show that cookies are engaging and that consumers noticed a change in the information provided relating to the use of cookies after the GDPR was implemented.

Do we find any evidence of cue-to-action [3] in our research? Meaning, do our participants describe any "wake-up calls" that have led them to take more action? From the comments provided in the open-ended questions, we noted that there were descriptions of incidents, such as having e-mails sold to third parties. However, we did not find that the incidents were severe enough. One reply reads: *"If I had been really concerned about privacy, I would have stopped using Facebook and Google a long time ago".*

6.2 Using other elements from the diffusion of innovations

Rogers claimed that most studies within the diffusion of innovations theory have been from a variance perspective, and he issued a call for more research using a process perspective [3]. Variance research is a type of analysis of a set of variables that examines cause and effect, while process research seeks to determine the sequence of events over time [32]. Rogers did not provide any reasons for the predominance of variance research, but we believe that the reason is rather obvious: research over time requires, well… time. Thus, we argue that the main strength of this study is the empirical data collected four times between 2018 and 2023. By drawing on both quantitative and qualitative data, we demonstrated knowledge, attitude, and practice over time using graphs, and we unravelled some insights among consumers, as summarised in Table 5.

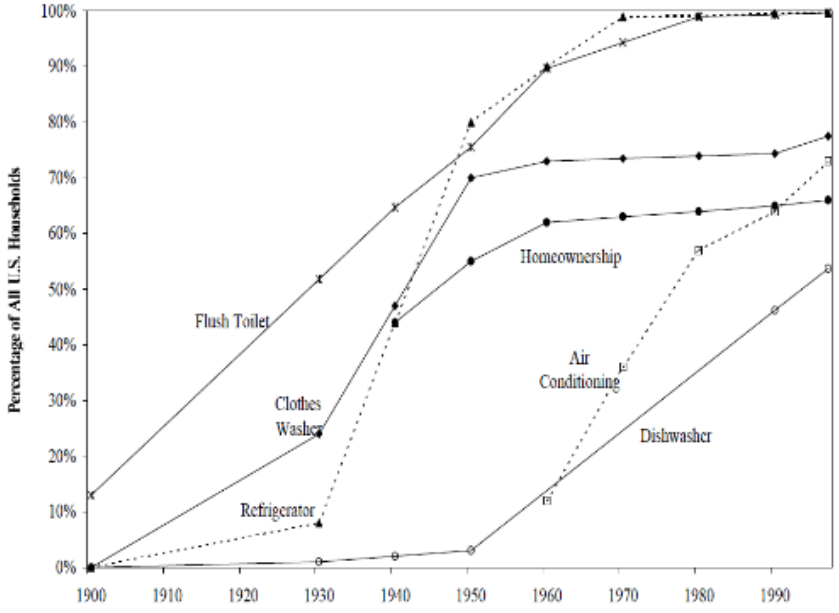
As with any theory, the diffusion of innovations faces several weaknesses, despite its popularity. One criticism provided by Rogers himself is the lack of attention to *anti-diffusion* — that is, the spreading of *bad innovations*, such as cigarettes. Is the increasing ability of information systems to capture, store, and exploit consumer data to be regarded as a *bad innovation*? Add to this machine learning, artificial intelligence, and algorithms. Companies that do not follow this evolution may find themselves out of business if they do not match the actions of their competitors. Researchers have placed a high emphasis on *algorithmic transparency* and *explainable AI*, and it will be interesting to follow the running race between innovative technologies and the call for transparency.

Another criticism that Rogers addressed is that diffusion researchers tend to rely too much upon models, such as KAP, as too rationalistic. Other elements are at play, for example, culture and other decision traps that individuals tend to fall into, such as anchoring, sunk cost, confirming evidence, and more [33]. People are not as rational as we like to think

that we are regarding decision-making [34]. Confirming previous studies [13, 24, 25], we think that our respondents made somewhat informed decisions regarding their personal data, but they had the potential to take more action and place higher value on their personal data.

Third, Rogers drew our attention to the researcher's lack of consequences when an innovation has reached critical mass and becomes self-sustaining. As a serious example, we have the *tragedy of the commons* [35], in which the rational choice of one individual *"...ironically drives the entire system (the is, the "commons") to disaster"* [3 p. 348]. A less serious example is the diffusion of fashion: *"A woman wearing a new fashion becomes furious when she meets another woman at a party wearing the same dress"* (p. 360). This leads us over to the concepts of S-curve and critical mass.

An element of Rogers' diffusion of innovations is the S-curve, introduced in 1913 by Tarde (in Rogers [3]). The strength of S-curves is that they promote forecasting. The weakness is that S-curves can be found in almost *"anything with a beginning and an ending"* [36]. Examples include the number of women with the ability to read, the number of one-year-old infants being vaccinated, and the share of the US population owning a refrigerator [37]. The refrigerator example is depicted [38] with the dotted line in Figure 7 below. To have an S-curve, we need critical mass. Following a critical mass, we get self-sustainability.



Sources: *American Housing Survey for the United States in 1997;* and U.S. Bureau of the Census, "Housing Then and Now," www.census.gov/hhes/www/housing/census/histcensushsg.html.

Fig. 7: *Improvement in U.S. Housing* [38, p. 19].

Our case is not about home appliances, but rather making people care about their information privacy and enhanced rights. This can be harder to quantify than sales numbers. Nevertheless, none of our graphs depict any S-curves and our findings indicate that we are nowhere near critical mass. We keep in mind that researchers warn against placing too much emphasis on S-curves, and we probably need more than five years of study to draw further conclusions. How can we reach critical mass, S-curves and self-sustainability? Rogers suggested four strategies for reaching critical mass:

First strategy: Highly respected individuals should embrace innovations.

Second strategy: If possible, change the perception of the innovation, for example, by indicating that the critical mass has already been reached.

Third strategy: Introduce the innovation to groups that are most perceptive to innovations.

Fourth strategy: Provide incentives for using the innovation.

Regarding the use of a new information system, for example, these strategies are logical. Hence, the following is plausible: Introduce the new HR/CRM/ERP system to a few cool people in the department (first strategy), focus on the great benefits that "everybody" talks about (second strategy), target the *right* people instead of *many* people (third strategy), and provide free training or sell the information system cheap at first (forth strategy).

However, we struggle with these strategies in our context. For example, many people resisted taking the polio vaccine in the 1950s, until Elvis Presley appeared on television while getting the shot. Suddenly, 80% ran to get the vaccine (see, for example [39, 40]). Will it help if we get a contemporary rock star to promote the GDPR? Probably not. Actually, our analysis showed that our respondents were focused on themselves, and they did not mention any network or influence from others. Nobody mentions being affected by peers, for example. It does not seem to matter what family, friends, or colleagues do. Thus, it is tempting to conclude that we need another explanation. As mentioned earlier, Rogers reminded researchers of the cultural aspects of innovations. According to, for example, Hofstede [41], Norway's culture is individual-centred but also with high trust in the authorities. One participant wrote that *"Terms and conditions of that kind are largely invalid in Norway, so they mostly do not apply to me".* We are unsure of how to interpret this statement. Is it naïve? We argue that most of our respondents did not appear naïve but rather demonstrated that they were aware of companies' (mis)use of their personal data.

Table 8 summarises our discussion. This table also constitutes our contribution, which is mainly new insights to the industry but also to academia due to our strong use of the diffusion of innovations theory.

Table 8. Summing up our discussion and main findings.

The diffusion of innovations [3] is a process of four main elements: we need (1) an innovation that is (2) communicated through certain channels (3) over time among (4) members of a social system.		
Element	**Description by Rogers [3]**	**Our study and findings**
1) An innovation	An idea, practice, or object that is perceived as new by an individual. The innovation can be planned or spontaneous. *Innovation* and *technology* are often used as synonyms.	The innovation is both the technology and the analytical tools as part of information systems, as well as the implementation of the GDPR.
2) Communicated through channels	The means by which messages get from one individual to another. Radio, TV, newspaper, Internet, or face-to-face exchanges between two or more individuals or peers.	Privacy has been debated for many years, probably mostly in newspapers and books. In addition, we have TV, telephone, and, lately, the Internet. The words of the GDPR are accessible to anyone with a laptop and the Internet.
3) Over time	Usually, when visualised by a graph, the innovation evolves with an "S-curve", if critical mass occurs. After critical mass, the innovation becomes self-sustainable by adding more value to the new users and adopters of the innovation.	Our study is between 2018–2023, with four sets of data collection. Our graphs do not form S-curves, and we lack critical mass. Will one individual's care about privacy and use of the GDPR make it more valuable to everyone? 5 years of study may not be sufficient. It took 150 years before the fax machine became successful.
4) Members of a social system	A social system is a set of interrelated units that are engaged in solving problems or reaching a common goal. The members can be individuals, groups, villages, organisations, or subsystems. Smoking, for example, was an individual choice until it became illegal by law to smoke in public places (restaurants and others).	Making use of enhanced rights (the articles of the GPDR) is an individual act. Using credit cards and opting out of cookies from websites may no longer be an actual choice. The members in our study are mainly the individuals, namely the citizens within EU/EAA. However, the data protection authority enforces violations of the GDPR.

7. Conclusion, limitations, and suggested future research

This study has been guided by the research question: *How has five years of the GDPR influenced consumer's knowledge, attitude, and practice of their enhanced rights?* Based on our empirical data, it should be safe to conclude that the GDPR has not changed too much for consumers. The graphs presented in this study indicate unclear patterns regarding knowledge. The graphs either show fluctuations, as in the knowledge of the GDRP, or stability, as in the low execution of the articles. We may not be able to draw any conclusions about the influence of the regulation. Our participants possessed a high level of knowledge about the GDPR and technology, both before and after the implementation of the regulation. Their attitude is positive towards the GDPR in theory, but they question the feasibility. Recurring examples are cookies on websites and long-term regulations when downloading an app. Regarding the practice, our respondents acted differently. Some took much action, others did not, but both groups reflected on their actions or lack of action. Our findings regarding the use of selected articles, such as the right to access, data portability, and deletion, are crystal clear. Most respondents *might want to execute* their rights, followed by *will most likely not execute* these rights.

Our contribution consists of insights. We applied elements from the diffusion of innovations, which helped us structure the study. However, the theory proved less useful in discussing how to make consumers take more action. This is but one limitation of our study. Another limitation is that we cannot fully explain the insights that we offer, and we hope that future research projects will conduct in-depth interviews with consumers, for example. We note that there is a lack of network effects or influence from peers. Thus, it is tempting to conclude that for the GDPR or future regulations to be used by consumers, authorities and legislators must be the main drivers. This could also be subject to future research.

Our surveys were completed by Norwegian citizens. It will be interesting to follow the development in, for example, the US, where similar regulations are being implemented. Future studies can include cultural aspects. For example, will we witness more network effects in countries with a more collective culture than in Norway? Future studies can try to pinpoint the typical *change-agent* [3]. In this case, a change-agent is a person with a high score in knowledge and attitude towards the GDPR and technology, and one who has made use of their rights (forgive our far-fetched association of a "GDPR-Elvis Presley"). Other related research question arises: How can we raise a population that is "algorithm literate"? Studies drawing on different theoretical frameworks or other elements of the diffusion of innovations are also suggested.

This study was built on empirical data collected over five years by the same research team and emphasised the GDPR from a consumer's perspective. We believe that this paper is of interest to both academia and the industry, as well as to individuals and companies. Five years is not long compared to the history of technology and jurisprudence, and more research is needed on the interaction of information systems, information privacy, and regulations in the years to come. We welcome any research that confirms, contradicts, and/or extends, our present study.

Acknowledgments

We thank the editor and the anonymous reviewers at the IJISPM for valuable feedback that raised the quality of our study. Also, we thank all our survey participants. We emphasise that this present journal article builds on three previous publications by Presthus and Sørum, namely CENTERIS 2018 [27], IJISPM 2019 [28], and IADIS 2021 [29]. Our gratitude goes once again to the editors and reviewers of the former publications.

References

[1] D. J. Solove. (2023, January 11). *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*. [Online]. Available: https://ssrn.com/abstract=4322198

[2] K. E. Martin, "Ethical issues in the big data industry," *MIS Quarterly Executive*, vol. *14*, no. *2*, pp. *67-85*, June, 2015.

[3] E. M. Rogers, *Diffusion of Innovations*, *5*th ed. The Free Press, 2003.

[4] K. D. Martin and P. E. Murphy, "The role of data privacy in marketing," *Journal of the Academy of Marketing Science*, vol. *45*, pp. *135-155*, March, 2017.

[5] H. J. Watson and C. Nations, "Addressing the Growing Need for Algorithmic Transparency," *Communications of the Association for Information Systems*, vol. *45*, pp. *488-510*, January, 2019.

[6] P. Vassilakopoulou, E. Parmiggiani, A. Shollo and M. Grisot, "Responsible AI: Concepts, critical perspectives and an Information Systems research agenda," *Scandinavian Journal of Information Systems*, vol. *34*, no. *2*, pp. *89-112*, December, 2022.

[7] D. J. Solove. (2020, January 26). *Privacy + Security Blog. News, Developments, and Insights.* [Online]. Available: https://teachprivacy.com/cartoon-the-history-of-privacy/

[8] T. Kaapu and T. Tiainen, "Consumers' Views on Privacy in E-Commerce," *Scandinavian Journal of Information Systems*, vol. *21*, no. *1*, pp. *3-22*, 2009.

[9] F. Bélanger and R. E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, vol. *35*, no. *4*, pp. *1017-1041*, December, 2011.

[10] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. *26*, no. *2*, pp. *xiii-xxiii*, June, 2002.

[11] B. Dahlbom, "The New Informatics," *Scandinavian Journal of Information Systems*, vol. *8*, no. *2*, pp. *29-48*, 1996.

[12] I. J. Aasen, T. Brattvåg and I. Eidhammer, *Innføring i databehandling*, [Norwegian] *2*th ed. Tano Aschehoug, 1998.

[13] W. Presthus and L. R. Andersen, "Information Privacy from a Retail Management Perspective," in *Proceedings of the 25th European Conference on Information Systems (ECIS),* Guimarães, Portugal, June 5-10, 2017, pp. *1968-1983.*

[14] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P. A. Vervier and I. Santos, "Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, Auckland, New Zealand, July 9-12, 2019, pp. *340-351.*

[15] E. Jarbekk and S. Sommerfeldt, *Personvern og GDPR i praksis*. [Norwegian] Cappelen Damm, 2019.

[16] W. Presthus, H. Sørum, and L. R. Andersen, "GDPR compliance in Norwegian Companies," in *Norsk konferanse for organisasjoners bruk av IT (NOKOBIT),* Svalbard, September 18-20, 2018, pp. *1-14.*

[17] A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera and E. Weippl, "Measuring cookies and web privacy in a post-gdpr world," In *Passive and Active Measurement: 20th International Conference, PAM 2019, Proceedings 20* Springer International Publishing, Puerto Varas, Chile, March 27–29, 2019, pp. *258-270.*

[18] J. Dexe and U. Franke, "Nordic lights? National AI policies for doing well by doing good," *Journal of Cyber Policy*, vol. *5*, no. *3*, p. *332-349*, December, 2020.

[19] W. Presthus and K. F. Sønslien, "An analysis of violations and sanctions following the GDPR," *International Journal of Information Systems and Project Management*, vol. *9*, no. *1*, pp. *38-53*, February, 2021.

[20] J. Dexe, U. Franke, K. Söderlund, N. van Berkel, R. H. Jensen, N. Lepinkäinen and J. Vaiste, "Explaining automated decision-making: a multinational study of the GDPR right to meaningful information," *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. *47*, no. *3*, pp. *669-697*, May, 2022.

[21] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra and C. Colautti, "Privacy calculus model in e-commerce – a study of Italy and the Unites States," *European Journal of Information Systems*, vol. *4*, no. *15*, pp. *389-402*, 2006.

[22] N. Momen, M. Hatamian, and L. Fritsch, "Did app privacy improve after the GDPR?", *IEEE Security & Privacy*, vol. *17*, no. *6*, pp. *10-20,* 2019.

[23] R. N. Zaeem, and K. S. Barber, "The effect of the GDPR on privacy policies: Recent progress and future promise," *ACM Transactions on Management Information Systems (TMIS),* vol. *12,* no. *1,* pp. *1-20,* December, 2020.

[24] D. J. Solove, "The Myth of the Privacy Paradox," *George Washington Law Review, Legal Studies Research Paper*, vol. *89*, no. *1*, pp. *1-52*, January, 2021.

[25] B. Knijnenburg, E. Raybourn, D. Cherry, D. Wilkinson, S. Sivakumar and H. Sloan. (2017, February 27). *Death to the Privacy Calculus*? [online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2923806

[26] T. Alashoor, "Explaining the Privacy Paradox through Identifying Boundary Conditions of the Relationship between Privacy Concerns and Disclosure Behavior," Doctor of Philosophy Dissertation, Georgia State University, 2019.

[27] W. Presthus and H. Sørum, "Are Consumers Concerned About Privacy? An Online Survey Emphasizing General Data Protection Regulation," *Procedia Computer Science*, vol. *138*, pp. *603–611,* 2018.

[28] W. Presthus and H. Sørum, "Consumer perspectives on information privacy following the implementation of the GDPR," *International Journal of Information Systems and Project Management*, vol. *7*, no. *3*, pp. *19-34*, May, 2019.

[29] W. Presthus and H. Sørum, "A three-year study of the GDPR and the consumer," in *14th IADIS International Conference Information Systems*. Virtual Conference, March, 2021, pp. *153-160*.

[30] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*. Thousand Oaks: Sage Publications, 1994.

[31] R. Sharda, D. Delen, and E. Turban, *Analytics, Data Science & Artificial Intelligence: Systems for Decision Support. 11*th ed. Hoboken, NJ, Pearson, 2020.

[32] A. Burton-Jones, E. R. McLean and E. Monod, "Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit," *European journal of information systems*, vol. *24*, p. *664-679*, September, 2015.

[33] J. S. Hammond, R. L. Keeney and H. Raiffa, "The Hidden Traps in Decision Making," *Harvard Business Review*, vol. *84*, no. *1*, pp. *118-126*, January 2006.

[34] H. A. Simon, *The new science of management decision*, (Revised). Prentice-Hall, Inc. 1977.

[35] G. Hardin, "The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality," *Science*, vol. *162*, pp. *1243-1248*, 1968.

[36] T. Modis, "Strengths and weaknesses of S-curves," *Technological Forecasting and Social Change*, vol. *74*, pp. *866-872*, July, 2007.

[37] H. Rosling, O. Rosling, and A. R. Rosling, *Factfulness. Ti knep som hjelper deg å forstå verden,* [Norwegian]. *1*st ed. Cappelen Damm, 2018.

[38] S. Moore and J. L. Simon, "The greatest century that ever was: 25 miraculous trends of the past 100 years," *Cato Institute*, no. *368*, pp. 1-32, December, 1999.

[39] M. Hungeberg. (2023, January 6) *Vaccinehistorier: Elvis, kampagner og erstatninger [Danish]*. The Polio Society [Online]. Available: https://www.polio.dk/publikationer-polio/vaccinehistorier-elvis-kampagner-og-erstatninger/

[40] H. Hershfield and I. Brody. (2021, January 18). *How Elvis Got Americans to Accept the Polio Vaccine* Scientific American [Online]. Available: https://www.scientificamerican.com/article/how-elvis-got-americans-to-accept-the-polio-vaccine/

[41] G. Hofstede, "Cultural predictors of national negotiation styles," in *Processes of international negotiations*, Frances Mautner-Markhof, Westview Press, Boulder, San Franscisco & London, 2019, Routledge, 2019, ch. *3*, pp. *193-201*.

Appendix: Our questionnaire (from 2023) consisting of 12 questions

1. Gender
2. Age
3. Level of education
4. Main occupation

5. To what extent are you generally concerned about privacy, when it comes to yourself as a consumer?
[None whatsoever - Low degree - Medium degree - High degree - Do not know]

6. On July 20, 2018, the GDPR (General Data Protection Regulation) was introduced in Norway. Have you heard about it (before you started answering this survey)?
[Yes, and I know what it means - Yes, I know a little, but not enough about what it means - Yes, but I do not know what it means - No, I have never heard of the GDPR]

7. The GDPR means that individuals have gained new rights regarding the collection and storage of personal data. Which answer option suits you best?
[I think my rights have improved - I do not think my rights have improved - I do not care at all - Do not know]

8. Data portability is a central part of the GDPR. This means that you can transfer all data about you that a business has stored. E.g. you can request that your telephone company sends your mobile usage data to a competitor if you wish to change mobile operator. Which answer option suits you best?
[This is something I have used - I will possibly use - I most likely will not use - I do not care at all - Do not know]

9. The GDPR has given you a greater right to demand that certain personal data (that businesses have collected about you) be deleted. Which answer option suits you best?
[This is something I have used - I will possibly use - I most likely will not use - I do not care at all - Do not know]

10. The GDPR gives you the right to an answer within 30 days when you approach businesses with questions related to your data (the right to access). The overview must be sent in a readable format and that way you can correct any errors. Which answer option suits you best?
[This is something I have used - I will possibly use - I most likely will not use - I do not care at all - Do not know]

11. The GDPR states that you can accept some cookies, but not all, when you visit a website. In addition, information must be given to a greater extent about the purpose of the data that is stored about you. Tick all the answer options that you think applies to you.
[Companies have become much better at informing about cookies - The companies give me the opportunity to opt out of some cookies - I am unsure what the companies actually do when it comes to cookies - I do not care at all - Do not know what cookies are]

12. If you have any experiences related to privacy and GDPR beyond what is covered in the questions above, please describe: [open question with text box]

Wanda Presthus
Wanda Presthus is an Associate Professor at Kristiania University College in Oslo, Norway. She holds a Ph.D. from the University of Gothenburg (Sweden). Her research focuses on information systems, business analytics, research methods, privacy and the GDPR. She has published in international journals and conferences.

Hanne Sørum
Hanne Sørum is an Associate Professor at Kristiania University College in Oslo, Norway. She holds a Ph.D. from Copenhagen Business School (Denmark). Her research focuses on information systems, human-computer interactions, eGovernment and privacy and the GDPR. She has published in international journals and conferences.