Data Protection or Data Frustration?
Individual perceptions and attitudes towards the GDPR

[European Data Protection Law Review, 2020 6(3), pp.407-421]

Joanna Strycharz
Amsterdam School of Communication Research, University of Amsterdam
Jef Ausloos
Institute for Information Law, University of Amsterdam
Natali Helberger
Institute for Information Law, University of Amsterdam

Abstract

Strengthening individual rights, enhancing control over one's data and raising awareness were among the main aims the European Commission set for the General Data Protection Regulation (GDPR). In order to assess whether these aims have been met, research into individual perceptions, awareness, and understanding of the Regulation is necessary. This study thus examines individual reactions to the GDPR in order to provide insights into user agency in relation to the Regulation. More specifically, it discusses empirical data (survey with $N = 1288$) on individual knowledge of, reactions to, and rights exercised under the GDPR in the Netherlands. The results show high awareness of the GDPR and knowledge of individual rights. At the same time, the Dutch show substantial reactance to the Regulation and doubt the effectiveness of their individual rights. These findings point to several issues obstructing the GDPR's effectiveness, and constitute useful signposts for policy-makers and enforcement agencies to prioritise their strategies in achieving the original aims of the Regulation.

I. Introduction

In May 2020 it will be two years since the General Data Protection Regulation (GDPR) entered into force. This regulation was introduced by the European Commission specifically in order to (1) ensure appropriate protection for individuals in all circumstances; (2) increase transparency for data subjects; (3) enhance control over one's own data; and (4) raise awareness; (5) ensure informed and free consent; (6) protect sensitive data; and (7) make remedies and sanctions more effective. A lot has already been written on the impact of the GDPR on businesses[1] as well as the many issues surrounding enforcement by data protection authorities (DPA)[2]. Yet, not much information appears to be available on how the new data protection rules are actually understood, used and perceived by individuals. Understanding how individuals – i.e. data subjects – actually experience the GDPR in real life, is necessary to properly assess whether the first five sub-objectives of the Commission have been achieved. After all, these objectives put individual agency, understanding, and awareness central.

When the Commission first announced its plans for a major data protection law overhaul in 2010, the first objective it listed was to strengthen individuals' rights[3]. 'It's your data – take control' is the title of an EU citizen's guide to data protection in the EU, explaining that 'The EU's data protection rules give you more control over your personal data, meaning you can shop, share and surf with confidence'.[4] In a recent document, titled 'Data protection rules as a trust-enabler in the EU and beyond – taking stock', the Commission specifies that 'The EU data protection legislative framework is a cornerstone of the European human-centric approach to innovation.'[5] In the same document the European Commission also concludes that while individuals are increasingly aware of, and exercise their rights, there is also still considerable room for improvement and more awareness.[6] Thus,

---

[1] E.g., Colin Tankard, 'What the GDPR means for businesses' [2016] Network Security 6; Center for Information Policy Leadership, 'GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges' [2019]

[2] E.g., European Data Protection Board, 'First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities' [2019]

[3] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Comprehensive Approach on Personal Data Protection in the European Union' [2010]

[4] European Commission 'It's your data – take control. A citizen's guide to data protection in the EU' [2019]

[5] European Commission, 'Data protection rules as a trust-enabler in the EU and beyond – taking stock' [2019]

[6] According to the Commission, 67 % of Europeans are aware of the GDPR, and filed 144,376 complaints and queries to DPA's (state: May 2018).

the question that this article poses is: what is the users' perspective on GDPR? Do they feel empowered indeed, and did the GDPR succeed in strengthening individual rights and conveying a feeling of confidence and control?

Actual research on individuals' perspective on the GDPR is rather scarce. To the best of our knowledge, the only systematic surveys were done either by private (Deloitte)[7] or public (Commission)[8] organisations, and not by academic institutions. So far, academic research has investigated questions such as the GDPR's effectiveness in light of individual biases[9] and its impact on informed consent and privacy policies[10], but studies on individual perceptions are lacking. The Deloitte report (December 2018, 1.650 respondents from 11 countries[11]) focuses on the impact of the GDPR on the relationship between organisations and its clients and investigates how the GDPR has changed consumer behaviour online. It alleges that only 34% of EU respondents do not read privacy notices, 78% of respondents being aware of 'the key rights that they have', and 10%, 9% and 12% having exercised their rights of access, portability and erasure respectively. The Eurobarometer (March 2019, 27.525 respondents from all EU member states) aims to explore general awareness among Europeans of the GDPR as well as describes their data sharing and protection behaviour. According to the report, 60% of respondents reads privacy policies, 65% (18%) and 56% (13%) of respondents had heard of (and exercised) the right of access and erasure respectively. While both surveys offer relevant insights into the effect of the GDPR on individuals and their relation with organizations, they disregard individuals' affective perceptions of the Regulation. At the same time, social scientific theories[12] inform us that such affective reactions are crucial for effective strengthening of individuals' rights, which is one of the main aims of the Commission.

This paper complements these earlier surveys by offering rigorous and well-documented empirical data on the knowledge of, reaction to, and rights exercised under the GDPR within the Netherlands. The Netherlands are a relevant context for this research as this

---

[7] Deloitte, 'A New Era for Privacy: GDPR Six Months On' [2018] <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>
[8] European Commission, 'Special Eurobarometer: The General Data Protection Regulation' [2019] 487a
[9] Iris van Ooijen and Helena U. Vrabec, 'Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective' [2019] 42(1) Journal of consumer policy
[10] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub and Thorsten Holz. 'We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy.' [2018] arXiv preprint arXiv:1808.05096
[11] I.e. UK, Spain, Italy, Netherlands, France, Germany, Sweden, USA, Canada, India, and Australia.
[12] E.g., the Protection Motivation Theory: Ronald Rogers, 'A protection motivation theory of fear appeals and attitude change' [1975] 91 The Journal of Psychology

country has the highest relative number of households with home Internet access (97%) and mobile access to the Internet (91% of population) in the EU [13]. This paper describes the results of a panel survey (N=1288), specifically aimed at investigating user agency (are individuals aware of their rights and do they use them); people's understanding of the GDPR and its aims; and their affective reaction to the GDPR. This focus, not just on *awareness*, but also on user *perceptions*, adds a new dimension to existing discussions on measuring the effectiveness of the GDPR. While awareness is undoubtly curcial for individuals' ability to evoke their rights and thus for the effectiveness of those rights, social scientific research emphasises the importance of perceptions as well. In fact, a combination of awareness and positive perceptions determines whether or not an individual will exercise protective behavior such as using their rights.

The current study thus makes multiple contributions. We believe that empirical data like this is a critical component in any effort aimed at evaluating the GDPR's overall effectiveness. Conclusions drawn from such data allow to identify key challenges that might obstruct the GDPR's effectiveness, helping policy-makers and enforcement agencies to prioritise their efforts and identify strategies to improve effective data protection. Moreover, we believe the findings to be valuable to a broader set of actors – including the media, enterprises and NGOs – that may use them in their own respective informational, compliance and/or campaigning efforts. On a more theoretical level, the findings also contribute to research on individual empowerment in the privacy and data protection context. Investigating attitudes towards the GDPR, as well as individual knowledge and use of rights enables drawing conclusions about possible causes and consequences of individual reactance to the Regulation and lack of empowerment. Research into user perceptions of the GDPR, moreoever, adds a further important bottom-up perspective through which the Regulation can be assessed. Too often, law and legal analysis tends to view 'the user' in rather abstract terms. Empirical insights into who those users are, their perceptions and the factors that influence their legal behaviour has the potential to to enrich the legal analysis, and ultimately contribute to more effective laws and policies. More concretely, the findings from our study shed a new light on the so-called privacy paradox. They also draw attention to the fact that users are not only subject to the protective provisions but also obligations under GDPR, obligations that many experience as cumbersome and problematic. Effective data protection laws need to be based on a deeper understanding of the role of data as constituting element of

[13] European Commission, 'Special Eurobarometer: E-Communications and the digital single market' [2018]

engaging in social, political and economic practices. This study hopes to contribute to developing such an understanding.

II. Research into individual reactions to the GDPR and its relevance

1. Past research into consumer reactions to GDPR

In the last years, the GDPR has received great public attention in the Netherlands. Already before the law was introduced, the topic of privacy and data protection was widely covered in the media[14]. In fact, this study showed that the authorities' responsibility to protect individuals' privacy was one of the main topics that Dutch media reported on in relation to privacy in the last ten years. As media play an important agenda setting role in society[15], one could expect that this media attention would result in increased awareness and interest among general population.

As mentioned before, two recently published studies focused on the reception of the GDPR among the general population: one by consultancy firm Deloitte,[16] and a EuroBarometer survey.[17] The Deloitte study was conducted six months after the Regulation went into force, and took an organizational perspective. More specifically, the survey's aim was to discover how the regulation impacted consumers' relations with organizations. The study did not investigate affective reactions of individuals to the regulation, but focused on how organizations complied with the GDPR, how the regulation had changed individuals' trust in organizations who handle users' data and if individuals were aware of their rights. The report thus provides interesting findings regarding public reception of the GDPR. First, the authors conclude that regarding public opinion, a perceptual change has taken place in consumers' minds. More specifically, 44% of respondents believe that organizations care more about their privacy since the GDPR is in force. However, the report does not clarify whom the respondents see as responsible for privacy and data protection nor if they see the current privacy protection measures taken by e.g., organizations as effective. To bridge this gap, we aim to answer these questions in the current study. Second, the report draws positive conclusions regarding strengthening of individuals' rights, one of the aims of the GDPR. In

---

[14] Joanna Strycharz, Guda van Noort, Edith Smit, Rens Vliegenthart, and Natali Helberger, 'Media effects on public opinion about online privacy' [2017] Proceedings of the International Conference on Computational Social Science.
[15] Maxwell E. McCombs and Donald L. Shaw, 'The agenda-setting function of mass media' [1972] 36(2) Public opinion quarterly
[16] Deloitte, 'A New Era for Privacy: GDPR Six Months On' [2018] <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>
[17] European Commission, 'Special Eurobarometer: The General Data Protection Regulation' [2019] 487a

fact, the authors conclude that when it comes to consumer rights, consumers have a very high level of awareness, with 78% on average being aware of the key rights that they have been offered. It is worth noting that the report only presents findings regarding awareness of the rights, which does not automatically imply that individuals understand what they entail. The high awareness stands in contrast to low actual usage of the laws (highest use: right to opt-out of direct marketing: 20% of respondents) and even lower intention to use the rights in the future (with 24% of respondents having no intention ever to use their right to portability). The reasons for this strong contrast between awareness and actions has not been further researched in the report and is thus central in the current study. The Deloitte report also concludes that most consumers do not feel that their data is better handled by organizations since the introduction of the GDPR. In fact, the results highlight that consumers feel that certain practices used by organizations online, such as placing cookies, are excessive and make them concerned. The study does not however report how this relates to use of cookie opt-out notices by individuals who want to protect their privacy. All in all, the report delivers relevant insights into consumer reception of the Regulation and suggests that even though individuals are aware of the GDPR and their rights, they do not show an intention to use them. However, due to the report's organizational focus, it fails to answer questions central to the issue of individual empowerment, such as attitudes towards and perceived effectiveness of the GDPR.

About a year after it entered into force, the European Commission published a special Eurobarometer on the GDPR . While the Deloitte study took an organizational perspective, the Eurobarometer puts individuals central and explores awareness of the GDPR in particular, as well as more general opinions related to data sharing and protection. More specifically, it covers such topics as knowledge of the GDPR, privacy and data protection concerns and control, attitudes towards privacy policies and use of social networking privacy settings. Similarly to the Deloitte study, the Eurobarometer concludes high awareness of the GDPR: 67% of respondents have heard of it and 73% are aware of at least one right guaranteed by the regulation (with the right to object to receiving direct marketing, the right to access personal data and the right to correct personal data if it is wrong being most widely known). While knowing at least some of their rights, most respondents have not exercised them (with the right to object to receiving direct marketing being most often exercised (24% of respondents) and the right to object automated decision-making being least exercised (8% of respondents). However, the Eurobarometer did not investigate the reasons behind these numbers, such as perceived effectiveness of rights and existing privacy or data protection

tools. Regarding attitudes, the Eurobarometer shows that 62% of respondents are at least fairly concerned about not having complete control over the information they share online. The Eurobarometer did not discuss this finding in light of the GDPR – no conclusions were made regarding how the regulation contributes to or mitigates this concern. All in all, while the Eurobarometer delivers valuable insights into awareness of the GDPR as well as relevant behaviours such as reading privacy policies or adjusting social media privacy settings, it does not inform us about individual understanding of and attitudes towards the GDPR and related rights. These three factors not investigated in the Eurobarometer require further attention as social scientific research has shown that knowledge and affective perceptions are crucial is shaping one's motivation to protect themselves by for example making use of their individual rights.

2. Individual attitudes and protection motivation

Questions on antecedents of individuals' intention to use and perceived efficacy of their rights have been widely researched in the social sciences. For the purposes of this article, Protection Motivation Theory (PMT) is particularly relevant, explaining why people are motivated to protect themselves from threats. PMT was originally developed by Rogers to explain why people were motivated to protect themselves from health threats.[18] The theory identifies two cognitive processes that motivate a person to act: a *threat appraisal* and a *coping appraisal*. While threat appraisal relates to the perceptions of the threat itself, coping appraisal assesses one's belief to be able to protect oneself and that the protective action is effective (so-called *response efficacy*). In the context of assessing rights effectiveness, response efficacy is particularly important – PMT assumes that one needs to believe in the rights available to them, in order to be motivated to use them. While the theory has been developed in the context of health threats, it has been applied to threats online, such as self-disclosure[19]. In recent years, this theory has also been commonly applied to explain why and how individuals (do not) protect their privacy and data online: Boerman, Kruikemeier and Zuiderveen Borgesius[20] concluded that response efficacy substantially predicted one's motivation to undertake different protective actions (such as declining tracking cookies),

[18] Ronald Rogers, 'A protection motivation theory of fear appeals and attitude change' [1975] 91 The Journal of Psychology

[19] Mohammadreza Mousavizadeh, and Dan Kim, "A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory." [2015] 9 Asspciation for Information Systems.

[20] Sophie Boerman, Sanne Kruikemeier, and Frederik Zuiderveen Borgesius, 'Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data' [2018] Communication Research

while Strycharz, van Noort, Smit and Helberger pointed to response efficacy as one of the main predictiors of opting out of online data use for personalization.[21] We thus expect that, in order to feel empowered to make use of their rights when needed, individuals need to not only be aware of their data protection rights, but also *understand* them, have a *positive attitude* towards these rights and *believe in their effectiveness*.

Similarly, psychological studies into reactance to policies and laws[22] have shown that when an individual experiences reactance, i.e. 'a motivational state directed toward the reestablishment of threatened or eliminated freedom'[23] to a law, this makes them hostile towards it and they are thus less likely to e.g. consider exercising rights guaranteed by it. Therefore, the current study adds to past research into awareness of the GDPR and investigates not only if consumers are aware of the Regulation, but also their affective reactions to the regulation, which are crucial from the perspective of empowerment. As such, this study furthers our (empirical) understanding of users' perceptions of, and attitudes toward the GDPR, and is also of interest to legal scholars and policy makers, to the extent that it can lead to a better understanding of the workings of the GDPR in practice, and possible ways of improving its effectiveness and utility to users.

III. Methods

1. Participants and procedure

This study uses data from a questionnaire that was part of a longitudinal survey administered online by a large research institute in the Netherlands. The data used in this study was collected between July 19 and August 9, 2019. A total of 2106 respondents participated (response rate = 35%). Quotas (on age, gender and education) were enforced in sampling from the database. The data are representative of the population aged 18 years or older. Out of the 2106 respondents participating in the bigger study, 1288 were asked questions about the GDPR (the rest was excluded from this study as they participated in an experiment that could influence their answers). The final sample shows appropriate distributions in terms of gender, age and education compared to census data and consists of 48% female respondents, with a mean age 53 (SD = 16, range 18 – 89). Most had finished a

[21] Joanna Strycharz, Guda van Noort, Edith Smit, and Natali Helberger, 'Protective behavior against personalized ads: Motivation to turn personalization off' [2019] 13(2) Cyberpsychology: Journal of Psychosocial Research on Cyberspace

[22] E.g., Devon Proudfoot and Aaron Kay, 'Reactance or Rationalization? Predicting Public Responses to Government Policy' [2014] 1 Policy Insights from the Behavioral and Brain Sciences

[23] Jack Brehm, 'A theory of psychological reactance.' [1966] Academic Press

medium level of education (50%) followed by a lower level of education (30%) and a higher level of education (20%).

Answering the GDPR survey took approximately 10 minutes. First, responsibility attribution and trust in safe data handling were measured. Next, respondents were asked about their awareness of the GDPR. The ones who were aware of it were asked about their source of information as well as perceptions of the regulation. Those who showed high reactance to the GDPR (scoring on average above the midpoint of the scale) were also asked to explain the reason for it in an open answer. Next, understanding of the regulation was measured. Finally, all respondents (regardless of their previous awareness of the GDPR) were given a short description of the different individual rights and were asked about their effectiveness and use motivation. While the focus of the survey was on the GDPR, a limited number of questions used the term *privacy* in order to make them more understandable for respondents (eg. who is responsible to safeguard your privacy?).[24]

2. Measures

Responsibility attribution was operationalized with a single question: 'Who do you think is responsible for privacy protection' with an answer scale ranging from 1 (Not at all) to 7 (Very much)[25]. The items included the data protection authority, activist groups, companies, individuals, the international community and the state.

Trust in safe data handling reflects the degree to which people believe different actors are dependable in handling their personal data. The following actors were included in the survey: companies, health institutions, media, educational institutions, the state, social media, friends and family.

Awareness of the GDPR was measured with a single yes/no question: 'Have you ever heard of the General Data Protection Regulation?'. To determine possible *sources of information about the GDPR* we conducted a small-scale pre-test with a convince sample (*N* = 16) to construct a list of sources of information (nine sources). In the main survey, the respondents could choose more than one of the following sources: the news (TV, newspapers etc.), employer, friends and family, posts on social media (e.g., Twitter or Facebook), notices on websites (e.g., cookie notices), emails sent by companies that process one's personal

[24] This paper is not intended to dig into the hotly-debated distinction between data protection and privacy. Moreover, we also wish to point out that even if the Charter contains two discrete rights to privacy (Art.7) and data protection (Art.8), the GDPR is aimed at safeguarding both of them (cf. Art.1 GDPR).

[25] Scale adopted from Kerrie L. Unsworth, K.L., Sally V. Russell and Matthew C. Davis 'Is dealing with climate change a corporation's responsibility? A social contract perspective' [2016] 7 Frontiers in psychology

information (e.g., email from one's bank), personal contact with a company that processes one's personal information (e.g., conversation with a customer service employee), educational institutions (e.g., schools or universities), health institutions (e.g., hospitals) and other sources.

Perceived reasonability of the GDPR, i.e., the perception that the scope of the regulation is appropriate, was measured using 4 items adopted from past research[26], measured on a scale ranging from 1 (Totally disagree) to 7 (Totally agree). The example item was: 'In general, the General Data Protection Regulation seems legitimate.' The scale that was constructed by taking a mean was concluded reliable ($\alpha = .73$, $\omega = .75$).

Reactance to the GDPR was based on the Psychological Reactance Theory and was measured using four items adopted from past research[27], measured on a scale ranging from 1 (Totally disagree) to 7 (Totally agree). The example item was: 'The General Data Protection Regulation makes me angry.' The scale, which was constructed by taking a mean of the items, was concluded reliable ($\alpha = .82$, $\omega = .82$). Respondents who scored above the midpoint of the reactance scale were asked to explain the reason for this in an open question. *Reasons for reactance* listed by respondents were coded according to a codebook constructed based on Psychological Reactance Theory (11 categories, see Table 2). All thoughts that did not fit in any of the pre-defined categories were collected and coded in two steps. First, open codes were assigned to each answer. Initial properties of categories were defined in this step. In the second step, with the help of the initial codes, axial codes were assigned to group the initial codes into overarching categories[28]. The newly identified concern categories are presented in the Results section.

Knowledge about the GDPR was measured in two ways. First, a battery of six true/false statements inspired by past research on policy understanding[29] was used (overview of the statements in presented is Table 4). Second, we constructed a question in which respondents were asked which rights the privacy law guarantees them. The answer list included existent (six) and non-existent (four) rights and respondents could choose multiple of them.

---

[26] Scale adopted from Caleb Warren and Margaret C. Campbell 'What makes things cool? How autonomy influences perceived coolness.' [2014] 41 Journal of Consumer Research

[27] Scale adopted from Nicholas Tatum, Michele K. Olson and T. K. Frey 'Noncompliance and dissent with cell phone policies: a psychological reactance theoretical perspective [2018] 67 Communication Education

[28] Juliet Corbin and Anselm Strauss 'Grounded theory research: Procedures, canons, and evaluative criteria.' [1990] 13 Qualitative sociology

[29] Scale inspired by Yong Jin Park, 'Digital literacy and privacy behavior online.' [2013] 40 Communication Research

Finally, to measure *practical use of rights*, all respondents were presented with a list of seven ways to exercise their rights currently offered by digital services with a short explanation of each of the actions and were asked if they have ever undertook of any of them. *Perceived efficacy of rights* focused on the individual rights themselves (regardless of the means to exercise them) and was measured with a single-question inspired by past research on protection motivation[30]: 'To what extent are the following elements of the GDPR an effective way to protect Internet users' privacy?' Here, the respondents were presented with a list of nine individual rights. Overall efficacy of individual rights was constructed by taking the mean of the items ($\alpha = .93$, $\omega = .93$). To measure *motivation to exercise rights* a question was asked also inspired by the Protection Motivation Theory and the same list of nine rights was used. The overall motivation was constructed by taking a mean of the items ($\alpha = .96$, $\omega = .95$).

IV. Analysis and results

Regarding attribution of responsibility for privacy and data protection, a series of t-tests with Bonferroni correction was conducted. This makes it possible to compare scores between different actors and conclude if they significantly differ from each other and thus who is held responsible by the respondents. Four groups differ significantly when it comes to individual perceptions. First, the government and data protection authority were both considered to bear the most responsibility according to respondents. In second place, respondents considered themselves responsible. Third, companies and the international community were considered equally responsible. Finally, activist groups are seen as least responsible for the protection of respondendents' privacy and data protection. In general, the scores are high, with all means above the midpoint of the scale and median of 6 for all but activist groups (see Appendix 1 for detailed results).

Next, the same procedure was used to test respondents trust in safe data handling. Respondents were asked to rate the level of trust they have in the safe processing of their personal data by seven different actors. From these actors, friends and family are seen as significantly most trusted. Health institutions are seen as second trusted. Third, respondents trust educational institutions with their data; fourth, the state. The media and companies shared the second to last place of trusted actors. On the fifth place, and thus considered least

[30] Scale adapted from Sophie Boerman, Sanne Kruikemeier and Frederik Zuiderveen Borgesius, 'Exploring motivations for online privacy protection behavior: Insights from panel data.' [2018] Communication Research

trustworthy, were social media. It is also worth noting that for companies and for social media the median score is lowest (3; see Appendix 1 for detailed results).

Out of all respondents, 79% had heard about the GDPR before taking part in this study. Regarding respondents' source of information about the Regulation, most learned about it from the news (47%), followed by their employers (36%) and notices on webistes (such as cookie notices; 28%). Appendix 1 includes a detailed overview of the main sources respondents first learned about the GDPR from. Regarding perceptions of the Regulation, respondents felt that it was somehow reasonable (M = 4.39) and provided them with some feeling of safety (M = 4.03). Regarding reactance, the respondents felt slightly reactant (*M* = 3.68). In total, 590 respondents (out of 1021 aware of the GDPR) scored above the midpoint of the scale and were asked the additional question about their reason for reactance. In total, they provided 627 thoughts. On average, each respond wrote down 1.1 thoughts (10% did not know reason for they reactance, 70% provided one reason and 20% provided two reasons). These answers were coded following the procedure explained before. Table 2 presents an overview of categories that were with illustrative examples as well as an overview of results.

Table 2. Overview of reported reactance reasons.

Category	Illustrative example	*N*	Percentage
Law imposed in general	*The government imposed the law without any public participation*	152	24.2
Other		96	15.3
Negative consequences for professional life	*It costs a lot of extra time at my work to follow the GDPR. My workload has increased.*	89	14.2
Disproportional scope	*In many instances it is too strict and impossible to work with.*	84	13.4
Negative consequences for personal life	*It has a lot of negative influence on my club – many things are not possible any more.*	81	12.9
Inconvenience	*You have to give your consent literally everywhere. Even in this survey you get this long page on privacy.*	50	8.0
Pressure	*You are more or less obliged to obey*	30	4.8

Anger	*All this bullshit about cookies is annoying!*	23	3.7
Lack of understanding	*[The law] is not clear and simple to me while you come across it all the time and it impacts your data.*	13	2.1
Law imposed by the EU	*It was decided in Europe. I don't need it*	6	1.0
Information overload	*You are bombarded with information about it.*	3	0.5
Manipulation	-	0	0

N = 627 reasons provided by 590 respondents

To further investigate the reasons for reactance not included in the Psychological Reactance Theory, uncategorized responses (the category 'Other') were open-coded (see Methods for full procedure). Table 3 provides an overview of the newly-identified reasons for reactance.

Table 3. Newly identified reasons for reactance.

Category	Illustrative example	*N*	Percentage
Omnipresent	*You are constantly confronted with it everywhere!*	26	27.1%
Ineffective	*It is not easier now to share and request information*	12	12.5%
Strong impact	*The GDPR has more impact than I had expected (e.g., when posting pictures)*	9	9.4%
Unintended consequences	*When everything we do has to be tested against the GDPR, I feel people become less spontaneous*	6	6.3%
Insufficient scope	*I have the idea that I cannot always choose exactly what data I share with whom*	6	6.3%
Selective applicability	*It seriously impacts people while companies do not do anything about it*	6	6.3%

Lack of trust	*This is an obligation that fosters distrust*	5	5.2%
Complexity	*Everything becomes more complicated because of this law*	4	4.2%
Mistakes in enforcement	*The enforcement of the GDPR is bad*	4	4.2%
Patronizing	*There is no choice in what you find important in privacy protection*	4	4.2%
Lack of freedom	*Certain freedoms are not possible now*	3	3.1%
No privacy	*There is no privacy anyway*	3	3.1%
Useless	*I do not see a use in this law*	3	3.1%
Unnecessary	*I don't need this, wasn't waiting for it*	2	2.1%
Limiting for law enforcement	*In case of a crime, you cannot look for the identity of a person*	1	1.0%
Privacy invasive	*To me the law sometimes feels like infringement of my privacy*	1	1.0%
Sensitivity of issue	*The GDPR touches upon sensitive issues*	1	1.0%

N = 96 reasons provided by 590 respondents

Regarding knowledge respondents answered six true/false questions. When the scores are summed, respondents score on average 4.03 (SD = 1.19). Overview of all answers with the correct answer marked in bold is presented in Table 4.

Table 4. Overview of knowledge statements

Statement	% True (*N*)	% False (*N*)
I have the right to ask a search engine to delete certain search results that are being shown when one looks for my name.	**83% (847)**	17% (174)
Important decisions that impact my legal or financial situation (for example, price of life insurance, amount of a fine, recruitment decisions) can be made by an algorithm without me having influence on it.	30% (306)	**70% (715)**

I cannot ask for correction of the data collected about me by a website.	38% (389)	**62% (632)**
The GDPR requires websites to have an easy to understand privacy policy.	**75% (766)**	25% (255)
As an individual, I am simply allowed to post pictures of my family and friends online.	23% (235)	**77% (786)**
I always have to be informed in which country data that has been collected about me is being stored.	64% (653)	**36% (369)**

N = 1021, correct answers are marked in bold.

Regarding rights that respondents believed to have, 66% correctly believed to have the right of access to data collected online (Art.15). 63% correctly selected the right to rectification (Art.16). Next, the right to portability (Art.20) of data was correctly selected by 40% of respondents. The right to be forgotten (Art.17) was correctly selected by 32%. Next, 81% correctly selected the right to object (Art.21). Only 16% thought that the right to object in relation to automated decision making and profiling was real (Art.22). Regarding 'fake rights', 70% of respondents thought to have the right to know in which country their data is being stored. Next, 11% incorrectly selected the right to financial compensation for data. The right to encryption of online messages was incorrectly selected by 30% of respondents. Finally, the right to inheritance of data was incorrectly selected by 26% of respondents.

In the last section, respondents were asked about actions they have taken to exercise their rights. The highest number of respondents, namely 8% (103), have asked a company not to process their data for certain purposes. Next, 5% (64) have used tools that are made available by companies to enable individuals to access information that they have collected about them. 4% (52) have asked a search engine to remove search results related to their name. 3% (39) have requested access to data that a company has collected about them and contacted a company to inquire how they process your data. Next, 2% have asked a company to transfer their data to another company (right to data portability) and for a human intervention in cases of automated decision-making. Overall, 83% (1069) reported not having taken any action. Table 5 gives an overview of the perceived efficacy of rights and motivation to use them in the future. Overall, the right to erasure and right of access are perceived as most effective, while the right to data portability is perceived as least effective. At the same time, respondents have the intention to reject cookies the most and to use data portability and human intervention the least. The overall perceived efficacy of the rights and

motivation to use them in the future are significantly correlated with moderate strenght ($r(1286) = .23$, $p < .01$).

Table 5. Overview of rights' usage and their perceived efficacy

Individual right	Efficacy *M* (*SD*)	Motivation *M* (*SD*)
Right to restrict processing	4.1 (1.42)	3.12 (1.49)
Right to object	4.36 (1.45)	3.18 (1.55)
Right to data portability	3.85 (1.41)	2.92 (1.43)
Right to be forgotten	4.38 (1.52)	3.19 (1.55)
Right of access	4.47 (1.48)	3.31 (1.60)
Right to human intervention in automated decision making	3.99 (1.39)	2.98 (1.40)
Right to rectification	4.25 (1.44)	3.16 (1.50)
Right to erasure of data	4.23 (1.50)	3.07 (1.53)
Right to object to cookies	4.06 (1.74)	4.01 (1.87)
Overall	4.19 (1.18)	3.22 (1.33)

V. Discussion

The aim of this research was to examine individual reactions to the GDPR in order to provide insights into user agency in relation to the Regulation. Guided by social scientific theories on individual reactance to laws and the Protection Motivation Theory, this research empirically investigated knowledge of, reactions to, and rights exercised under the GDPR within the Netherlands. The results of a panel survey show that the Dutch are aware of the law and know at least some of the individual rights granted to them. At the same time, they show substantial reactance to the Regulation and doubt in the effectiveness of their individual rights. In this section, we discuss the empirical findigs in order to position them within the ongoing scholarly debates on the GDPR and its effectievness.

Regarding knowledge of the GDPR, the Dutch seem to be relatively well informed about the current data protection framework. One explanation for this could be the active reporting on GDPR and privacy/data protection related matters in the Dutch media.[31] Indeed, one first insight from this study is the critical role that the media play in informing people about the GDPR. It was the number one source respondents indicated as where they learned

[31] Joanna Strycharz, Guda van Noort, Edith Smit, Rens Vliegenthart, and Natali Helberger. 'Media effects on public opinion about online privacy' [2017] Proceedings of the International Conference on Computational Social Science

about the GDPR from, followed by their employers, cookie notices on websites and company mailings. If anything, this finding stresses the important role that the media hold in advancing digital literacy and informing the public about privacy and data protection related issues. As such, one can argue that the media have a growing responsibility towards society to report on privacy and data protection related matters, as well as to train journalists in understanding the existing regulatory framework so that they are able to accurately report on new and emerging data protection challenges. The findings also demonstrate that the media can be a strong partner in future awareness and privacy literacy campaigns, maybe even more so than the 'usual suspects', such as NGOs, consumer organisations, regulatory authorities, schools and other educational institutions. Their (near) complete absence in the list of sources of information about the GDPR is probably as striking as is the prominent position that the media hold (though the low number of respondents that learned from the GDPR in school or university can probably also be attributed to the focus of this survey on adults).

The centrality of commercial communications such as newsletters and notices on websites emphasises the importance of businesses taking their transparency obligations seriously. Dry and legalese privacy and data policies alone will rarely fulfil GDPR requirements and will not contribute to better understanding among individuals.[32] In fact, companies processing personal data have a responsibility to inform individuals in a 'concise, transparent, intelligibe and easily accessible form' (Art. 12). Looking at their important role as information source for individuals, it is not only important that they simply list the required information under GDPR (Artt.13-14), but also do so in an easy to comprehend manner.

Despite individuals showing high awareness of the GDPR and reporting many sources of information about the Regulation in general, knowledge and understanding of the actual provisions is mixed among the Dutch. On the positive side, a clear majority of individuals correctly believed that they had the right of access to data, the right to rectify their data, and the right to object. Respondents also understood what many of their rights meant in practice: more than half of respondents correctly answered knowledge questions about practical consequences of the right to be forgotten, right to rectify their data, right to be informed about data collection by websites. On the negative side, there seem to be some (strong) misconceptions about the law: more than two thirds of users incorrectly believed that they had a right to know in which country their data was being stored, almost one third of

[32] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP260

respondents believed they had a right to encryption, and about one quarter thought they had a right to inherit data. At the same time, only a very small fraction of people believed they have a right to seek financial compensation for their data. For future research it would be interesting to learn more about the reasons for these misconceptions, which in turn could inform policy makers and literacy initiatives. In contrast, some rights that *do* exist scored very low in awareness. Indeed, only 16 % of respondents were aware of the right to object to a automated decision-making, including profiling. Also, the fact that the majority of respondents (60%) was not aware of the right to data portability sheds some doubts on the effectiveness of the respective provision in the GDPR to stimulate the transfer of data between platforms as a means of spurring inter-platform competition. In short, these misconceptions should be a call to action for policymakers, regulators, consumer protection authorities and NGOs alike, to set priorities on educating citizens, enforcement and strategic action.

More generally, and in line with the findings from the Eurobarometer and the Deloitte report, our study also found a stark contrast between the (theoretical) awareness and understanding of rights and the perceived efficacy and actual use of (or intention to use) those rights. Some rights (e.g. rights to access information or asking removal of information) were considered by respondents to be more effective in protecting individual privacy and data protection than others (such as right to data portability or human intervention in automated decision-making). Importantly, this finding should not be interpreted as indicating that these rights are superfluous, as there are still important normative reasons to include these rights into the GDPR. Indeed, similar to many other rights aimed at individuals (e.g., consumer rights), they do not necessarily have to be exercised in great numbers in order to be considered 'effective'. Many of the rights in the GDPR primarily serve a fail-safe function, empowering individuals to hold companies responsible when they are not fulfilling their obligations in the first place[33]. That being said, the lack of understanding of the right to human intervention, and the limited perceived usefulness of this and some other rights, do point to a need to revisit these rights and to engage in (evidence-based) evaluations of how to improve their normative content and practical utility for users. As social scientific research informs us, making sure that individuals are not only aware of the existence and substance of individual rights, but also perceive them as effective means of privacy and data protection is

[33] Gloria González Fuster, 'Beyond the GDPR, above the GDPR.' [2015] Internet Policy Review; Jef Ausloos 'The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection.' [2020] Oxford: Oxford University Press

crucial for related behaviour. The current study shows a moderate positive correlation between perceived efficacy of rights and motivation to ever use them in the future. This can be brought back to the Protection Motivation Theory commonly applied to explain individuals' motivation to use their rights and protect their privacy[34]. According to this theory, believing in efficacy of a protective action (such as asking for a human intervention in automated decision-making) is crucial for the motivation to exercise it. Therefore, improving the 'image' of individuals rights among users is central to individual agency online.

Maybe the most striking finding from the study is the high level of reactance to the GDPR – a piece of legislation that has been widely announced, and celebrated as a move on the side of the EU to improve the standing of individuals in the digital economy and put the digital citizen central. Vice-president Timmermans, and Commissioners Jourova and Gabriel announced the GDPR in a joint press release with the words: 'One of the main aims of the General Data Protection Regulation is to empower people and give them more control over one of the most valuable resources in modern economy - their data.'[35] And elsewhere the Commission explained: 'The EU data protection legislative framework is a cornerstone of the European human-centric approach to innovation.'[36] The European regulator might have had the ambition to adopt a human-centric approach, but from our study it becomes clear that a significant part of the (Dutch) population does not appreciate this effort, nor feel very central to this regulatory project. Strikingly, almost a quarter of respondents indicated that they felt the GDPR had been imposed on them. As one participant responded: *Everyone pretended that citizens had impact on it through public participation, but this was not the case* and *It was introduced by the government; I didn't ask for it and I don't think it benefits the society as a whole.* It is worth mentioning the much lower number of users who indicated that the rules had been imposed on them by Brussels in particular. This is a surprising finding in the light of past research on Euro-scepticism and anti-European propaganda that concluded high presence of such discourse in Dutch media[37]. And yet, despite the ambition that the Regulation must provide users with more control and agency, a significant part of the Dutch

---

[34] E.g., Ronald Rogers 'A protection motivation theory of fear appeals and attitude change' [1975] 91 The Journal of Psychology; Sophie Boerman, Sanne Kruikemeier, and Frederik Zuiderveen Borgesius, 'Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data' [2018] Communication Research

[35] European Commission 'Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel ahead of Data Protection Day' [2019]

[36] European Commission 'Data protection rules as a trust-enabler in the EU and beyond – taking stock' [2019]

[37] For example, Marcel Lubbers and Eva Jaspers 'A longitudinal study of euroscepticism in the Netherlands: 2008 versus 1990' [2011] 12(1) European Union Politics; Patrick Bijsmans 'EU Media Coverage in Times of Crisis: Euroscepticism Becoming Mainstream?' [2017] Euroscepticism, Democracy and the Media

do not feel that they had a lot of agency in making the rules: *I do not think that I had any influence here. And if I did, I did not know about it at all.* Findings like these are shed a critical light on the 'citizen participation' rhetoric of the European Union. According to Art. 10(3) of the TEU, '[e]very citizen shall have the right to participate in the democratic life of the Union. Decisions shall be taken as openly and as closely possible to the citizen'[38]. Maybe Flear and Vakulenko are right when they critically observe: 'the stress on participation … seems more like an education initiative' with the goal to instil trust and a feeling of legitimacy among the laymen in the expertise of the experts drafting the laws[39]. But as the responses in our survey showed, data concern everyone – both as data subjects *and* as active data users themsevels – and the perceived lack of a democratic deficit has direct repercussions for the general acceptance of rules that were designed to 'empower' people.

Apart from this general feeling of being imposed rules that are meant to improve the position of the individual, a certain level of frustration or even injustice can be discerned. A small number of respondents felt that the GDPR had a disproportionate scope. For instance, they felt that *It goes too far and is simply not workable for many organizations. This should have been better thought of.* and that *The GDPR goes bit too far: it also impacts 'normal' social relations.* At the same time, the results show that the Regulation negatively affected respondents both in their professional (14 %) and personal lives (13 %). In professional life, respondents who worked in different sectors felt that the regulation negatively influenced their daily work: *I work in a school and we cannot even take pictures of the kids on a trip any more* or *I cannot make a test copy of production database any more. The rules are so invasive because they hinder routine operational processes.* In their private life on the other hand, they expressed that *They make a fuss even about a picture on the sport field* and *You come across the GDPR in then most unexpected places. For example, the library. When you want to reserve a book, you cannot do it on your name any more, but you need to know your library ID number. Odd!*

While this perception of negative consequences cannot be solely attributed to the GDPR (also before GDPR data protection rules applied, and applied to individuals as well), it is with the introduction of the GDPR that many people seemed to have become aware of the fact that data protection law does not only apply to companies, but to individual users, too. At the same time, in order to understand the perceived negative influence on social contacts and

---

[38] See also" Commission of the European Communities, 'European Governance. A White Paper' [2001]
[39] M Flear and A Vakulenko 'A Human Rights Perspective on Citizen Participation in the EU's Governance of New Technologies' 10(4) Human Rights Law Review, 676

personal lives of individuals, it is important to remember that data protection frameworks, and the GDPR in particular, are not designed to regulate individuals. Instead, these frameworks have traditionally been designed to regulate the (data-processing) operations of governmental and commercial institutions[40]. The so-called household exception, defining situations in which private individuals that process personal data are exempted from the GDPR's regime, is very limited in scope[41]. The result is that very often, individuals might be considered data controllers in their own right, and thus subject to the many obligations in the GDPR – a situation that has been argued to impose disproportionate burdens on users. This is also substantiated by some of the reactions in our study, with respondents stating that: *A complex set of rules that is difficult to understand and comply with for almost all companies, but completely unworkable for individuals in hobby clubs etc.* Although not a new realization, the findings from this study highlight the urgency for further research into the position of individual users under data protection law. The question arises how to apply the necessary level of differentiation between digital citizens, collecting and sharing data as part of everyday life, and (large) commercial organisations whose entire business model revolves around the processing personal data. Such differentiation could either take place on the level of enforcement, or would require additional legal clarification. In recent years, the Court of Justice has married a narrow interpretation of the household exemption (with most individuals being considered controllers), with a flexible interpretation of the ensuing obligations imposed on the individuals (as data controllers). This approach prevents under-inclusion (e.g., a wide interpretation of the household exemption might effectively exempt problematic processing operations), while at the same time compensating for the risks of over-inclusion (e.g., trivial processing operations falling within the GDPR's scope).[42]

VI. Further reflection

Apart from informing the operationalisation of regulators' mandate under the GDPR (Art.57), the insights into individuals' knowledge and perceptions of the GDPR also enable more theoretical reflections on the sharing of data in today's digital society. Notably, we consider the findings to highlight the need to critically revisit and engage into further

---

[40] Brendan Van Alsenoy, 'Data Protection Law in the EU: Roles, Responsibilities and Liability' [2019] 3(1) Journal of Data Protection & Privacy

[41] Natali Helberger and Joris Van Hoboken, 'Little Brother is Tagging You-Legal and Policy Implications of Amateur Data Controllers' [2010] 4 Computer Law International

[42] Jef Ausloos, 'The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection' [2020] Oxford: Oxford University Press

research on the so-called 'privacy paradox'. The privacy paradox is the idea of a dichotomy between information privacy attitude and actual information privacy behaviour[43]. It assumes that on the one hand, individuals are concerned about their informational privacy and show desire to protect it by e.g., using individual rights, while on the other hand, they voluntarily disclose information online and rarely make use of their rights. In the literature, there have been various attempts to explain the paradox, including resignation[44] or privacy cynicism[45]. An alternative explanation, that is at least hinted at in our findings, is that there is no paradox at all: people are aware of privacy and its importance, they are also aware of the rights they have, but in our digital society using and sharing data has become such an integral part of our life, that their 'choice' is not a real one. In fact, people choose to share data because it forms an inherent part of their daily life. These intial conclusions call into question if the decisions made by individuals when sharing data are paradoxical, or rather simply reflect their needs in a highly 'datafied' society. Further research on individual attitudes and privacy behaviour is needed to further explain the effect of lack of choice on user privacy behaviours.

Seen in this light, arguably the concerns about the GDPR identified here should not only be read as individualistic concerns (namely regarding the obligations for individuals to comply with the rules and limitations to what they can do with data, and the respective inconvenience of complying with the GDPRs requirements). They most importantly hint at a broader, societal concern: data permeates every aspect of our lives, our environments and society more broadly. In the digital, highly mediatized and constantly connected society users face 'new pressures to perform [them] self online in order to just function as a social being'[46]. The sharing of data and the leaving of digital traces becomes a constituting element of living as a digital citizen, and engaging in social, political and economic practices[47]. From this also follows that any rules affecting the way in which data can be processed will necessarily have an impact on individuals as well. Whether it is only perceived or not, curbing individuals' rights to collect and share data has repercussions for what it means to be, and behave as a

[43] Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' [2005] 3(1) IEEE security & privacy
[44] Nora Draper, 'From privacy pragmatist to privacy resigned: challenging narratives of rational choice in digital privacy debates' [2017] 9(2) Policy & Internet; Joseph Turow, Michael Hennessy and Nora Draper, 'The trade off fallacy: How marketers are misinterpreting American consumers and opening them up to exploitation.' [2015] SSRN Electronic Journal
[45] Christian Pieter Hoffmann, Christoph Lutz and Giulia Ranzini 'Privacy cynicism: A new approach to the privacy paradox' [2016] 10(4) Cyberpsychology: Journal of Psychosocial Research on Cyberspace
[46] Nick Couldry and Andreas Hepp 'The mediated construction of reality.' [2018] John Wiley & Sons 60
[47] José van Dijck 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology' [2014] 12(2) Surveillance & Society

digital citizen. Against the findings from our study, recital 4 of the GDPR must be read in a new light: 'The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.' While a high level of protection of personal data is warranted, we cannot expect any actor in society to have the same responsibility in safeguarding that right. As has been said many times before, in a society where data is everywhere, and everyone has become a potential 'data controller' subjected to the GDPR, it is vital to clearly delineate the different roles and responsibilities. Our study emphasises that, even if there is consensus (among courts, DPAs, etc.) on the allocation of responsibilities – e.g. the light-touch enforcement regarding individual data controllers versus commercial companies – it is critical to also clearly communicate this to society at large. While experts would agree that some of the frustrations identified in this study are often unwarranted, this is not clear to the general public. These frustrations are in fact a clear signal that there is still much to be done on informing the public. Even if the GDPR legislator's intention was not to regulate the day-to-day behaviour of individual citizens – nor is it a priority for many data protection authorities – there are still a lot of frustrations among individuals on this perceived regulatory burden. Any effort going forward should therefore also incorporate a strategy to reverse that perception, which – as argued by the Protection Motivation Theory – will in turn contribute to increased perceived effectiveness of the Regulation and higher agency of individuals. The move towards a digital economy has digitised our lives, social relations and daily routines, and the sharing of data is deeply engrained in our digital culture. Imposing a legal framework to protect personal data without a deep understanding of the function of data in society does not work for users and leads to frustrations and unintended consequences among the public.