Perception of Privacy in the light of GDPR

Mirkó Gáti
Corvinus University of Budapest
Attila Simay
Corvinus University of Budapest

Cite as:
Gáti Mirkó, Simay Attila (2020), Perception of Privacy in the light of GDPR. *Proceedings of the European Marketing Academy*, 11th, (85181)

Paper presented at the 11th Regional EMAC Regional Conference, Zagreb (online), September 16-19,2020

Perception of Privacy in the light of GDPR

Abstract:

GDPR is the general data protection regulation of the European Union, which aims to harmonize legislation related to privacy and personal data in Europe. The regulation contains the protection of users' personal data, and to change how different organizations should process these data. Legal regulation presumably changes internet users' privacy-related attitudinal and behavioural characteristics. The empirical research sheds light to the perception of general privacy and GDPR among university students. The study was conducted one year after GDPR took effect, which was assumed to be enough time for users to consciously perceive its significance.

Keywords: GDPR, privacy, user perceptions

1. Introduction

In the past 10-15 years the development of technology and the social changes challenged and challenge the data regulation formed in the end of 1990s. Contents generated and published by users significantly expanded the quantity of online data. Big data came into view and appeared in the data regulation literature, too. Likely that these tendencies contributed to the present EU regulation, which shift the emphasis from individual rights to the responsibility of data users. Thus, the regulation instead and next to the individual informational self-determination rights and individual data consciousness emphasizes the data managers' duties, responsibilities and accountability.

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years, replacing an outdated data protection directive from 1995. The European Parliament adopted the GDPR in April 2016. The regulation entails provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. According to the regulation, enterprises that collect data from citizens in EU) countries will need to comply with strict new rules around protecting customer data by May 25, 2018 (Geospatial World, 2018). So, we did our research in the first anniversary of GDPR to see any possible changes in users' attitudes and consciousness. The exact text of the regulation has been available in all official languages of the EU since 2016 (EU, 2016). The regulation was published 2 years before its application, which could provide time to the organizations to prepare the new regulation about privacy and personal data. The regulation contains a lot of details about privacy and personal data management (including recording, collecting, storing, using, transferring or modifying those data) and provide the definition of personal data. Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information – which were collected together – can lead to the identification of a particular person who also constitutes personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR (EC, 2019).

According to the Hungarian Act CXII of 2011 on information self-determination and freedom of information 'personal data' shall mean data relating to the data subject, and data' processing' shall mean any operation or the totality of operations performed on the data, irrespective of the procedure applied in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (Act CXII of 2011).

As a regulation GDPR is not a directive, thus compliance is mandatory, without the need for each member state to ratify it into its own legislation. The GDPR expands the scope of data protection so that anyone or any organization that collects and processes information related to EU citizens must comply with it, no matter where they are based or where the data is stored. Cloud storage is no exception. Moreover, the definition of personal data has also been expanded too. It states that personal data includes information from which a person could be identified, either directly or indirectly. Consumers must unambiguously give their consent for their data to be processed, which must be informed and voluntary (Tankard, 2016).

This law was implemented in order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union. So, the level of protection of the rights and freedoms of natural persons regarding the processing of such data should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data,

as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements. Because rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly (EU, 2016).

The GDPR is established to create consistent data standards and protect EU citizens from potential privacy abuses. The implications and ramifications are enormous, and the initiatives reach global scale. Consumers are allowed to file complaints with each EU national data protection authority, which will investigate the claim. So GDPR change the way data collection takes place to the way corporate databases are designed and used, because the regulation allows consumers to remove themselves from a database or online source at any time. Companies violating GDPR face fines of up to 4% of their global annual revenues (Greengard, 2018). So, the digital footprints could be removed by consumers, which could have a significant impact how personal data is stored, used and transferred online, like cloud storages.

Beside the legal regulations we consider the perception of these regulations is also a significant issue. In our paper we also include the perception of privacy and privacy policies as we believe that it influences the perceived risks about misuse of personal data is related to that issue.

2. Law and Perception

Perception is the process how people select, organize, and interpret information inputs to create a meaningful picture of the world. create a meaningful picture of the world.39 It depends not only on physical stimuli, but also on the stimuli's relationship to the surrounding environment and on conditions within each of us. People emerge with different perceptions of the same object because of the perceptual processes. These processes could be selective attention, selective distortion, and selective retention, because people cannot possibly attend to all stimuli, so their attention select their focus, distortions can happen due to how people interpret information in a way that fits their preconceptions, and likely to remember good points about what their like (Kotler & Keller, 2012). Therefore, in this study we focused on individuals, as the regulation has an objective legal impact, but the individual perception of its effects can be different by users.

Adjerid, Peer, and Acquisti. (2018) found in their study that users were more satisfied with security measures and were less worried about privacy protection-related issues by high perceived Internet security measures. At the same time, they had less concern that their provided data would have adverse effects on them. However, respondents who could expect a low level of protection of their privacy provided significantly fewer personal data. Relative and objective risks are capable of influencing people's behaviour in connection with privacy protection. Nevertheless, they also concluded that objective changes have a diminishing effect on risk between the theoretically possible and the actually applied settings, i.e., they are more essential than the theoretically possible settings. The role of relative risks, in contrast, increases between the theoretically possible and the actual settings, therefore, the effect is stronger by the actual settings (Adjerid et al., 2018). Therefore, changes in the legal framework referring to privacy protection and striving to make users' data management safer may eventually have an impact on the sharing of users' personal information in the online space. Based on this, it is worth analysing what actual changes the regulation caused in users' security-related perception, and there also may be grounds for the analysis whether the introduction of GDPR can play a role in increased consumer confidence in the long term.

The issue of regulation and perception is relevant, because in a last year's publication, Fox and Royne (2018) concluded that users' fears about personal data management are stronger when the information includes voices or images, than in the case of solely texts. Information containing either voices or images draws user's attention more to privacy protection. However, nowadays most websites inform users about their data management policy exclusively with texts (Fox & Royne, 2018). At the same time, Schmeiser's results confirm that a considerable number of users are not interested in the impacts on their privacy in the online space, which may derive from advertisements and applied technology solutions. Users who often install related extensions on Internet browsers pay more attention to the protection of their privacy. The application of ad networks and technologies tracking consumer behaviour may increase users' confidence in websites, although the reason for that may also be the users' ignorance about the applied technologies and that more visited websites automatically enjoy greater user confidence (Schmeiser, 2018). Consequently, users' information and education related to the protection of their privacy and their personal data may be a relevant issue in which the creation of GDPR can be interpreted as a possible legislative step. An interesting issue in the future may be the creation of additional rules which do not necessarily draw users' attention to data management practice and setting options with only texts.

3. The Possible Added Value of the Theory of Planned Behaviour to the Issues related to Privacy Protection

The appearance of concerns related to privacy protection in the literature is a relatively well documented area (Williams, 2018), where Internet users' concerns are constantly present. Still, despite this, they share their sensitive personal data, and allow third persons to have access to these data. With the spread of smartphones, a new tool became available for users, through which a substantial part of their activities necessary for life can be performed, everything from mobile payment through telebanking services to social media activities, and all this is complemented by a user behaviour which – partly because of usage patterns and characteristics changed by social media systems – distracts users from the consumer behaviour formed by the usual principles. Of course, organisations can stand up against this, or regulations similar to GDPR can be introduced, but the question is still if it is the change of the external regulatory environment which primarily contributes to users' awareness, or the internal, organic way which, with the change of user interface (UI) can authorise users by informing them about their possibilities on the interaction platforms and can remind them of their concerns in connection with the protection of their privacy, thereby drawing their attention to the possible dangers arising from the access to personal data.

The scientific analysis of this problem was carried out by Hughes-Roberts and Kani-Zabihi (2014), where the authors approached the theoretical background of the topic through the Theory of Reasoned Action and then its complemented model, the Theory of Planned Behaviour (TPB). The Theory of Planned Behaviour was created with the modification – adding the perceived behavioural control to the model – of the Theory of Reasoned Action model. In the case of the latter one, several studies found that attitude and subjective norm do not completely describe behavioural intention, and then other researches highlighted that another factor was missing, which was named perceived behavioural control (Madden, Ellen, & Ajzen, 1992). According to the theory, attitude towards behaviour, subjective norm and perceived behavioural control lead to the formation of the intention to act (Ajzen, 2002). The Theory of Planned Behaviour may help to understand consumer behaviour, provided that the research focuses on the psychological background of privacy protection and on which influencing factors determine the behaviour-related factors (intention and action). Based on the analysis of Hughes-Roberts and Kani-Zabihi (2014: 226), users, who built privacy protection-related information

into the user interface published considerably less information than the participants of the control group in their experiment.

If we examine which characteristics describe the features of attitude and behaviour concerning users' privacy protection with the appearance of the Internet, it is worth taking into consideration that users share personal information (for example in the case of a type of social media, i.e. on personal social networks, e.g. Facebook) with each other almost indiscriminately, or at least in very uncontrolled circumstances during everyday use. The privacy protection-related paradox which reflects the typical results of the related researches reveals the interesting correlation that users' intention – especially on social networks – does not reflect their online behaviour (Acquisti & Gross, 2006). This paradox may stem from several reasons, including users' ignorance of the consequences of their actions (related to privacy protection), and users' ignorance of the system they use and whose conditions of use they accepted (Alashoor & Baskerville, 2015).

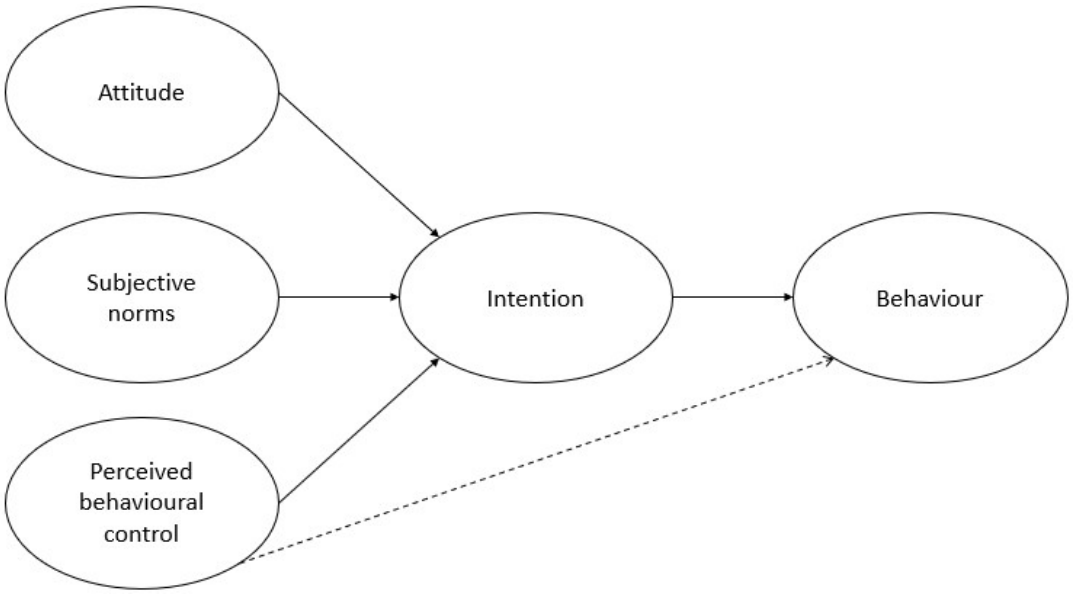

Figure 1. Attitudinal and behavioural elements based on the Theory of Planned Behaviour in the context of privacy
Source: own elaboration based on Madden et al. (1992) and Hughes-Roberts & Kani-Zabihi (2014)

To interpret Figure 1, the concepts of its constructs are going to be presented as follows. The concept of the attitude towards behaviour is the perception of the knowledge related to the consequences of behaviour, meaning whether the person has a favourable or an unfavourable opinion of the given behaviour. Subjective norms are factors representing the perceived social pressure in connection with the actual execution of the behaviour. Perceived behavioural control means the ease or difficulty in executing the behaviour, which is formed by the experiences gained in the past and considering the predicted difficulties (Ajzen, 2002: 666-667.). The Theory of Planned Behaviour may therefore be able to forecast the actual, personal data protection-related behaviour – and the extent of the preceding intention to act – of persons to be examined (Internet users) in a social media environment, in accordance with the defined conditions. The connections explored by the Theory of Planned Behaviour may be of great help in revealing the influencing effect of the external regulatory environment related to the GDPR regulation.

4. Empirical Research and Methodological Considerations

It can be said that data collection was carried out in the form of an online questionnaire, and since the topic examines online consumer behaviour among users, this method seemed to be appropriate. The statistical analysis of the structured responses could be done with the questionnaire. In addition, the online survey makes it possible to do fast and large-sample data collection. Data were analysed with SPSS 25.

The questionnaire survey was carried out between April 26 and May 8, 2019, because it was assumed that this period of nearly one and a half weeks would provide a large number of responses, and at the same time it would be a time interval short enough to minimize potential bias. Voluntary sampling was applied. Since respondents are university students from Hungary, results cannot be considered as representative. However, results are likely to show exciting tendencies related to the topic. At this point it must be mentioned that the selected sample differs from the average population in terms of certain characteristics. As regards digital literacy, for example, they have much higher values, furthermore, their general education, reading literacy and abstract reasoning are much more developed as compared to the average values of the society. Based on this, it has to be highlighted that the generalisability of the results is limited due to the characteristics of the sample, because of the indicated reasons. During the research, already tested international models and scales are applied, of which results relevant to GDPR are presented in this study. This is primarily represented by the application of Fox and Royne's (2018) privacy protection-related scales and their adaptation to the context of GDPR.

After data cleansing the examined sample contained 606 people. 40.1% of the sample were men, while 59.9% were women. Considering the characteristics of the sample, it can be said that respondents were predominantly born in the years 1998-1999 (75%). The majority of respondents live in the capital [(56.6%, but the presence of the agglomeration of Budapest is also significant (10.4%)], while 12% live in county seats and 15% in other towns. Consequently, the examined sample can basically be characterised as a group of young adults living in towns and cities. In terms of perceived financial circumstances, the majority perceive their financial circumstances to be average (46.2%), while others rather have above-average values. The percentage of respondents indicating perceived financial circumstances slightly (38.6%) or significantly (7.4%) above average is much higher than the percentage of respondents with values slightly (6.6%) or significantly (1.2%) below average.

5. Privacy and GDPR Perceptions

First, respondents were tested whether they know what does the abbreviation GDPR mean, where they had to select the right definition among 4 alternatives. The vast majority of the respondents gave the right answer (83.2%), but at the same time it indicates that cc. every sixth of them were not aware of the term (16.8%). After this question, every respondent could read a short description of the meaning and content of GDPR to have a general image of user perception in this issue.

In the case of questions related to GDPR regulation respondents had to declare their subjective judgement about GDPR data privacy policy. They had to decide about their attitudes towards GDPR regulations related to the people they know. Distribution of results is shown in Table 1.

	Absolutely disagree	Rather disagree	Neutral	Rather agree	Absolutely agree
I fully understand GDPR's privacy policy.	2.8	14.5	30.4	*43.6*	8.7
I understand the terms used in the GDPR.	3	18	29.7	*41.3*	8.1
I am confident in my understanding of the GDPR.	4.5	23.1	38.4	*29.4*	4.6
I understand how my information will be used according to GDPR.	3.5	23.3	30.5	*37.1*	5.6
I understand enough about the GDPR to feel confident about my actions on the site.	4.3	15.8	28.2	*43.2*	8.4
I am knowledgeable about how my information will be used according to GDPR.	9.6	31.7	31.2	23.6	4
I could explain GDPR to others with confidence.	24.1	38.3	25.4	10.7	1.5

Table 1. GDPR perceptions (%)
Source: own elaboration

Based on the results it can be said that the majority of these young people in the sample understand the most important GDPR privacy directives and terms and believe that they comprehend regulatory environment to use confidently the accessible internet sites. Related to the exact meaning of GDPR and how it regulates data processing and use of their personal data, respondents are not so sure anymore. In the case of the proper interpretation of privacy policy, respondents show lower confidence. The majority of respondents would not be so sure if they had to explain these policies to others, which can be interpreted as the exact understanding of the legal environment did not materialize, despite the perceptions they gave about it.

To reveal the connections related to the data protection regulation, correlation coefficients were used. Based on the results significant correlation was found among certain questions (significance level: 1%). Correlation coefficients were among moderately strong (at least .455) and strong (.734), and the connections were significant. This indicates that respondents' perceptions about GDPR are mostly associated with more general questions of data protection when the topic is personal data security and the related legal environment.

It was also asked what kind of user expectations are identified related to the collection and processing of personal data, in connection with data protection regulation. This question was asked knowing that the legal effects of GDPR affected mostly data protection directives and communication practice of for-profit firms since the regulation took effect. The related attitudes and expectations are shown in Table 2.

	Absolutely disagree	Rather disagree	Neutral	Rather agree	Absolutely agree
Companies seeking information online should disclose the way the data are collected.	.8	4,8	9,4	*43,1*	*41,9*
Companies seeking information online should disclose the way the data are used.	.2	3,6	4,1	*32,5*	*59,6*
A good consumer online privacy policy should have a clear and conspicuous disclosure.	.2	2	7,6	*36,5*	*53,8*
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	.8	4.8	17	*41.9*	*35.5*
A GDPR compatible privacy policy should have a clear and conspicuous disclosure.	.2	1.7	7.6	*38.1*	*52.5*

Table 2. Expectations towards data protection directives (%)
Source: own elaboration

Based on the respondents, there was a visible need of the users to be informed how their personal data is collected and used, and all this should be communicated in their privacy directives and communication with their consumers. Companies should most importantly recognize and communicate the use of data they own. There is an elemental need from the respondents to disclose the privacy directives transparently. This need was not only formulated in the case of general privacy directives, but especially in accordance with privacy directives related to GDPR regulations.

Connections related to data protection were also analysed with correlation coefficients (significance level: 1%). The way how data is collected is strongly correlated with the need that companies should disclose how they use data (.537). The connection was slightly weaker in the case of general (.356) and GDPR-related (.324) data disclosure, and the connection was weak (.145) with the need that users should know how the date is used. The way how data is used is also correlated with the need to transparent and visible data disclosure both in general (.397) and related to GDPR (.331), and it correlated weakly with the conscious use of data (.168). The correlation between general and GDPR-related transparent data disclosure is moderately strong (.489), and their correlation with the deliberation of users' data processing is moderately weak generally (.237) and in the case of GDPR, too (.297). These results show it clearly that questions related to data protection and privacy are connected to each other in many ways, and a synchronized management is needed from companies and regulatory bodies.

Conclusions

In sum, it can be stated that the general data protection regulation (GDPR) may be a significant progress in personal data management from a legal aspect. The centre of gravity of the European-level regulation shifted from the affected people's rights towards the obligations of data management already at the time of legislative planning of GDPR regulation. Furthermore, GDPR itself extends the scope of data protection as well. Although it can be considered to be a European regulation, it can also be applied to every person or organisation which collects data or transmits information about EU citizens. The regulation entered into force on May 25, 2018, and this empirical research focused on the perceptions related to the regulation, because it is assumed that one year must have been enough for citizens to perceive the changing data management environment due to the regulation.

With this empirical research the study sought to highlight that users take into consideration both this legal environment and, generally, all data protection directives during their perception. Therefore, it is reasonable from a legislative point of view that the protection of personal data and generally, privacy should regulate all the affected areas. This can thereby increase users' perceived sense of security, providing an opportunity to have control over personal data and providing affected people with information about their use. The year that has passed since the introduction of GDPR also points out that making people get to know and understand regulations in detail would necessitate further information tasks, in order to citizens make themselves more aware of regulations related to data protection issues.

In the future, it may be an interesting research area to analyse the opportunities given by the GDPR regulation in a practical context, especially via the examination of users' behavioural characteristics. The analysis of the actual activities (e.g. if they apply special data protection settings on social media websites, if they read the privacy policies of service providers, whether they have prohibited the management of their data on certain websites) as the continuation of the present research would provide a more holistic insight into GDPR regulation with great complementary results by revealing the connections among users' perceptions.

References

Act CXII of 2011 on information self-determination and freedom of information. https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf (Last accessed: June 18, 2019).

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Proceedings of the 6th Workshop on Privacy Enhancing Technologies* (pp. 1-16.). PET.

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, 42, 465-488.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32, 665-683.

Alashoor, T., & Baskerville, R. (2015). *The privacy paradox: The role of cognitive absorption in the social networking activity* (1-20.). Thirty Sixth International Conference on Information Systems, Fort Worth.

EC (2019): European Commission: What is personal data? Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu (last accessed: 12 April, 2019).

EU (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). EUR-Lex Access to European Union Law. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (Last accessed: May 4, 2016).

Fox, A., & Royne, M. (2018). Private information in a social world: Assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice*, 26, 72-89.

Geospatial World: How GDPR will impact location data. Retrieved from: https://www.geospatialworld.net/article/how-gdpr-impacts-location-data/ (Last accessed: May 23, 2018).

Greengard, S. (2018). Weighing the impact of GDPR. *Communications of the ACM*, 61, 16-18.

Hughes-Roberts, T., & Kani-Zabihi, E. (2014). On-line privacy behavior: using user interfaces for salient factors. *Journal of Computer and Communications*, 2, 220-231.

Kotler, P., & Keller, K.L. (2012). *Marketing Management*, N.J.: Prentice Hall, 2012.

Madden, T.J., Ellen, P.S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin*, 18, 3-9.

Schmeiser, S. (2018). Online advertising networks and consumer perceptions of privacy. *Applied Economics Letters*, 25, 776-780.

Tankard, C. (2016). What the GDPR means for businesses. *Networking Security*, 5-8.

Williams, M. (2018). *Exploring the influence of privacy awareness on the Privacy Paradox on smartwatches*. University of Oxford, Doctoral dissertation, 2018.