Exploring data subjects' knowledge on the rights GDPR guarantees: an exploratory research in Greece

Maria Sideri*

Privacy Engineering and Social Informatics Laboratory,
Department of Cultural Technology and Communication,
University of the Aegean,
GR 81100, Lesvos, Greece
Email: msid@aegean.gr
*Corresponding author

Stefanos Gritzalis

Laboratory of Systems Security,
Department of Digital Systems,
University of Piraeus,
GR 18534, Piraeus, Greece
Email: sgritz@unipi.gr

Athanasios Fontaras

e-Governance Department,
National Centre for Scientific Research "Demokritos",
GR 15310, Athens, Greece
Email: a.fontaras@egov.demokritos.gr

Abstract: In a data driven era, the implementation of the General Data Protection Regulation in the member-states of the European Union signals enforceable rights for data subjects attributing them more control over their data. However, the actual protection of personal data and natural persons' freedoms does not depend only on the legal framework, but relies also on data subjects' rights knowledge highlighting thus the individual responsibility for personal data protection. In the frame above, this exploratory research investigating the knowledge of a Greek adults group regarding the rights GDPR guarantees reveals fluctuations in rights knowledge related to the information sources on GDPR, data subjects concerns and the socio-demographic characteristics of the participants. The research findings highlight the need for data subjects to have more information on GDPR and become fully aware of their rights in order to protect their data.

Keywords: general data protection regulation; data subjects; rights knowledge; concerns; demographic characteristics; information sources; awareness; Greece.

Reference to this paper should be made as follows: Sideri, M., Gritzalis, S. and Fontaras, A. (2022) 'Exploring data subjects' knowledge on the rights GDPR guarantees: an exploratory research in Greece', *Int. J. Electronic Governance*, Vol. 14, Nos. 1/2, pp.28–57.

Biographical notes: Maria Sideri holds a PhD from the Department of Social Anthropology and History (University of the Aegean) and an MSc on gender issues. She teaches in the Department of Cultural Technology and Communication of the University of the Aegean and she is a Member of the Privacy Engineering and Social Informatics (PrivaSI) Laboratory. Her research interests focus on social media and privacy issues, social networks in social media, social media and digital identity construction, social media effects on human behaviour, politics and social movements in social media, diversity and social cohesion and intercultural communication.

Stefanos Gritzalis is a Professor in the Department of Digital Systems (University of Piraeus) and the Director of the Postgraduate Programme "MSc in Law and ICT". He was the Rector of the University of the Aegean (2014–2018) and has acted as Special Secretary for the Hellenic Ministry for Administrative Reform and Electronic Governance (2009–2012). His scientific work includes more than 10 books, 34 book chapters, 316 papers in refereed journals and proceedings of international conferences and workshops. He is Area Editor for the "IEEE Communications Surveys and Tutorials" journal and Editor-in-Chief or Editor or Editorial Board member in 35 journals.

Athanasios Fontaras received his degree in Mathematics from the University of Patras (Greece) and his MSc in Social Information Systems from the Open University of Cyprus. He works at the E-Government Office in the National Centre for Scientific Research 'Demokritos' (Greece) being the Computer Systems Manager and acting as the Head of the Users Assistance Office.

This paper is a revised and expanded version of a paper entitled 'What do we know about our rights to data protection? A Greek case study' presented at *8th International Conference on e-Democracy: Safeguarding Democracy and Human Rights in the Digital Age*, Athens, Greece, 12–13 December, 2019.

1 Introduction

In Information Society, the protection of privacy and the security of personal data confront new challenges. The global penetration of internet, the increasing usage of social media platforms, cloud services, mobile and wearable devices by citizens and the crowdsourcing models exploited by governments or companies have led to the collection of personal data in a volume and form that in the past would have been difficult to gather. This evolution creates new opportunities for public and private sector operators to process personal data with specialised techniques for a variety of goals, while data are transmitted and exchanged between different actors, agencies and states worldwide. Thus, a risky situation emerges for social subjects and several threats come up regarding personal data protection and human rights.

The strengthening of data protection legislation is considered over time very important for the regulation of data collection technological planning and data control (Buschel et al., 2014). In Europe, several legal documents regarding data protection have been produced since 1980s, while the Directive 95/46/EC was implemented in all member-states of the European Union (EU). Despite the legal measures taken, countries differentiated in their legal culture and practice (Mitrou, 2002; Sobolewski et al., 2017;

Custers et al., 2018). In other words, states used different definitions for personal data and applied different rules throughout data processing until recently. This situation generated challenges for data safeguarding, which the General Data Protection Regulation (GDPR) is expected to confront by further harmonising both legislation and legal practices between EU member-states.

GDPR (EC, 2016) is applicable to all EU member-states since May 2018, having replaced Directive 95/46/EC. Following a human-centric approach, the Regulation gives data subjects a set of enforceable rights aiming to increase data subjects' control over personal data and to ensure data transparent and safe processing regardless the format used (online or paper). Simultaneously, GDPR introduces a stricter framework regarding data controllers' obligations emphasising on regulatory compliance monitoring measures too. The monitoring of GDPR implementation and the control of compliance is supervised in each EU member-state by one or more independent public authorities called 'Supervisory Authority' that cooperate throughout the Union.

Beyond legislation, data subjects' vigilance for personal data protection as well as knowledge about their rights are equally significant. Although the concerns regarding personal data protection and privacy safeguarding grow worldwide and legal measures are taken at national and supranational level, citizens are not always fully aware of the relevant legislation, their rights and the actions they should take for protecting personal data (Surveillance Project, 2008; Mantelero, 2014). Ignorance regarding data protection legislation or misunderstanding of rights is expected to make data subjects more vulnerable to anyone (public or private sector agency) who seeks to process personal data. In this context, considering that in a data-driven society those who control personal data exert power over social subjects' lives in multiple ways, the necessity to investigate whether data subjects are aware of data protection legislation and thus able to protect themselves is critical.

In this context, an exploratory research aiming to investigate the knowledge regarding the right to data protection took place in spring 2019, in Greece. Specifically, the research explored the knowledge of a Greek adults group regarding the rights GDPR guarantees and the provisions of the Regulation for the collection and processing of personal data. Research results reveal fluctuations in rights knowledge, which can be associated mainly with the source of information on GDPR, less with privacy concerns and lesser with other factors. The findings highlight thus the need for more information on GDPR and give prominence to the necessity for future research in other European countries.

The paper is organised as follows. Section 2 refers to the research framework highlighting also the importance of data subjects' knowledge regarding data protection right. Section 3 records and discusses the results of the research, while Section 4 concludes the paper raising future research directions.

2 Research framework

2.1 Related work and scope of the research

Several events that data subjects experience or are informed about ranging from personal data breaches to personalised advertisements, increase their concerns regarding data protection. Nevertheless, data subjects keep sharing different types of personal data with

public authorities or private companies, consciously or unconsciously. Moreover, data subjects often think they can control the data they share, ignoring that others control their data now (Conger et al., 2013; Mantelero, 2014). This situation becomes more complicated when data subjects are shown to be unaware of data protection laws and/or in cases they believe that others protect their data (e.g., governments or service providers) (Surveillance Project, 2008; Kelley et al., 2013; Mantelero, 2014).

In this context, the knowledge that individuals have about their rights and the legislation for data and privacy protection is extremely important. In fact, data subjects' knowledge of technical aspects and data collection practices exploited by organisations and service providers, knowledge about legislation, legal aspects of data protection and protection policies and strategies as well as knowledge about personal rights can help data subjects to make informed decisions to control their data and take appropriate actions to protect themselves (Park, 2011; Trepte et al., 2015).

Data subjects' knowledge about their rights and the legislation regarding data protection as well as about the role of public Authorities or service providers has been studied before GDPR (Kelley et al., 2013; Miltgen and Peyrat-Guillard, 2014; Trepte et al., 2015; EC, 2015). Referring to the period after the implementation of GDPR, to the best of our knowledge there was no relevant research in Greece or EU exploring data subjects' awareness of the rights GDPR guarantees up to the date our research began. Special Eurobarometer 487a is the first official survey, published in June 2019 (EC, 2019), exploring awareness of GDPR and the rights it sets, specifically the right to access, correct, and have personal data deleted, data portability right, right to object to receive direct marketing and right to have a say when decisions are automated.

The investigation of knowledge extent on GDPR rights is an essential need not only considering Park (2011) and Trepte et al. (2015) arguments about the importance of data subjects' knowledge, but also acknowledging that data protection and privacy preservation presuppose both individual and collective responsibility, while their infringement seriously affects natural persons and societies (Sideri and Gritzalis, 2020). Data subjects are granted with enforceable rights in the frame of GDPR and this is not a typical act of the EU legislators but a crucial step for data subjects to have more control over their data. The success of GDPR does not rely only on the monitoring of its implementation and the control of compliance, but relies also -and mainly- on data subjects' behaviour regarding data protection. In this frame, data subjects' knowledge on the rights GDPR guarantees should be studied, since knowledge can drive behaviour. Acquiring insights on data subjects' rights knowledge is essential in order for national and European authorities to take remedial measures to enhance citizens' awareness and knowledge regarding data protection, if necessary.

In this frame, our exploratory research aimed to investigate a group of Greek data subjects' extent of knowledge regarding GDPR rights, while also exploring other issues related to data protection. Comparing to Eurobarometer 2019 (EC, 2019) our research included several items addressing to data subjects' right to be informed and data subjects' consent. The right to information fits in the first stage of processing timeline being linked to consent which is valid only if it is informed (van Ooijen and Vrabec, 2019), while consent is the very first decision that data subjects make.

2.2 Research tool and methodology

A four-section structured questionnaire (Appendix) measuring the extent of knowledge, the behaviour and views of the participants regarding data protection was used for the research carried out from 18 March to 18 April 2019. This form of questionnaire contributes to the standardisation of analysis making conclusions drawing easier.

Section A: General Data Protection Regulation. The 4 items explore issues regarding respondents' source of information on GDPR and their knowledge on GDPR objectives.

Section B: The rights of the data subjects. This section includes 14 items exploring respondents' extent of knowledge regarding GDPR rights. The questions were selected in order to cover the most important legal provisions of GDPR excluding special cases that would be probably confusing.

Section C: Risks for personal data and ways of protection. This section is divided into two sub-sections; the first (*Personal Data Control and Risks*) (10 items) addresses to respondents' perceived control over personal data, privacy concerns and perceived risks, while the second (*Personal Data Protection*) (7 items) explores respondents' practices and views regarding data protection. Question A.4 and several questions in sub-Section C1 (2-5 and 8-10) and C2 (1-6) have been drawn from a previous survey (EC, 2015).

Section D: Personal information. The four questions record respondents' demographic and social characteristics (gender, age, education level, employment).

In order to calculate the reliability of the scale regarding data subjects' knowledge about their rights (questions B1-14) Cronbach's Alpha reliability index was used ($a = 0.937$). The same index was used for privacy concerns (questions C.1.3-7) ($a = 0.786$) and for respondents' views on data protection (question C.2.7a-f) ($a = 0.852$).

Considering that the number of Greek potential research population (adults using digital services) is big, the sample was selected using convenience sampling method (Babbie, 2011; Zafeiropoulos, 2015). In other words, participants were recruited based on their availability and willingness to participate in the research. Although this non-probability method does not allow the generalisation of the research results, it is extremely helpful for pilot studies, exploratory researches and hypothesis generation, while the results can highlight future research trends. Questionnaire design followed the rules set by Javeau (1996). The participants were clearly informed about the research purpose in the introductory note (Babbie, 2011) being asserted about their responses' anonymity.

The questionnaire was checked for its language, clarity, difficulty and validity in a pilot survey addressed to 10 participants. This stage is important since it detects

a if the questions are understood

b if they ensure the information for which they were designed

c the interest and cooperation of the respondents (Oppenheim, 1992).

After the pilot implementation, the questionnaire was corrected receiving its final form and was implemented in Google forms. Data collected online were analysed using IBM SPSS 21.

3 Results and discussion

This section presents new findings from further statistical analysis of the research data. These findings refer to concerns impact on the extent of data subjects' rights knowledge and the impact that rights knowledge and privacy concerns have on data subjects' views about data protection. Results from previous analysis (Sideri et al., 2020; Sideri and Gritzalis, 2020) being in many cases further elaborated are also presented in order for the readers to have a better insight to the research findings. Previous findings refer mainly to data subjects' extent of knowledge per right, data protection practices and the impact of the demographic characteristics and information sources on rights knowledge.

One hundred one people participated in the research. The demographic data are presented in Tables 1–4.

Table 1 Participants' gender

Valid	Men	48.5 (n = 49)
	Women	50.5 (*n* = 51)
Missing		1 (*n* = 1)
Total		100.0 (*n* = 101)

Table 2 Participants' age

Valid	18–25	5.9 (*n* = 6)
	26–35	25.7 (*n* = 26)
	36–45	49.5 (*n* = 50)
	46–55	15.9 (*n* = 16)
	>56	3.0 (*n* = 3)
Total		100.0 (*n* = 101)

Table 3 Participants' educat. level

Valid	Primary school	0 (*n* = 0)
	Secondary sch	15.8 (*n* = 16)
	University	38.6 (*n* = 39)
	MSc	42.6 (*n* = 43)
	PhD	3.0 (*n* = 3)
Total		100 (*n* = 101)

Table 4 Participants' employment

Valid	Public sector employee	36.6 (*n* = 37)
	Private sector employee	31.7 (*n* = 32)
	Freelancer	17.8 (*n* = 18)
	Teacher	2.0 (*n* = 2)
	Student	8.9 (*n* = 9)
	Other	3.0 (*n* = 3)
Total		100 (*n* = 101)

3.1 Section A: General Data Protection Regulation

Participants were asked to state (A.1) the source of their information on GDPR. Not surprisingly, the majority was informed by internet (44.5%), 13.9% by mass media, 16.8% by another person, while 24.8% stated being informed because of personal interest/engagement on the topic. Mass media as a source of information and information by someone else were stated more by women than men, while the opposite was recorded for information by internet and personal interest on GDPR.

Question A.3 was posed to respondents in order to identify GDPR objective having the choice of multiple answers:

a data subjects' rights strengthening

b obligations increase of entities collecting and managing data

c stricter delimitation of data collection and processing procedures

d tighter regulatory compliance control measures.

Considering that "Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (EC, 2016, article 1, par. 2), data subjects' rights enforcement is GDPR's priority in order for data subjects' control over their data to be increased. Referring to GDPR, van Ooijen and Vrabec (2019) note that "the need for individual control seems to be addressed more explicitly and with greater prudence compared to earlier regulations" (p.92). According to our results, 17.8% of the participants stated that GDPR addresses to (c). Option (a), (b) and (d) was selected by 5%, 2% and 5% of the respondents respectively, all options by 21.8%, while combinations of answers were recorded in lower rates (from 1% to 9.9%). These findings reveal that GDPR is considered as a legal framework referring more to data controllers and their obligations than to data subjects and their rights.

3.2 Section B: the rights of data subjects

To protect personal data, data subjects must know their rights in order to exercise them, along with the individual privacy protection strategies they may employ when interacting online. Respondents were asked to self-assess the extent of their knowledge about GDPR rights using a 5-point scale, from 1 'not at all' (absence of knowledge) to 5 'very well' (excellent knowledge). This scale was used in all questions with the exception of B.13 and B.14 that explore knowledge regarding the conditions for the exercise of the right to be forgotten and the right to data processing restriction.[1] In order to compare the results of these two questions measured in nominal scale with the previous (B.1-12) measured in ordinal, we assumed that those having chosen

i all four replies in B.14 accomplish a score of 5

ii three replies a score of 4

iii two a score of 3

iv one a score of 2.

Regarding question B.13, a 4-point rating scale was used. Thus, participants who had chosen

i all the suggested replies achieve a score of 4

ii two of the replies a score of 3

iii one reply a score of 2.

The 'don't know' reply was assessed for both questions as equivalent to 'not at all' (score 1). The results regarding the extent of knowledge for each of the rights are presented in Table 5.

Table 5 Data subjects' extent of knowledge per right

		Not at all (1)	*Little (2)*	*Mode-rate (3)*	*Well (4)*	*Very well (5)*	*Mean*	*Std. dev.*
Right to be Informed about	Data processing and subject's rights (B.1)	9.9	10.9	23.8	28.7	25.7	3.50	1.26
		20.8			*54.4*			
	Data used for profiling and consequences (B.7)	14.9	19.8	19.8	29.7	14.9	3.10	1.30
		34.7			*44.6*			
	Data transmission to third party (B.8)	18.8	19.8	17.8	20.8	21.8	3.07	1.43
		38.6			*42.6*			
	High-risk pers. Data breach, consequences, measures taken (B.9)	18.8	20.8	19.8	18.8	21.8	3.04	1.42
		39.6			*40.6*			
Consent	Required for data use (B.3)	5.0	9.9	9.9	27.7	46.5	4.02	1.19
		14.9			*74.2*			
	Form (free, specific…) (B.4)	7.9	7.9	23.8	36.6	23.8	3.60	1.16
		15.8			*60.4*			
	Withdraw (B.5)	18.8	11.9	21.8	17.8	26.7	3.22	1.46
		30.7			*44.5*			
	Not required for service usage (unless necessary for service provision) (B.6)	16.8	16.8	28.7	20.8	15.8	3.02	1.31
		33.6			*36.6*			
Right to Oppose	To data processing (incl. Profiling) (B.10)	13.9	25.7	21.8	23.8	13.9	2.98	1.27
		39.6			37.7			
	(not to be subjected) to automated decision (B.11)	17.8	28.7	25.7	15.8	10.9	2.73	1.24
		46.5			26.7			
Right to data rectification (B.2)		10.9	10.9	30.7	26.7	18.8	3.32	1.22
		21.8			*45.5*			
Right to data portability (B.12)		29.7	23.8	14.9	22.8	7.9	2.55	1.34
		53.5			30.7			
Right to be forgotten (B.13)		22.8	29.7	32.7	14.9		2.39	1.00
		52.5						
Right to data processing restriction (B.14)		29.7	19.8	21.8	18.8	9.9	2.60	1.34
		49.5			28.7			

Results show that only in the case of question B.1 more than half of the respondents (54.4%) were 'well' and 'very well' aware of the right to be informed by data controller within a reasonable time for the processing their data will be submitted and their rights. In all other cases of information provided to data subjects, the respective rates range between 40.6% (B.9) and 44.6% (B.7). This is worrying as data subjects were expected to be more aware of their right to be informed about data breaches and potential consequences (B.9) or about data transmission to third party (B.8) due to often expressed related concerns. Regarding question B.7, it is interesting that 34.7% of participants did not know or knew this right 'little', which may imply that either they ignore profiling as a technique used for which they should be informed or they consider profiling as a normal practice.

Referring to consent, it is notable that although the percentage of respondents who knew 'very well' and 'well' that consent is required for personal data processing (B.3) is high (74.2%), the corresponding percentage regarding the right to withdraw consent at any time is much lower (44.5%), as findings in B.5 show. This may imply that respondents believe that once they have given their consent, they have little or no legal ability to withdraw it. On the other hand, regarding the form of consent (B.4) the majority of the respondents had at least a moderate knowledge about the form that consent must be provided. People often think that their consent is a prerequisite for services provision, although Poullet (2018) argues that consent is a false precondition for specific social needs (e.g., internet access or search engines and social networks usage). In this frame, the results of question B.6 are rather promising revealing a trend about users gradually acknowledging that consent is not a prerequisite for using a service.

Questions B.2 and B.12 respectively refer to data subjects' right to ask data controller to rectify incorrect personal data without undue delay and the right to receive personal data delivered to a controller and transfer them to another. Respondents' replies in B.12 reveal that more than half of the participants (53.5%) knew 'little' or 'not at all' the data portability right, which is one of GDPR innovations. The failure of users to recognise the importance of data portability is crucial for the effective implementation of GDPR (Sobolewski et al., 2017) since this right increases users' control over their data. Moreover, this right constitutes an opportunity for services interoperability and increased competition between digital services (De Hert et al., 2018). Nevertheless, respondents seemed to be more aware of the right to data rectification (B.2).

Questions B.10 and B.11 refer to data subjects' right to object, on grounds relating to their particular situation, at any time, to the processing of personal data concerning them including profiling and their right not to be subjected to a decision taken solely on the basis of automated processing by which personal aspects that concern them are assessed, producing effects that affect them (e.g., legal effects). Results show that the cumulative percentages for 'well' and 'very well' replies were low in both cases, and much lower for the right not to be subjected to a decision taken, solely based on automated processing (26.7%). Poullet (2018) argues that the regulation of the right to object to data processing in the frame of GDPR is not satisfactory for the effective protection of data subjects. She highlights that it is not enough to apply so that profiling will not happen again or to resist a decision taken solely on automated processing basis, but what is necessary for data subjects is to understand the criteria taken into account for the profile creation, the data and the algorithm used. GDPR determines the information about algorithms but this happens only in advance with reference to the functionality of the system rather than ex-

post that would help data subjects to be informed about the logic and the decision criteria (van Ooijen and Vrabec, 2019).

Both the right to be forgotten (B.13) and the right to data processing restriction (B.14) are of significance, considering that the first effectively eliminates the possibility of uncontrolled digital reproduction of personal data and increases subjects' control over the flow of their data (van Ooijen and Vrabec, 2019), while the second is important in cases when the first cannot be applied. The percentages for the 'well' and 'very well' replies in both cases of rights were shown to be low.

The mean for the total score of data subjects' rights knowledge is estimated at 42.75 (std. dev. = 13.07), with a minimum and maximum observed value of 14 and 68 respectively, revealing thus that data subjects' extent of knowledge regarding GDPR rights is rather moderate in general.

3.3 Section C: risks for personal data and ways of protection

Beyond rights knowledge, data subjects' awareness regarding the way that others manage their data and the risks potentially arising from this management is significant. The first two questions of subsection C.1 refer to data control. Respondents were asked to declare how sure they are about controlling the personal data they provide online (C.1.1), and to state the extent of control they feel having over the information they provide online (e.g., the ability to correct, change or delete this information) (C.1.2). Results for both questions are presented in Tables 6 and 7. Van Ooijen and Vrabec (2019) define individual control as "the extent to which an individual is consciously aware of a situation and has the conscious intention and the ability to start, stop or maintain a situation" (p.93). The perception of control is crucial as it may lead to either a sense of security and thus greater disclosure of information or high privacy concerns and consequently reduced willingness to disclose information even in cases where the risks from the disclosure are lesser (Brandimarte et al., 2012). Brandimarte et al. (2012) differentiate between two processes -the process of information disclosure and the process of information access, use or misuse of information- noting that people fail to think that the resulting cost regarding data control depends on access and use or misuse of information, as they focus on the first level of control (information release). In this frame, the inconsistency revealed between the replies in the questions above demonstrates that respondents can distinguish between the two processes, acknowledging that after data provision these are no longer under their control as supported by Conger et al. (2013).

Table 6 Control of personal data provided online

		Control certainty
Valid	Absolutely sure	12.9 (n = 13)
	Quite sure	39.6 (n = 40)
	Not really sure	33.7 (n = 34)
	Not sure at all	13.9 (n = 14)
	Don't know	0 (n = 0)
Total		100 (n = 101)

Table 7 Feel controlling information provided online

		Feeling of control
Valid	Complete control	3.0 (n = 3)
	Partial control	55.4 (n = 56)
	No control at all	19.8 (n = 20)
	It depends	15.8 (n = 16)
	Don't know	5.0 (n = 5)
Missing		1.0 (n = 1)
Total		100 (n = 101)

Questions C.1.3 to C.1.7 explore data subjects' privacy concerns on specific issues. Hong and Thong's (2013) four large-scale empirical studies have focused on internet privacy concerns in particular, acknowledging that previous researches showed significant differences in the conceptualisation and measurement of information privacy concerns and internet privacy concerns. The results of their studies have led to a conceptual model that "contains two second-order factors of interaction management and information management, and six first-order factors of collection, secondary usage, errors, improper access, control, and awareness". Moreover, the researchers highlighting the need for consistent measures of internet privacy concerns dimensions have focused on "individuals' perceptions of their concerns for others' behaviour rather than their expectations of others' behaviour" (Hong and Thong, 2013, p.293). Building upon these findings and drawing items from Eurobarometer 2015 (EC, 2015), respondents were asked to state the extent of their concerns about

a others having control over the information data subjects provide online (C.1.3)

b governmental agencies collecting personal data on a large scale for national security purposes (C.1.4)

c public and private actors using personal data for different purposes than those initially collected without informing users (C.1.6)

d search engines such as Google recording the websites users originated from and the ones they visit (C.1.7).

Moreover, they were asked to state how comfortable they feel about companies' websites using information regarding their online activity to create content that suits their preferences (e.g., personalised ads) (C.1.5). Results are presented in Table 8 after having reversed respondents' scores in C.1.5 in order to comply with concerns measurement. High concerns were shown in all cases. Specifically, 70.2% of the respondents stated 'very concerned' and 'quite concerned' for case C.1.4, 89.1% for C.1.6, the same percentage for C.1.5, 83.1% for C.1.7 and 82.2% for case C.1.3.

The mean for the total score of data subjects' concerns is quite high (15.38) (std. dev. = 2.91) with a minimum and a maximum observed value of 6 and 20 respectively.

Table 8 Respondents' concerns extent

		Others control information provided online (C.1.3)	*Gover. Agencies collect personal data (C.1.4)*	*Companies websites use personal information (C.1.5)*	*Data used for different reasons than those collected (C.1.6)*	*Search engines record navigation history (C.1.7)*
Valid	Don't know	1.0	1.0		1.0	3.0
	Not at all	2.0	5.0	1.0	3.0	4.0
	No particularly	14.9	22.8	9.9	6.9	9.9
	Quite	67.3	48.5	40.6	49.5	55.4
	Very	14.9	21.7	48.5	39.6	27.7
Missing			1.0			
Total		100.0	100.0	100.0	100.0	100.0
Mean		2.93	2.86	3.36	3.23	3.00
Std. dev.		0.68	0.85	0.70	0.79	0.90

Respondents declared their worries regarding the possibility their personal data to be lost or stolen (C.1.8) and acknowledged risks when providing personal data (C.1.10) focusing on security issues ("personal safety being at risk" 74.3%) and personal data usage for fraud ("becoming a victim of fraud" 76.2% and "online identity used for fraudulent purposes" 77.2%). Personal data usage without data subjects having been informed (63.4%) and data transmission to third parties without subjects' consent (64.4%) were also stated as risks. Misunderstanding of views and behaviour (37.6%) and personal data usage for sending people unwanted advertising material (34.7%) were recorded at lower rates.

Sub-section C.2 explores data subjects' practices regarding data protection. Information about personal data processing is crucial in order for data subjects to make informed decisions about their data. Providers can supply this information through privacy policies, but data subjects may encounter problems in understanding the information. Literature has shown that data subjects often do not read privacy policies and this is a risky behaviour (Marwick et al., 2010). The findings in question C.2.1 show that only 6.9% of the participants read the whole privacy policy text, 64.4% stated 'partially' and 28.7% declared not reading at all. The low reading rate is due to the extent of the text (73.4%) and the complexity including the use of technical terms (55.4%) as responses in C.2.2 reveal, supporting previous researches (Proctor et al., 2008; Cadogan, 2011). Furthermore, 21.8% of respondents stated as a reason for not reading or partially reading privacy policies that "websites will not honor them anyway" showing thus lack of trust to providers. On the contrary, 13.9% declared that it is sufficient for them to see that websites have a privacy policy, which implies users' confidence to providers. The latter supports Hoofnagle and Urban (2014) findings having shown that participants consider that the existence of privacy policy in a website would not allow the sharing of personal information without their permission. Such a view reduces privacy concerns and increases disclosure behaviour. Only 2% stated that they did not know where to find the

privacy policy, 4% that they did not think it is important to read it and 8.9% that law will protect them in all cases.

Participants were asked to reply to question C.2.3 "Who will you address to if you have a problem regarding the protection of your personal data?" having the option of multiple choices. This question and the proposed answers were all retrieved from a previous survey (EC, 2015). Data subjects' knowledge regarding to whom they should address is an indication that they understand their right to legal remedies exercise. The results showed that 11.9% of the participants did not know where to address to and 1% stated that it would not address anyone. The 'Regulatory Authority' option was selected by 28.7% and the "Independent Authority for the Protection of the Data Subject" by 10.9%. At lower rates, respondents chose "Authority or private body that handles my data", 'Court' and 'European Authority' (5.9%, 4% and 2% respectively), while a combination of answers was also recorded. Acknowledging at first that the question is rather broad pertaining to a very wide range of problems the perception of which may differ between respondents based on their experiences and secondly that the proposed answers are probably confusing since one should distinguish between the responsibilities of different entities according to a specific problem, future research should focus on scenarios regarding data protection problems in different cases in order to investigate whether people can identify the appropriate Authority to address to and complain.

In the next three questions (C.2.4-C.2.6), data subjects' practices with reference to

a providing consent

b right to be informed

c right to data portability were explored.

All three issues were carefully selected; consent is the very first decision that data subjects make, right to be informed is the fundamental condition for data subjects to make informed decisions being able to give their consent or opt out if consent is required for processing, while the right to portability is a new right that increases data subjects' control over their data. The results for these questions are presented in Tables 9–11.

Table 9 Explicit consent for any kind of personal data to be collected and processed

		Explicit consent (C.2.4)
Valid	Yes, in all cases	18.8
	Yes, in case of online data	18.8
	Yes, in case of sensitive data	15.8
	No	20.8
	Not sure	24.8
	Total	99.0
Missing		1.0
Total		100.0

Table 10 Information on the conditions of data collection and processing when asked to provide data online

		Information provided (C.2.5)
Valid	Always	4.0
	Sometimes	37.6
	Rarely	39.6
	Never	10.9
	Not asked to give data online	2.0
	Don't know	5.9
Total		100.0

Table 11 Evaluation of the data portability right importance

		Data portability (C.2.6)
Valid	Very important	38.6
	Quite important	38.6
	No particularly important	18.8
	Not important at all	2.0
	Don't know	4.0
Total		100.0

What is interesting is that the results recorded in the first two tables do not match with the high percentages of data subjects' self-assessment regarding the extent of knowledge about the right to be informed on their data processing and give their consent as recorded in previous questions. The data portability right is essential for enhancing data subjects' control constituting a first step towards the 'preselected ownership' of personal data (De Hert et al., 2018, p.201). Participants' replies (C.2.6) reveal that most of them recognised this right as 'very important' or 'quite important', despite the fact that, as recorded in question B.12, half of the respondents (54%) did not know or knew the right 'little'. According to a recent report on GDPR (EC, 2020), data portability right is not fully used yet so its "unlocking…is one of the Commission's priorities, in particular since, with the increasing use of 'Internet of Things' devices, more and more data are generated by consumers" (p.8).

The last question (C.2.7) includes 6 phrases with which respondents were asked to state their agreement/disagreement using a 5-point scale from 1 (totally agree) to 5 (totally disagree). These statements address to views and beliefs regarding data protection referring to data subjects, providers, law and Regulatory Authorities, and governments' role, using all positive expressions. Findings are shown in Table 12.

With none of the statements the rates of agreement/absolute agreement were higher than those of disagreement/absolute disagreement. The same was observed when comparing agreement/absolute agreement rates to 'neither agree nor disagree' rates with the exception of statement (e). The higher percentages of disagreement/absolute disagreement were recorded for statements (f), (a) and (c) showing that data subjects trust neither governments nor providers, while being conscious that their data can be exploited by others. The latter may explain the rather equal distribution of rates in the case of (e)

revealing respondents' uncertainty whether their careful behaviour when providing data is sufficient for their protection. Moreover, responses to statement (b) revealed that not more than 1/3 of the participants were sure they know the law to protect their data. Distrust towards legislation and Supervisory Authorities was recorded in statement (d).

Table 12 Percentage of agreement/disagreement on personal data protection statements

	Totally agree	*Agree*	*Neither agree nor disagree*	*Disagree*	*Totally disagree*
a) *I am confident that the personal data I provide will not be used by anyone else*	3.0	14.9	*28.7*	34.7	18.8
	17.90			*53.50*	
b) *I am aware of data protection legislation to protect myself*	1.0	25.7	*34.7*	24.8	13.9
	26.70			*38.70*	
c) *I trust service providers to protect my data*	2.0	14.9	*30.7*	36.6	15.8
	16.90			*52.40*	
d)*Legislation and Supervisory Authorities fully protect my personal data*	3.0	16.8	*39.6*	35.6	5.0
	19.80			*40.60*	
e) *To protect myself it is sufficient to be careful about the data I provide online*	9.9	22.8	*32.7*	25.7	8.9
	32.70			*34.60*	
f) *Governments protect my data*	3.0	10.9	*24.8*	42.6	18.8
	13.90			*61.40*	

Table 13 presents the mean per statement and in total. Considering that value 3 addresses to 'neither agree nor disagree' and 4 to 'disagree' a tendency to reject the positive statements is revealed.

Table 13 Mean value per respondents' statement and in total

Statement	*Mean*	*Std. dev*
(a)	3.51	1.05
(b)	3.24	1.02
(c)	3.49	0.99
(d)	3.22	0.89
(e)	3.00	1.11
(f)	3.63	1.00
Total	20.12	

3.4 More findings

Taking into account that the first research results (Sideri et al., 2020) revealed fluctuations in data subjects' rights knowledge, the impact of the demographic variables[2] and of information sources on rights knowledge extent was investigated (Sideri and Gritzalis, 2020). Eurobarometer 2019 (EC, 2019) explored whether participants had

heard each of the six rights investigated, but did not focus on the information source. Based on Custers et al. (2018) argument that differences have been recorded between EU member-states "in the intensity and scope of information campaigns, media attention, and public debate" regarding data protection (p.234), we assumed that knowledge extent may be related to some kind of expertise or the sources of information on GDPR.

Regarding the impact of the demographic variables on knowledge extent, our data analysis using Mann-Whitney test revealed that there is statistically significant difference between men and women regarding the form of consent [U(49,51) = 883.00, $p = 0.009$]. Women have a higher mean (3.88) than men (3.28), while the opposite was shown for the right to data processing restriction [U(49,51) = 959.00, $p = 0.040$] where men had a higher mean (2.91) than women (2.33). Age is shown to be negatively related at low degree to knowledge extent regarding the right to be forgotten (rho = –0.269, $p = 0.007$), revealing that as age increases the knowledge regarding all or most of the conditions for the exercise of the right decreases. Educational level is positively related at a low degree to consent withdraw (rho = 0.229, $p = 0.023$) and the right to data processing restriction (rho = 0.217, $p = 0.029$). Specifically, those holding a M.Sc./Ph. D. have a higher extent of knowledge for these rights. Kruskal-Wallis test showed that employment affects knowledge extent regarding the form of consent [$H(2) = 7.071$, $p = 0.029$] with students and others being in the higher mean rank (67.83).

On the other hand, information sources influence more rights knowledge extent. Specifically, those personally interested or engaged with GDPR showed unsurprisingly higher extent of knowledge regarding their rights, followed in all cases by those informed by internet. The ones informed by mass media are in the 3rd mean rank with the exception of the right to object to data processing, the right to data rectification, the data portability right and the right to have data deleted where those informed by someone else precede. No statistically significant relationships were shown for consent form (B.4), consent withdrawal (B.5), right to be informed for data transmission to third party (B.8) and for high-risk personal data breach (B.9).

Up to this point, our findings reveal that the fluctuations recorded in data subjects' rights knowledge are attributed mainly to the information sources and less to the demographic characteristics. Moreover, our research revealed data subjects' high concerns regarding the issues they had been asked for as well as a tendency for data subjects to disagree with the six positive statements regarding data protection. Building upon these, it is interesting to explore the possible impact of data subjects' concerns on their rights' knowledge assuming that the higher the concerns are the more data subjects will know their rights, since privacy concerns would be a motivation for rights awareness. Furthermore, considering that replies to the six statements record data subjects' views on data protection, it is of significance to investigate the impact that privacy concerns and rights knowledge extent have on these views.

To evaluate the impact of data subjects' concerns on the extent of knowledge for each right, spearman rho was used. Results are presented in Table 14. The positive relationships between concerns about personal data usage for different purposes than those initially collected without informing users and

a right to be informed for data processing

b consent required for data processing

Table 14 Concerns impact on respondents' rights knowledge

		Others control information provided online (C.1.3)	*Gover. Agencies collect personal data (C.1.4)*	*Companies websites use personal information (C.1.5)*	*Data used for different reasons than those collected (C.1.6)*	*Search engines record navigation history (C.1.7)*
Right to be Informed about	Data processing and subject's rights (B.1)	ns	ns	ns	rho = 0.279 p = 0.005	ns
	Data used for profiling and consequences (B.7)	ns	ns	ns	ns	ns
	Data transmission to third party (B.8)	ns	ns	ns	ns	ns
	High-risk pers. data breach, consequences, measures taken (B.9)	ns	ns	ns	ns	ns
Consent	Required for data use (B.3)	ns	ns	ns	rho = 0.312 p = 0.002	rho = 0.20 9 p = 0.037
	Form (free, specific…) (B.4)	ns	ns	ns	rho = 0.222 p = 0.026	ns
	Withdraw (B.5)	ns	ns	ns	ns	ns
	Not required for service usage (unless necessary for service provision) (B.6)	ns	ns	ns	ns	ns
Right to oppose	To data processing (incl. profiling) (B.10)	ns	ns	ns	ns	ns
	(not to be subjected) to automated decision (B.11)	ns	ns	ns	ns	ns
Right to data rectification (B.2)		ns	ns	ns	ns	ns
Right to data portability (B.12)		ns	ns	ns	ns	ns
Right to be forgotten (B.13)		ns	ns	ns	ns	ns
Right to data processing restriction (B.14)		ns	ns	ns	ns	ns

c the form of consent

as well as between concerns regarding search engines recording history of navigation and consent required for data processing reveal that as these concerns increase so does the extent of knowledge for the specific rights.

Table 15 presents the results of the correlation between the views of the participants regarding data protection (question C.2.7) and

i rights total score

ii concerns total score.

Results show that there is a negative relationship between rights total score and participants' views in all cases. In other words, as the extent of rights knowledge increases the agreement with these statements decreases. On the contrary, a positive relationship is shown between concerns and two of the statements revealing that as concerns increase the disagreement with statements (a) and (d) also increases.

Table 15 Rights knowledge and concerns impact on respondents' views regarding data protection

	Rights total score	*Concerns total score*
a) I am confident that the personal data I provide will not be used by anyone else	rho = –0.562, p = 0.000	rho = 0.297, p = 0.003
b) I am aware of data protection legislation to protect myself	rho = –0.349, p = 0.000	ns
c) I trust service providers to protect my data	rho = –0.412, p = 0.000	rho = 0.254, p = 0.011
d) Legislation and Supervisory Authorities fully protect my personal data	rho = –0.251, p = 0.011	ns
e) To protect myself it is sufficient to be careful about the data I provide online	rho = –0.352, p = 0.000	ns
f) Governments protect my data	rho = –0.247, p = 0.013	ns

The findings above show that respondents view data protection as a state in which many stakeholders get involved (data subjects, providers, governments, Authorities). This reminds Datoo's (2018) argument that GDPR implementation is a complex process requiring a holistic approach with reference to people, processes and systems since all these are involved, in a different way, in data processing.

4 Conclusion

Nowadays, the increasing ability of private and public sector agencies to collect and process large-scale data raises questions and worries that inevitably place privacy and data protection at the heart of the public debate worldwide. The new legal framework for

data protection as implemented with GDPR aims to enforce European data subjects' rights, harmonising also the legal culture and practices between EU member-states.

The actual protection of personal data and natural persons' freedoms does not depend only on the legal framework which guarantees their rights or on the data processing procedures that are adopted by the organisations in order to become GDPR compliant. The actual protection of personal data relies also on data subjects' rights knowledge highlighting thus the individual responsibility for personal data protection. In this frame, data subjects need to become more aware of their rights, understand these fully and exercise them (Sideri and Gritzalis, 2020). In other words, data subjects should acquire a new modus operandi regarding the protection of personal data, while eliminating their misconception that law or governments or service providers alone should take the appropriate measures to protect data and data subjects' rights. In fact, relying upon others to protect us or showing trust to them that they abide the law consist two of the vulnerabilities that have turned personal data to tradeable asset besides data subjects' ignorance of their rights or indifference about their data. Recently, European Commission published an evaluation report on GDPR underlining that although it has met many of its objectives, there is still work to be done. The report concludes that "individuals are increasingly aware of their rights" and that although "GDPR strengthened procedural rights...and individuals are increasingly using these rights, there is a need to facilitate their exercise and their full enforcement" (EC, 2020, p.8).

Our exploratory research investigated the extent of GDPR rights knowledge of a Greek adults group. Evaluating the research results it becomes clear that awareness increase is required for several rights in order for data subjects to make informed decisions to optimise control over personal data and ultimately protect themselves. Even in the cases where data subjects showed high extent of knowledge (e.g., for the form of consent) differentiations were recorded that need to be eliminated.

The demographic variables (gender, age, educational level and employment) showed a limited impact on the extent of knowledge with reference to specific rights. On the contrary, the impact of information sources on knowledge proved to be more significant for most of the rights explored. This reveals that there is still the need for citizens to be more informed on GDPR rights. In this frame, national information campaigns are very important in order for all citizens to be fully aware of their rights. Such a practice is expected to safeguard a homogenous landscape with regard to rights knowledge reducing or eliminating inequalities between citizens that derive from rights knowledge gap.

Results also revealed respondents' high concerns for the topics they were asked. Our assumption that concerns increase would lead to higher extent of rights knowledge was supported for some cases only. Respondents' concerns for personal data usage for different purposes than those initially collected without informing them had a positive impact on

a right to be informed for data processing and subject's rights

b the form of consent

c consent required for data processing.

Consent required for data processing was shown to be positively related to concerns regarding search engines recording data subjects' history of navigation. These findings imply that privacy concerns are not –at least in this case- a major incentive for data subjects to increase their knowledge on GDPR rights and this situation is consistent with

Baek's (2014) argument that people ultimately fail to transform their privacy concerns into protective behaviour.

The discrepancy revealed between rights knowledge and data subjects' behaviour, in the case of consent for example, is indeed interesting and should be further investigated in order to clarify whether it constitutes a paradox, a contradiction between knowledge and behaviour in this case -in accordance to the already recognised Privacy Paradox (contradiction between attitude and behaviour)- or whether behaviour is not determined by knowledge but by a shaped system of dispositions, tendencies, perceptions and social actions, which is outlined by the concept of 'habitus' (Bourdieu, 1977).

Participants' replies showed their tendency to disagree with the positive statements proposed to them regarding data protection. This tendency is related more to the extent of rights knowledge. Results revealed that as knowledge increases the agreement with the statements decreases. Concerns, on the other hand, affect these statements only in two cases ("I am confident that the personal data I provide will not be used by anyone else" and "Legislation and Supervisory Authorities fully protect my personal data") showing that as concerns increase the disagreement with statements also increases. Consequently, rights knowledge seems to affect more participants' views regarding data protection comparing to privacy concerns. This finding highlights once more the necessity for more rights awareness.

Since GDPR implementation, organisations in order to become GDPR compliant have given emphasis to data protection awareness training programs for their staff (Perry, 2019). This verifies the need for data subjects' awareness increase too. Enhancing awareness on GDPR rights and the risks that come up when personal data are not protected should be one of the priorities of the European Data Protection Authorities. Digital literacy is a basic life-skill and measures that "directly aim to strengthen users' awareness about the extent of their knowledge" should be taken (Moll et al., 2014, p.218). In this frame public informational campaigns that improve users' knowledge and provide skills to combat cyber threats (Marcolin et al., 2000) as well as educational programs and interventions including knowledge about current legislation (Sideri et al., 2019) and about data collection and processing procedures, data usage and accessibility by others (Lawler and Molluzzo, 2010) in an understandable way are extremely important in both formal and informal educational frames. Moreover, considering that data subjects should be informed on their right to data protection from an early age in order to become aware and active citizens, the topic of GDPR should be included in all curricula of Informatics regardless the level of education.

Beyond the fluctuations revealed in data subjects' rights knowledge within the sample recruited, differences in rights knowledge have been also recorded between EU citizens (EU, 2019). As Eurobarometer 2019 concludes "just because respondents in a country have a high level of awareness of GDPR and what it is does, it does not automatically follow they have heard of all the rights GDPR guarantees" (EC, 2019, p. 27). Considering both our findings and this statement, the deviation in rights knowledge seems to reflect a reality that may lead to a form of inequity between Europeans which should be prevented and reversed immediately. This requires data subjects' continual and consistent information on GDPR and their rights with every possible and prosperous way.

As stated, the sampling method does not allow the generalisation of the research results. However, the findings resulting from hypotheses testing are interesting highlighting the necessity for a more thorough investigation of data subjects' awareness regarding each right GDPR guarantees and the factors affecting awareness. These

findings may be useful for relevant researches carried out in other EU states that have cultural and social similarities with Greece, since cultural and social values are known to affect privacy concerns and privacy awareness (Krasnova et al., 2010; Cecere et al., 2015).

Future researches should explore how information provision by governmental agencies, Data Protection Authorities, mass and social media, data subjects' access to information sources, social inequalities, digital illiteracy and past experiences impact on the extent of rights knowledge which finally affects data subjects' behaviour regarding their responsibility to protect personal data exercising their rights. Relevant surveys in other EU member-states would be helpful for decision makers to take the appropriate actions in order to increase European citizens' awareness on the rights GDPR sets. Moreover, considering that personal data are also stored and processed offline, future research should explore the knowledge and behaviour regarding GDPR rights of people who do not use digital services.

References

Babbie, E. (2011) *Introduction to Social Research*, Kritiki Publ., Athens (in Greek).

Baek, Y.M. (2014) 'Solving the privacy paradox: a counter-argument experimental approach', *Computers in Human Behavior*, Vol. 38, pp.33–42.

Bourdieu, P. (1977) *Outline of a Theory of Practice*, Cambridge University Press, UK.

Brandimarte, L., Acquisti, A. and Loewenstein, G. (2012) 'Misplaced confidences: privacy and the control paradox', *Social Psychological and Personality Science*, Vol. 4, No. 3, pp.340–347.

Buschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y. and Elger, B. (2014) 'Protecting human health and security in digital Europe: how to deal with the 'Privacy paradox'?', *Science and Engineering Ethics*, Vol. 20, pp.639–658.

Cadogan, R.A. (2011) 'An imbalance of power: the readability of internet privacy policies', *Journal of Business and Economics Research*, Vol. 2, No. 3, pp.49–62.

Cecere, G., Le Guel, F. and Soulié, N. (2015) 'Perceived internet privacy concerns on social networks in Europe', *Technological Forecasting and Social Change*, Vol. 96, pp.277–287.

Conger, S., Pratt, J.H. and Loch, K.D. (2013) 'Personal information privacy and emerging technologies', *Information Systems Journal*, Vol. 23, No. 5, pp.401–417.

Custers, B., Dechesne, F., Sears, A.M., Tani, T. and van der Hof, S. (2018) 'A comparison of data protection legislation and policies across the EU', *Computer Law and Security Review*, Vol. 34, No. 2, pp.234–243.

Datoo, A. (2018) 'Data in the post-GDPR world', *Computer Fraud and Security*, Vol. 9, pp.17–18.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. and Sanchez, I. (2018) 'The right to data portability in the GDPR: towards user-centric interoperability of digital services', *Computer Law and Security Review*, Vol. 34, No. 2, pp.193–203.

European Commission (2015) *Special Eurobarometer 431. Data Protection Report* [online] https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf (Accessed 7 August, 2020).

European Commission (2019) *Special Eurobarometer 487a. The General Data Protection Regulation Report* [online] https://www.privacy-web.nl/cms/files/2019-06/ebs487a-en.pdf (Accessed 7 August, 2020).

European Commission (2020) *Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation* [online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264& from=EN (Accessed 7 August, 2020).

European Council (2016) *Regulation* (*EU*) *2016/*679 *of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation) [online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32016R0679& from=EN (Accessed 7 August, 2020).

Hong, W. and Thong, J.Y. (2013) 'Internet privacy concerns: an integrated conceptualization and four empirical studies', *MIS Quarterly*, Vol. 37, No. 1, pp.275–298.

Hoofnagle, C.J. and Urban, J.M. (2014) 'Alan Westin's privacy homo economicus', *Wake Forest Law Review*, Vol. 49, pp.261–317.

Javeau, C. (1996) *The Research Using Questionnaire*, Tipothito Publ., Athens (in Greek).

Kelley, P.G., Cranor, L.F. and Sadeh, N. (2013) 'Privacy as part of the app decision-making process', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Paris, France, pp.3393–3402.

Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand T. (2010) 'Online social networks: why we disclose', *Journal of Information Technology*, Vol. 25, No. 2, pp.109–125.

Lawler, J.P. and Molluzzo, J.C. (2010) 'A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet', *Journal of Information Systems Applied Research*, Vol. 3, No. 12, pp.3–18.

Mantelero, A. (2014) 'The future of consumer data protection in the EU re-thinking the 'notice and consent' paradigm in the new era of predictive analytics', *Computer Law and Security Review*, Vol. 30, No. 6, pp.643–660.

Marcolin, B.L., Compeau, D.R., Munro, M.C. and Huff, S.L. (2000) 'Assessing user competence: conceptualization and measurement', *Information Systems Research*, Vol. 11, No. 1, pp.37–60.

Marwick, A.E., Murgia-Diaz, D. and Palfrey, J.G. (2010) *Youth, Privacy and Reputation (Literature Review)*, Social Science Research Network, Rochester, NY.

Miltgen, C.L. and Peyrat-guillard, D. (2014) 'Cultural and generational influences on privacy concerns: a qualitative study in seven European countries', *European Journal of Information Systems*, Vol. 23, pp.103–125.

Mitrou, L. (2002) *'Law' in the Information Society*, Sakkoulas Publ., Athens (in Greek).

Moll, R., Pieschl, St. and Bromme, R. (2014) 'Competent or clueless? users' knowledge and misconceptions about their online privacy management', *Computers on Human Behavior*, Vol. 41, pp.212–219.

Oppenheim, A. (1992,) *Questionnaire Design, Interviewing and Attitude Measurement*, Pinter, London.

Park, Y.J. (2011) 'Digital literacy and privacy behavior online', *Communication Research*, Vol. 40, No. 2, pp.215–236.

Perry, R. (2019) 'GDPR-project or permanent reality?', *Computer Fraud and Security*, Vol. 1, pp.9–11.

Poullet, Y. (2018) 'Is the general data protection regulation the solution?', *Computer Law and Security Review*, Vol. 34, No. 4, pp.773–778.

Proctor, R.W., Athar Ali, M. and Vu, K-P.L. (2008) 'Examining usability of web privacy policies', *International Journal of Human–Computer Interaction*, Vol. 24, No. 3, pp.307–328.

Sideri, M. and Gritzalis, S. (2020) 'Are we really informed on the rights GDPR guarantees?', *Proceedings of 14th IFIP WG 11.12 International Symposium on Human Aspects of Information Security and Assurance HAISA. 2020*, Springer IFIP AICT 593, pp.315–326.

Sideri, M., Fontaras, A. and Gritzalis, S. (2020) 'What do we know about our rights to data protection? A Greek case study', *Proceedings of the 8th International Conference on e-democracy: Safeguarding Democracy and Human Rights in the Digital Age*, Springer International Publishing, pp.18–33.

Sideri, M., Kitsiou, A., Tzortzaki, E., Kalloniatis, C. and Gritzalis, S. (2019) 'Enhancing university students' privacy literacy through an educational intervention. A Greek case-study', *International Journal of Electronic Governance*, Vol. 11, Nos. 3–4, pp.333–360.

Sobolewski, M., Mazur, J. and Paliński, M. (2017) 'GDPR: a step towards a user-centric internet?', *Intereconomics*, Vol. 52, No. 4, pp.207–213.

Surveillance Project (2008) *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance. Summary of Findings*, Queen's Univ., Kingston [online] https://www.sscqueens.org/sites/sscqueens.org/files/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf (Accessed 7 August, 2020).

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. and Lind, F. (2015) 'Do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)', in Gutwirth, S., Leenes, R. and de Hert, P. (Eds.): *Reforming European Data Protection Law*, Springer, Heidelberg, pp.333–365.

van Ooijen, I. and Vrabec, H.U. (2019) 'Does the GDPR enhance consumers' Control over personal data? An analysis from a behavioral perspective', *Journal of Consumer Policy*, Vol. 42, pp.91–107.

Zafeiropoulos, K. (2015) *How to Do a Scientific Research*, Kritiki Publ., Athens (in Greek).

Notes

[1]In B.13 and B.14 respondents had the option of multiple responses as follows; B.13: (a) if data are no longer necessary, (b) if consent has been withdrawn, (c) if there is no legal basis for data processing, B.14: (a) when data accuracy is disputed, (b) when processing is illegal, (c) when data controller no longer needs personal data for the purposes of the processing, but data are required by the subject for the foundation, exercise or support of legal claims and (d) when data subject has objections to the processing, pending verification that the legitimate reasons of the controller prevail all those of data subject.

[2]Transformations in demographic variables values were made for the statistic tests to be better applied. Age, educational level and employment were re-codified in order for more coherent clusters within variables considering the small number of respondents in some clusters. Thus, regarding i) 'age', the cluster '18–25 years old' is included in the following (26–35), while the cluster '>56 years old' in the preceding (46–55), ii) 'educational level', the cluster of those holding a PhD is included in that of those holding a M.Sc., iii) 'employment', teachers are included in the cluster of public sector employees, freelancers in that of private sector employees, while students and other constitute one cluster.

Appendix

Questionnaire for the General Data Protection Regulation

Approximately one year ago, the General Data Protection Regulation (GDPR) was implemented in all member states of the European Union. The new Regulation brings significant changes to the protection of individuals with regard to personal data collection and processing.

This research investigates data subjects' knowledge, in Greece, regarding the provisions of GDPR about data subjects' rights and the collection and processing of personal data by organisations, entities and companies.

Within this frame, you are invited to participate in this online survey, replying to questions related to the knowledge you have about your rights regarding personal data, as

introduced in GDPR, the perceived risks deriving from possible loss or theft of your data as well as to state practices you follow regarding data security.

We estimate that it will take you approximately 20 min to complete the questionnaire.

Your participation in this survey is voluntary. You may exit the survey at any time without penalty. You are also free to decline to answer any particular question you do not wish to answer for any reason.

You will receive no benefits from participating in this research study. However, your responses will help us learn more about the issues investigated.

Your answers will be collected by the survey app Google Forms. Name, email address, or other data are not recorded in order for the participants not to become identifiable. Your responses will remain anonymous so no one will be able to identify you or your answers, and no one will know whether you participated in the research.

We thank you in advance.

A. General Data Protection Regulation (GDPR)

1 *How did you get information on the General Data Protection Regulation (GDPR)?*

☐ From mass media

☐ From Internet

☐ From personal engagement

☐ From a conversation with others

2 *In your opinion the enforcement of GDPR is a responsibility at…?*

☐ European Level ☐ National Level ☐ Regional or Local Level ☐ I do not know

3 *Which of the following issues do you think the GDPR meets* (*you can choose more than one answer*)*?*

☐ Strengthening the rights of data subjects

☐ Increasing the obligations of entities collecting and managing data

☐ Stricter delimitation of data collection and processing procedures

☐ Tightening up regulatory compliance control measures

4 *Do you know the Competent Supervisory Authority in our country which is responsible for protecting your rights regarding personal data?*

☐ Yes ☐ No

B. The rights of data subjects

1 *To what extent do you know that data controller must inform you within a reasonable time and in a clear way about the processing in which your data is going to be submitted and about your rights?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

2 *To what extent do you know that you have the right to require from the controller without undue delay to correct your inaccurate personal data?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

3 *To what extent do you know that your consent is required for the use of your personal data?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

4 *To what extent do you know that your consent for the use of your personal data should be free, specific and explicit?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

5 *To what extent do you know that your consent can be withdrawn at any time?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

6 *To what extent do you know that consent is not a prerequisite for services provision, unless the use of data is necessary for the provision of the service?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

7 *To what extent do you know that if data processing aims at profiling, you should be informed about the process and its potential consequences?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

8 *To what extent do you know that in case that data is transmitted to a third party, the* controller *must inform you after the first transmission, the latest?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

9 *To what extent do you know that when high-risk personal data breach occurs, the controller is obliged to inform you about the breach, its consequences and the measures taken?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

10 *To what extent do you know that you have the right to oppose, at any time and for reasons related to your particular situation, to the processing of your personal data* (*processing by public or private actors*)*, including profiling?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

11 *To what extent do you know that you have the right not to be subjected to a decision taken solely on the basis of automated processing, assessing personal aspects that concern you and producing effects that affect you* (e.g., *legal effects*)*?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

12 *To what extent do you know that you have the right to receive your personal data that you have provided to a controller and transmit it to another controller?*

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Not at all	Little	Moderate	Well	Very Well

13 *Do you know in which cases you have the right to ask from the controller to erase your personal data?* (*you can choose more than one answer*)

a) if these are no longer necessary

b) if you withdraw your consent

c) if there is no other legal basis for processing

d) I don't know

14 *Do you know in which cases you have the right to ask the controller the* restriction *of data processing?* (*You can choose more than one answer*)

a) when the accuracy of the data is disputed

b) when processing is illegal

c) when data controller no longer requires the personal data for the purpose of processing, but these data are required by you for the establishment, exercise or support of legal claims

d) when you have objections to processing, pending verification that the legitimate grounds of the controller override all those of yours

e) I don't know

C. Risks to personal data and ways of protection

C.1 Personal data control and risks

1 *I* control *the personal data I provide online*

☐ I'm absolutely sure ☐ I'm quite sure ☐ I'm not really sure ☐ I'm not sure at all ☐ Don't know

2 *How much control do you feel you have over the information you provide online* (*e.g., the ability to correct, change or delete this information*)*?*

☐ Complete Control ☐ Partial Control ☐ No control at all ☐ It depends ☐ Don't know

3 *How concerned are you about others having control over the information you provide online? Would you say you are …. ?*

☐ Very concerned ☐ Quite concerned ☐ No particularly concerned ☐ Not at all concerned ☐ Don't know

4 *How concerned are you of the recent revelations about governmental agencies collecting personal data on a large scale for national security purposes?*

☐ Very concerned ☐ Quite concerned ☐ No particularly concerned ☐ Not at all concerned ☐ Don't know

5 *How comfortable do you feel with the fact that companies' websites use* information *about your online activity to create content that suits your preferences?* (e.g., *personalised ads*)

☐ Very comfortable ☐ Quite comfortable ☐ No particularly comfortable ☐ Not at all comfortable ☐ Don't know

6 *Public and private actors holding data about you may sometimes use it for* different *purposes from the ones it was initially collected, without notifying you* (e.g., *for direct marketing, targeted online advertising, profiling*). *How concerned are you about such a use of your data?*

☐ Very concerned ☐ Quite concerned ☐ No particularly concerned ☐ Not at all concerned ☐ Don't know

7 *How concerned are you that popular search engines such as Google record the websites you originated from and the ones you visit?*

☐ Very concerned ☐ Quite concerned ☐ No particularly concerned ☐ Not at all concerned ☐ Don't know

8 *Would you like to be informed if your personal data is lost or stolen?*

☐ Yes ☐ No

9 *Which data would you be most concerned about, if it was lost or stolen?* (*You can choose more than one answer*)

a) Data stored in your computer

b) Data stored in your mobile phone or tablet

c) Data stored online or in the cloud

d) Other (spontaneous)

e) Don't know

10 *In your opinion, what are the most serious risks concerning your personal data when providing them online?* (*You can choose more than one answer*)

a) Becoming a victim of fraud

b) Your online identity being used for fraudulent purposes

c) Your data being used without your knowledge

d) Your personal information being stolen

e) Your data being transferred to third parties (companies or government agencies) without your consent

f) Your data being used for different purposes from those you initially provided it for

g) Your data being used to send you unwanted advertising material

h) Your personal safety being at risk

i) Your reputation being damaged

j) Becoming victim of discrimination (e.g., in job recruitment, being charged higher prices, not being able to access a service)

k) Your views and behaviour being misunderstood

l) Other

m) None

n) You never provide information online

o) Don't know

C.2 Personal Data Protection

1 *Thinking about privacy policies on the internet, which of the following sentences best describes what you usually do?*

a) You read them fully

b) Your read them partially

c) You do not read them at all

2 *What are the reasons you do not read the privacy policies or read them partially?* (*You can choose more than one answer*)

a) You think they are too long to read

b) You find them unclear, too difficult to understand

c) You think the websites will not honor them anyway

d) You believe that the law will protect you in all cases

e) It is sufficient for you to see that websites have a privacy policy

f) You don't think it is important to read them

g) You don't know where to find them

h) Other (Spontaneous)

i) Don't know

3 *If you experience a problem concerning the protection of your personal data, whom will you address to?* (*You can choose more than one answer*)

a) The (National) Supervisory Authority

b) The public or private actor managing your data

c) A court

d) An independent Authority for the protection of data subject

e) A European Authority

f) Other

g) Don't know

h) Nobody

4 *Do you explicitly give your consent in order for any kind of personal data to be* collected *and processed?*

☐ Yes, in all cases ☐ Yes, in the case of personal data required online ☐ Yes, in the case of sensitive data ☐ No ☐ Not sure

5 *When you are asked to provide personal data online, would you say that you are informed about the conditions of your data collection and processing?*

☐ Always ☐ Sometimes ☐ Rarely ☐ Never ☐ You are never asked to provide personal data online ☐ Don't know

6 *When you decide to change online service provider* (e.g., *an online social* network *or a cloud service provider*)*, how important is it for you to be able to transfer your personal data from the old provider to the new one?*

☐ Very important ☐ Quite important ☐ No particularly important ☐ Not at all important ☐ Don't know

7 Please *state your agreement or disagreement with the following statements:*

a) I am confident that the personal data I provide will not be used by anyone else

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

b) I am well aware of data protection legislation to protect myself

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

c) I trust service providers to protect my data

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

d) Legislation and Supervisory Authorities fully protect my personal data.

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

e) To protect myself, it is enough to be careful about the data I provide online.

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

f) Governments protect my data

☐ Strongly Agree ☐ Agree ☐ Neither agree nor disagree ☐ Disagree ☐ Strongly disagree

D. Personal Information

1 *Gender*

☐ Man ☐ Woman

2 *Age*

☐ 18 – 25

☐ 26 – 35

☐ 36 – 45

☐ 46 – 55

☐ > 56

3 *Educational level*

☐ Graduate of Primary School

☐ High School graduate

☐ University graduate

☐ Master holder

☐ Ph. D. holder

4 *Employment*

☐ Public servant

☐ Private Employee

☐ Freelancer

☐ Educator (all levels)

☐ Student

☐ Retired

☐ Other

Thank you for your participation!