Managing personal data in a digital environment - did GDPR's concept of informed consent really give us control?

Gergely G. Karácsony

Széchenyi István University Faculty of Law. 9026 Győr, Egyetem tér 1. Hungary.
karacsony@sze.hu

Abstract: As GDPR shifted the legislative focus toward a more human rights-based approach to privacy, consent became an even more important legal basis for handling personal data. In this paper I examine some of the shortcomings of the 'informed consent' principle of GDPR. Some of these shortcomings stem from the large amount of information privacy notices contain, while being written in a difficult legal language. Other issues rise from inherent psychological biases that make us disregard long-term adverse effects for short-term benefits. Finally I agree that simplification and standardisation together with education and raising awareness can help overcoming these issues.

UDC Classification: 341, 342.7

Key words: Consent, Privacy, GDPR, Data protection, Personal Data, Technology and law, Internet, Online

Introduction

In 2016 the legislative bodies of the European Union have enacted a regulation that is likely to shape our way of thinking about privacy in the next decade all around the globe. The General Data Protection Regulation[1], or GDPR in short, represents a great step forward in securing individual rights and freedoms concerning privacy in the digital age. Many of its rules explicitly deal with new technologies, such as artificial intelligence, automated decision-making, Big Data, and the internet. As the regulation itself points out in its recitals, technology has transformed both the economy and social life. The legislator's goals are twofold: ensuring the free flow of data to help business going, while ensuring a high level of the protection of personal data.[2]

As far as the legislator is concerned, they can be satisfied enough, because the new regulation represents a modern approach to a modern issue: protecting privacy in the age of information. The legislator sets forth that recent technological and economic developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data.[3] When discussing GDPR, one theoretical and philosophical characteristic should be pointed out: the regulation took a human rights approach to privacy, instead of a more technical, administrative one. It seeks to give back control over their personal data to the data subject, whereas placing

[1] 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
[2] GDPR recital (6)
[3] GDPR recital (7)

more emphasis on the obligations of the data controller to operate in a transparent and lawful manner.[4] In a human rights context, we should put it this way: the legislation seeks to provide a greater extent of autonomy for persons in making decisions concerning their privacy. That means, they get to make the decision whether they allow certain data management actions for a data handler or not. In this paper, I will argue that this concept of giving the control to the individuals has some flaws in the reality of everyday activities in an online context.

Legislative context

GDPR was announced as a powerful tool of regaining control over personal data, empowering individuals to make the most important decisions concerning the handling of their personal information. It all boils down to consent, as the main legal basis of processing personal data. Consent is one of the six conditions laid down in Article 6 of the GDPR, as being the only legal bases for lawfully processing personal data. Out of these six conditions, consent is somewhat of a 'Jolly Joker', since it is the only one that can be applied in all kinds of conditions, regardless of any other circumstances. All of the other 5 points of this Article apply only if certain preconditions are met: a contractual relationship exists between the data subject and the data processor, a legal obligation is vested on the data processor, etc. Therefore, we can consider consent as the most versatile legal basis for lawful data processing, since it requires none other conditions except for the consent to be expressed by the data subject.
Whereas consent is the easiest way to process data lawfully form the data processor's point of view, it is also the one that gives the most control to the person during the entire lifespan of data processing, including the right to withdraw their consent at any time, as well as the right to the erasure of their processed data ('the right to be forgotten'). These measures enable the person to control the processing of their personal data at any given time, and to stop the data processing if they find it necessary.

Informed consent means, in the context of data processing, that the person making the decisions about the processing of their personal data, has to have all the necessary information needed to consider the consequences of their consent. The GDPR places great emphasis on giving all the necessary information to the data subject in order for them to be able to assess all the circumstances and consequences of a certain data processing activity they are about to give their consent to. It is the obligation of the data controller to provide the obligatory information about the data processing to the data subject at the time when personal data are obtained, that is, before the actual processing of data takes place. Articles 13 and 14 give a list of the information that the data controller has to tell the person in this occasion. The principle of transparency sets forth that such communication should take place in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or

[4] Clifford D. – Graef I. – Valcke P. (2019): Pre-formulated Declarations of Data Subject Consent— Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. German Law Journal (2019), 20. p682.

by other means, including, where appropriate, by electronic means.[5] This regulation eliminates the formerly widespread practice of – almost illegible – small fonts in privacy notices and disclaimers, as well as overly complicated or ambiguous language. It also obliges data controllers to make their privacy notices easily accessible at all times, which gave rise to the appearance of permanent 'Privacy' links on websites.

Considering all the above mentioned regulations in GDPR, we can see that the legislator took great care to work out the details and specific rules of informed consent to data processing. The data controller has very specific obligations concerning the information that should be given to the person before obtaining consent to data processing. The data subject therefore can be sure that he has all the information he needs for the deliberation of giving his consent to a specific data processing activity. Although this regulation has all the safeguards necessary for a transparent process and an informed consent, it has some inherent and some practical shortcomings, which I will examine in the following points.

Issues regarding informed consent in an online context

Above we have briefly looked at the main regulations concerning consent as the legal basis of data processing. GDPR defines the concept of informed consent regarding privacy decisions. In the everyday use of online services, however, it turns out that the legal basis of consent is only used as an easy access to the personal data of someone, whereas the statement thus obtained neither is informed, nor is actually a real consent.

First, let us look at the declaration being informed. In a human rights context, informed consent means a decision made in the possession of all the information necessary to assess all of the implications of a decision to one's rights and liberties both short and long term. With this information at hand, the person can weigh the costs and benefits of giving or withdrawing consent to a certain operation. GDPR clearly identifies all the information to be disclosed to the data subject. Data controllers have adapted their practices to these regulations fairly quickly, and GDPR compliant privacy notices and consent forms have appeared. Although, upon examining these documents, we find that in the everyday use they have many shortcomings that make it harder to consider the data subject informed.
The information GDPR deems to be necessary to give to the person, creates a significant information overload. Privacy notices tend to be lengthy documents with detailed explanation of privacy practices of the service provider. For the sake of this paper, I have examined the length of privacy notices of some of the most famous businesses online. Some of the results are quite shocking: social media sites have privacy documents nearly 35 000 characters long (10 full pages), the ones of online booking services reach the length of 56 000 characters (16 pages), even a news site's privacy statement is at least five full pages (17 000 characters) in length. Using the services of a major international hotel chain can set the person back with reading

[5] GDPR Article 12, point 1.

57 000 characters, or 16 pages full.[6] Based on this data, it would take a significant amount of time to read all of the privacy statements thoroughly, which would be a necessity if one wanted to make a truly informed decision. The length of these documents is a clear effect of GDPR's attempt to provide all the information to the person in concern: it lists at least 30 required elements of a privacy notice, all of which tend to be at least a paragraph long in writing.
These texts also tend to be overly complicated and legalistic, using a 'GDPR lingo' not easily comprehendible for everyday users. Such complexity hinders cognition greatly, when presented to a person without previous legal training or routine in comprehending such documents. This phenomenon is probably because these texts are mostly written by the lawyers of these firms with one goal in mind: protecting their employer from future lawsuits and the potential of a significant fine.[7] Therefore they tend to cover all the data processing practices in a very precise, legally refined and detailed explanation. The language of these statements are sometimes ambiguous or manipulative: they tend to overstate the positive effects of consent and brush off the risks by a few short and seemingly harmless statements. Sometimes ambiguity stems from the technical reality that with the rise of Big Data and artificial intelligence based data mining techniques firms may find it impossible to provide adequate notice for the simple reason that they do not (and cannot) know in advance what they may discover.[8] Therefore sufficient notice and detailed explanation is not possible.

As we examined above, in the everyday reality it is hard to tell whether the consent given is actually informed, or just overloaded with information, and therefore actually uninformed or ignorant. Information overload tend to be a great issue these days, when time is a scarce resource, and people do not have the patience (or willingness) to read tens of pages of legal jargon before ordering goods online or checking out the news. Presenting the person with the entirety of the required information included in GDPR may seem contraproductive: there is a chance that they will just skip the privacy notice altogether, rather than read the whole 10-15 pages long document.

The other issue is with the nature of the consent itself. It is widely accepted that consent should reflect the person's autonomy in deciding upon giving up or preserving parts of his privacy in a given context.[9] However, several circumstances hinder the expression of the data subject's free will, thus making consent virtually an empty statement.

First, we have to mention the inherent biases and short-sightedness of data subject when making decisions on privacy matters. Tal Zarsky emphasizes that "consumer myopia"[10] is one of the

[6] data obtained by the author from the English language privacy notices of amazon.com, ebay.com, booking.com, google.com, facebook.com, bbc.com, and hilton.com
[7] Jarovsky L. (2018): Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs). European Data Protection Law Review 4/2018. p 449
[8] Rubinstein I. S. (2013): 'Big Data: The End of Privacy or a New Beginning?' International Data Privacy Law, 2013, Vol. 3, No. 2. p78.
[9] Jarovsky L. (2018): Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs). European Data Protection Law Review 4/2018. p 452
[10] Zarsky T. (2004): Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society, Maine Law Review 56, no. 1. p41

common problems affecting the use of personal data by businesses. Consumers do not have the right toolkit to judge the benefits and disadvantages of transferring their personal data. Online merchants often fail to make consumers aware of how data is collected, analysed and used, and consumers are not able to assess the potential negative consequences of sharing their personal data. In the recent past many cases revealed that online businesses use personal data for purposes well beyond the imagination of an average user, such as personalised pricing.[11]
By this manipulation, several inherent behavioural biases kick in as well, such as hyperbolic discounting, overconfidence, status quo bias, and rational ignorance.[12] Hyperbolic discounting is an interesting phenomenon among these, which means that people tend to prefer activities that reward immediate benefits, even if they carry long-term damages or risks.

We expect that the average person takes the time to gather information and ponder on giving consent to data processing in a historical and social situation where people are becoming more and more accustomed to meeting their needs instantly, in a fast-paced world where slow reflection and careful consideration lost any of its positive connotations. On top of this, in most cases, privacy notices and consent forms are presented to the user at the end of the purchase or registration process, when there is already a virtual shopping cart full of the desired goods or services barely at their fingertips; all that separates them is just a 'quick administrative formality'. In such a situation, it seems unlikely that the user interrupts the purchase or registration due to the service provider's data management practices, loses the work he has invested so far and, undertaking the associated frustration, he is looking for another provider or renounces his wishes. We may also consider it more likely that the user will only scan the information or not read it at all.[13] One result of framing technological engagement as voluntary rather than necessary is that when users disclose personal information in the course of normal online activity, that too is viewed as a voluntary disclosure, even when users are completely unaware that any information exchange is occurring.[14] Also, despite increasing attention drawn to the issue of online information privacy, many consumers seem to accept that some loss of privacy is a cost of doing business in the digital age. Numerous studies of consumer behaviour on social networking sites reflect users' tendency to disclose personal information on their profiles despite expressing generalized privacy concerns.[15]

The next issue can be paraphrased as the development of the 'circles of trust'. Recently, as large numbers of data protection warnings appeared on almost all forums, and huge privacy scandals were reported by the press, user behaviour has changed in the online services market. People

[11] Karácsony G. G. (2018): Automatizált személyre szabott árazási megoldások az online kereskedelemben. In: Glavanits J. (ed.) A nemzetközi kereskedelmi kapcsolatok egyes aktuális kérdései. Budapest, Gondolat Kiadó, pp.81-94.
[12] Acquisti A. – Grossklags J. (2007): What Can Behavioral Economics Teach Us about Privacy? in Acquisti A. et al (eds): Digital Privacy: Theory, Technologies, and Practices (CRC Press) pp 368-372.
[13] Ződi Zs. (2017): Privacy és a Big Data. Fundamentum 2017. 1-2. p 23.
[14] Ness D. W. (2013): Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy As We Know It. Cardozo Arts & Entertainment Law Journal vol. 31:2013. p 928-929.
[15] Brinson N. H. – Eastin, M. S. (2016). Juxtaposing the persuasion knowledge model and privacy paradox: An experimental look at advertising personalization, public policy and public understanding. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(1), article 7. p5.

are becoming more cautious and suspicious when a service provider asks for personal information. However, this did not necessarily brought around the result that one might expect in the first place, because, as research suggests, the average person will give their data to providers they trusted more easily, while they were more distrustful towards the less well-known data controllers. This has a clear effect to the market, so that the already big providers (such as Google and Facebook) will have an increasing share of the information society services market, while smaller companies lose their position due to the mistrust of users and slowly they can even fall out of the market.[16] In the long run, this can have a two-way consequence: our personal data will be concentrated in the hands of a small number of service providers and, in parallel, more and more personal data will accumulate at the remaining providers. Together, these two provide the large service providers with unprecedented influence: their operation affects the exercise of the right to express opinions, the formation of political opinions and the spread of news or even fake news.

Somewhat connected to the previously discussed issue is the phenomenon that most – if not all – of the service providers present their privacy notice and consent form as a take it or leave it offer. The user can decide to go along with the data collection and processing as it is requested by the provider, or to not have access to the service at all. Although GDPR formulates it clearly[17] that consent to data processing cannot be a requirement for providing a service, unless such consent is necessary for the provision of such service, it leaves it up to the data controller to determine what extent of data processing is necessary. This means that basically the service providers can exclude people from their service unless they consent to the data processing practices. In many cases, this exclusion means the complete lack of access to common services, or to services not available in any other form (e.g. social media platforms or online shopping). That makes consent only virtual, since no real alternative is given to the data subject, they have to decide whether they want to access the service in question or not, no roads being in between.

Finally, one of the most severe and global issue is the lack of education, practice, and experience in this field. Technological and economic development brought along the advent of the data-based economy and new business practices with such an unbelievable speed that almost no-one can keep up with the newest development in business practices. The speed with which technology evolved has led to adoption without comprehension. In many realms, people are increasingly expected to be competent in using these new technologies, regardless of whether they have ever had any in-depth training in or an understanding of the inner workings of these systems.[18] Using online services, ordering goods, booking trips, and getting involved in social media became so commonplace that we no longer think about it as a special technical process. This does not mean, however, that an average user has any kind of knowledge or experience in how these technologies really work, how they use personal data, and what happens with the

[16] Google and Facebook Likely to Benefit From Europe's Privacy Crackdown. The Wall Street Journal Online, 2018. 04. 23. https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324 (2018.08.06.)
[17] GDPR Article 7. point 4
[18] Ness D. W. (2013): Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy As We Know It. Cardozo Arts & Entertainment Law Journal vol. 31:2013. p 928-929.

collected and processed personal data in the long run. There was no time for experience and best practices to build up, or trust to be formed towards one data handler or another. Most of the users navigate blindfolded when making decisions concerning privacy. Consent, therefore, cannot be interpreted as a truly autonomous and well-founded decision, but rather an expression of anticipation, sympathy or trust towards a service provider.

Conclusion and possible solutions

Previously we looked at the legal regulations concerning the informed consent principle of GDPR. It is clear that the legislator intended to elevate consent to the most important legal basis for data processing, situating it at the core of the logic of the regulation. This happened with the purpose of emphasizing the human rights approach to privacy issues, and thus giving control to the person over their data. Informed consent also means that the data subject has to be provided with every detail needed to make the decision. We discussed that this approach has its shortcomings, both in the field of being informed, as well as the consent being the result of an actual deliberation and weighing one's options. The main issue with the information part is the amount and the complexity of the information GDPR requires data controllers to disclose before collecting personal data. Upon the consent itself, we could point out that several cognitive biases take action in such a situation, whereas the average user lacks the proper education and experience to make an informed decision. Finally, sometimes no real alternatives are presented to the data subject, they have to consent to the processing of their personal data in order to access some services or goods in an online context.
Is there a way to overcome these issues and reach the core of the legislator's intent, truly giving back control to the person over their data? The academic sources in this matter are almost consensual on the fact that consent is and will be the best way to ensure the autonomy of a person regarding decisions about their privacy. Eliminating or reducing the use of consent is not a viable alternative, since it almost surely diminishes the extent of autonomy of the data subjects. There are however some suggestions to improve the functionality of consent.

The first suggestion is simplification. Most of the contents of a privacy notice can be standardised, and presented in a simplified, short form. Many if the information such policies contain are not to any immediate use of the data subject (e.g. their rights and remedies will only be a matter of interest if they have any problem or request regarding the processing of their data). The informed decision is usually made with regards of the following points of interest:

- the purpose of data collection and processing
- the ways collected data will be used and its consequences (e.g. targeted advertisement, personalised pricing)
- forwarding the data to third parties

This information can easily be represented in a short written form, or even by pictographs or icons. This way the data subject can quickly assess the main points of interest, and if he isn't comfortable with the intended purposes of his personal data, he can choose not to give consent. If any more detailed information is needed, he can take the time to read through the full text

version of the privacy notice. In the early stages of legislation, there was a suggestion to implement a system of icons representing various information about the data processing. This icon concept did not make it to the final version of the regulation, although according to various authors it represents a very user-friendly approach, not different from many other system of pictograms people already use in everyday life (e.g. laundry signs, or the icons of operation systems and computer programs). The actual icon system suggested during the parliamentary phase of the legislative process is somewhat crude and hard to comprehend, studies suggest that uneducated users don't recognise these icons as ones connected to privacy at all.[19] Although with some more forethought and better design, I believe that a standardised icon system would actually improve awareness among data subjects, contributing to a more deliberate decision on consent. It is a necessity to standardise these icons, because great divergence in the used pictographs would lead to more confusion. GDPR can be an excellent vehicle in introducing such measures and icon systems, since it already serves as the gold standard of privacy all around the world, so the adaptation of its measures should be expected worldwide. GDPR already enables data controllers to display the required information using standardised icons[20] as well, but as of now such icon sets have not appeared in practice.

The other factor is education. With the proper education of users, many of the contents of a privacy notice become obsolete. For example, the rights of a data subject doesn't have to be repeated in every consent form he signs, because he is already aware of them. Education of course doesn't eliminate the need to point out the rights and obligations of the data subject, but it makes these formulas more familiar, and reduces the need to make the educational parts the core element of privacy notices. With proper education the level of awareness can be raised concerning the long-term effects of certain data processing practices, and in the long run better informed public opinion can drive away malicious business practices.

[19] Pettersson J. S. (2014): A brief evaluation of icons suggested for use in standardised information policies - Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011. Universitetstryckeriet, Karlstad.
[20] GDPR Article 12. points 7 and 8.

References

Clifford D. – Graef I. – Valcke P. (2019): Pre-formulated Declarations of Data Subject Consent— Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. German Law Journal (2019), 20.

Jarovsky L. (2018): Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs). European Data Protection Law Review 4/2018.

Rubinstein I. S. (2013): 'Big Data: The End of Privacy or a New Beginning?' International Data Privacy Law, 2013, Vol. 3, No. 2.

Zarsky T. (2004): Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society, Maine Law Review 56, no. 1

Karácsony G. G. (2018): Automatizált személyre szabott árazási megoldások az online kereskedelemben. In: Glavanits J. (ed.) A nemzetközi kereskedelmi kapcsolatok egyes aktuális kérdései. Budapest, Gondolat Kiadó, pp.81-94.

Acquisti A. – Grossklags J. (2007): What Can Behavioral Economics Teach Us about Privacy? in Acquisti A. et al (eds): Digital Privacy: Theory, Technologies, and Practices (CRC Press)

Ződi Zs. (2017): Privacy és a Big Data. Fundamentum 2017. 1-2.

Brinson N. H. – Eastin, M. S. (2016). Juxtaposing the persuasion knowledge model and privacy paradox: An experimental look at advertising personalization, public policy and public understanding. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(1), article 7.

Google and Facebook Likely to Benefit From Europe's Privacy Crackdown. The Wall Street Journal Online, 2018. 04. 23. https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324

Pettersson J. S. (2014): A brief evaluation of icons suggested for use in standardised information policies - Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011. Universitetstryckeriet, Karlstad.

Ness D. W. (2013): Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy As We Know It. Cardozo Arts & Entertainment Law Journal vol. 31:2013.