DOI: 10.1007/s10272-017-0676-5

End of previous Forum article

Maciej Sobolewski, Joanna Mazur and Michał Paliński

GDPR: A Step Towards a User-centric Internet?

Originated as a collaborative research project and designed as a decentralised network of networks, the internet was founded on the principles of openness, transparency, non-discrimination and user-centricity. The two fundamental elements for user-centricity are freedom of choice and ability to exercise control upon one's own online activities.[1] Since these origins, this network of networks has undergone substantial changes, casting doubts on whether the fundamental principle of user-centricity is still valid today. Firstly, the rapidly growing role of the internet as a commercial marketplace has shifted the focus to consumption of content and away from end-user service creation. Secondly, the rise and success of business models based on multi-sided intermediation, utilisation of personal data and monetisation of network effects has shifted the balance of control and power away from end-users. Incidents of competitive misconduct by dominant online platforms or abuse of personal data have led

Maciej Sobolewski, University of Warsaw, Poland; and European Commission, Seville, Spain.

Joanna Mazur, University of Warsaw, Poland.

Michał Paliński, University of Warsaw, Poland.

1 Internet Society (ISOC): Preserving the User Centric Internet, Discussion Paper, 2009.

to calls to reinforce user control, based on a return to the user-centric origins of the internet.

This paper discusses upcoming personal data protection reform in the EU from the user-centricity perspective. The new regulation – the General Data Protection Regulation (GDPR) – introduces extensive informative obligations on service providers and grants users with rights to data erasure, to object to processing, to the portability of data on request and to object to profiling.[2] These protection measures, as well as new obligations for providers to ask for explicit consent to collect data for all specified purposes, greatly enhance the control of end-users over the utilisation of their personal data online. While the potential empowering impact of the GDPR is huge, we argue that the ambivalent attitudes of users towards data protection, as well as the risk of differentiation of legal practice among member states, can seriously limit the real effects of the privacy reform.

The right to export on request all personal data collected by the given online provider is the key novel element of GDPR. Incumbent providers will no longer enjoy advantages resulting from the exclusive use of large volumes of user-generated data. As a consequence, portability dramatically lowers barriers to entry for innovative services and opens the market for business models in which personal data is controlled and leased by the users instead of being a sort of non-monetary currency paid in exchange for access to nominally free services. We argue that potential benefits from data portability are clearly underestimated by end-users, and therefore there is a need for its empowerment. Of particular importance is treating this instrument in an unrestricted and user-friendly manner to the broadest possible extent.

Protection of personal data in the EU – legal perspective

The approach towards privacy represented in EU law is based on the fundamental assumption that the right to privacy and the protection of personal data are basic human rights. Privacy is protected by the Charter of Fundamental Rights, in Articles 7 and 8, as a right of an individual.[3] There is tension between this approach and an alternative view that is currently gaining traction, according to which data is regarded as a tradable asset and is becoming a kind of online currency. This tension represents a challenging dichotomy of the online world.

According to the definitions in the GDPR, "personal data" means any information relating to an identified or identifiable natural person described as a data subject.[4] The functional approach towards defining personal data allows for a wide range of identifiers to be classified as such, as technology and online behaviour progresses even further.

Current and future legal framework

Currently, the legal ground for privacy protection in the EU is Directive 95/46. Electronic communication, however, is subjected to special regulations based on the regulatory framework of the ePrivacy Directive.[5] Both documents have since been perceived as inadequate for a growing data-driven economy, and therefore the member states agreed upon the necessity of implementing major reforms regarding the data protection framework.

The GDPR will come into force on 25 May 2018. Even though it will provide a unified framework concerning data protection for all the member states, countries would still be able to regulate to some extent the execution of rights and obligations created by the GDPR.[6]

The selection of regulations as a tool for data protection unification in EU member states has some important consequences. Regulations become immediately enforceable in all member states simultaneously. In contrast to directives, regulations do not need to be transposed into national law; in fact, this is forbidden. However, it is necessary to implement certain legal acts, for example concerning procedural aspects of the regulation or providing catalogues of exemptions, which can result in divergences in terms of the effects of the GDPR.

Unified or diversified legal practice?

Member states implement regulations for the handling of privacy cases (in accordance with the procedural autonomy of the member states) as well as solutions for the institutional environment. This may lead to a differentiation of legal practice.

2 European Parliament: 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), in: Official Journal of the European Communities, No. L 119, 4 May 2016.

3 European Union: Charter of Fundamental Rights of the European Union, in: Official Journal of the European Communities, No. C 365, 18 December 2000, pp. 1-22.

4 European Parliament, op. cit., p. 2.

5 Directive 2002/58/EC of the European Parliament and of the Council, 12 July 2002

6 J. Chen: How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation, in: International Data Privacy Law, Vol. 6, No. 4, 2016, p. 310.

Firstly, the autonomy of the member states allows for implementing national solutions, which can determine the extent to which the data subject's rights will be guaranteed. Even though the GDPR contains the possibility of significant financial sanctions in the case of non-compliance by data processors or controllers, the role of national regulations in providing their institutions with an appropriate framework to use options created by the GDPR should not be disregarded. The financial and organisational independence of national institutions responsible for privacy protection are crucial factors which cannot be underestimated.

Secondly, the derogations allowed for in the GDPR may lead to a differentiation of the scope of protection depending on national regulations. According to the GDPR, such derogations are allowed

> where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.[7]

Even though recital 54 of the GDPR introduces limitations concerning the possibility to process this data for other purposes by third parties, such as employers or insurance and banking companies, it is difficult to foresee how states will use the possibilities which they are granted by these exemptions. However, the jurisprudence of the Court of Justice of the European Union (CJEU) thus far proves that terms such as "public interest" should be interpreted carefully and the implemented solutions always need to be proportionate to the aims they serve.

Thirdly, a lack of regulation could also result in national divergences. For example, the GDPR does not regulate conditions under which profiling (understood as combining and processing personal data) may be used if a human factor is involved in this process. This means that the existence of mechanisms which allow human intervention in the processing leads to a state's ability to regulate the processing in its national legal system. The regulation does not introduce strict transparency imperatives concerning the algorithms which determine the outcome of this profiling. As the evolution of legal practice will be bound and partly determined by the development of technologies helping either to avoid or achieve compliance with the general rules of European privacy protection, it can be expected that new issues regarding internet privacy will soon emerge.

7 European Parliament, op. cit., p. 10.

Last but not least, some differences in legal practice which may occur will be due to the innovative character of some of the implemented solutions. Therefore, selected terms such as "automated processing" or "portability" still have not been sufficiently clarified.[8]

Legal concepts of GDPR

The GDPR introduces new institutions and also changes existing ones. The foundations for the new legal state of the art are the explicit concepts of data protection by design and by default.[9] They refer to the necessity of implementing data protection tools at the stage of creating the system which is used to collect data and in creating rules for the users. Assuming minimisation of personal data collection and use, both concepts provide the basis for the EU's data protection reform and should guarantee an adequate level of protection.

However, it should be noted that processing anonymised data is understood as complying with the privacy by design and privacy by default rules. This may raise concerns regarding the efficacy of data protection by design as it is defined in the GDPR. Well-known cases of data breaches – such as AOL in 2006[10] and Yahoo in 2014[11] – prove anonymisation to be a hardly satisfying data protection measure.

Consent to processing

One of the conditions under which data processing is lawful is if the user provides consent. Therefore, it is crucial how "lawful consent" will be understood under the GDPR. According to the GDPR, consent must be given by a statement or a clear affirmative action.[12] Moreover, consent should cover all processing activities carried out for the same purpose or purposes. In cases in which the processing has multiple purposes, consent should be given for each one. The GDPR directly claims that consent is

8 In this respect, it is worth mentioning the opinions contained in Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent, 01197/11/EN, WP187, 13 July 2011, which may help to unify the understanding of main concepts.

9 European Parliament, op. cit., p. 48.

10 The AOL data breach in 2006 led to the possibility of identifying certain individuals even though the data were anonymised. Documents regarding the legal action against AOL and the final settlement can be accessed online at https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/05/final-as-filed-landwehr-settlement-agreement.pdf and https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/05/https-ecf-vaed-uscourts-gov-cgi-bin-show_doc-pl-ca.pdf.

11 Another enormous data breach concerning Yahoo users resulted in legal action; see In re Yahoo! Inc. Customer Data Security Breach Litigation, Case No. 16-MD-02752-LHK, Order Selecting Lead Plaintiffs' Counsel and Plaintiffs' Executive Committee.

12 European Parliament, op. cit., p. 6.

presumed not to be freely given if a contract depends on this consent despite the data collection not being necessary to fulfil the contract.[13] The conditionality of a selected user's rights, which depend on the fact that processing was performed with the user's consent, may also be used to weaken the user's position as subject of the personal data. After all, one might argue, that "the consent model operates to undermine privacy and to some extent facilitates surveillance".[14]

Information requirements

The GDPR lists 12 categories of information that should be provided to the data subject. The data controllers will be obliged to provide the data subject not only with the identity of the data collector and the relevant data protection officer, but also about the aim of the data collection and about the handling and storage of the data. The GDPR requires that information should be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[15]

Right to erasure and right to object to processing

The GDPR strengthens the user's rights both to object to processing of data (through Article 21) and to demand erasure of one's data (the right to be forgotten). Article 17 of the GDPR contains a catalogue of situations in which "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay".[16] This clarifies the conditions under which it is possible to refer to the right to be forgotten as defined by the CJEU. The grounds for demanding erasure have to fulfil the conditions set out in the GDPR. Even though the catalogue of situations which allow the data subject to demand the erasure of data seems to be broad, there are some problems, such as the fact that third parties might have different arguments regarding the lawfulness of the data processing, which weakens the meaning of the right to erasure.

13 An example would be a situation in which one wants to purchase a service which is performed via the internet and the data processor demands e.g. the user's home address and consent for sending the advertisements via the post. This type of consent would not be regarded as freely given, because it not only leads to demand for data which is not necessary for the contract's performance, but which is also not necessary to perform the contract. See ibid., p. 8.

14 A. Sarat (ed.): A World Without Privacy: What Law Can and Should Do?, Cambridge 2014, Cambridge University Press.

15 Article 12 of the GDPR allows the use of graphic icons to fulfil the informative obligations: "The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing". See European Parliament, op. cit., p. 39.

16 Ibid., p. 43.

Right to data portability

The right to data portability creates a new right for the data subject. According to Article 20 of the GDPR,

> the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit this data to another controller.[17]

If the data is subjected to automated processing, the controller is obliged to fulfil the request of the data subject "without undue delay and in any event within one month of receipt of the request".[18] The actual meaning of the right to data portability will depend on the efforts to be made to gain possession of the data and the willingness of the customers to use the new opportunities.

Automated processing including profiling

According to Article 4 of the GDPR, profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person".[19] The legal perspective varies according to the aim and result of the profiling. For example, the data subject may object to processing for direct marketing purposes. Article 22 guarantees the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[20] Examples of such situations could be automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Economics of online privacy and GDPR

In 2010 Facebook aroused a controversy by introducing new default privacy settings for its 350 million users. According to numerous civil liberties campaigners, as well as some consumer protection organisations, the change was clearly intended to push the platform's users to expose more personal data online while decreasing their control

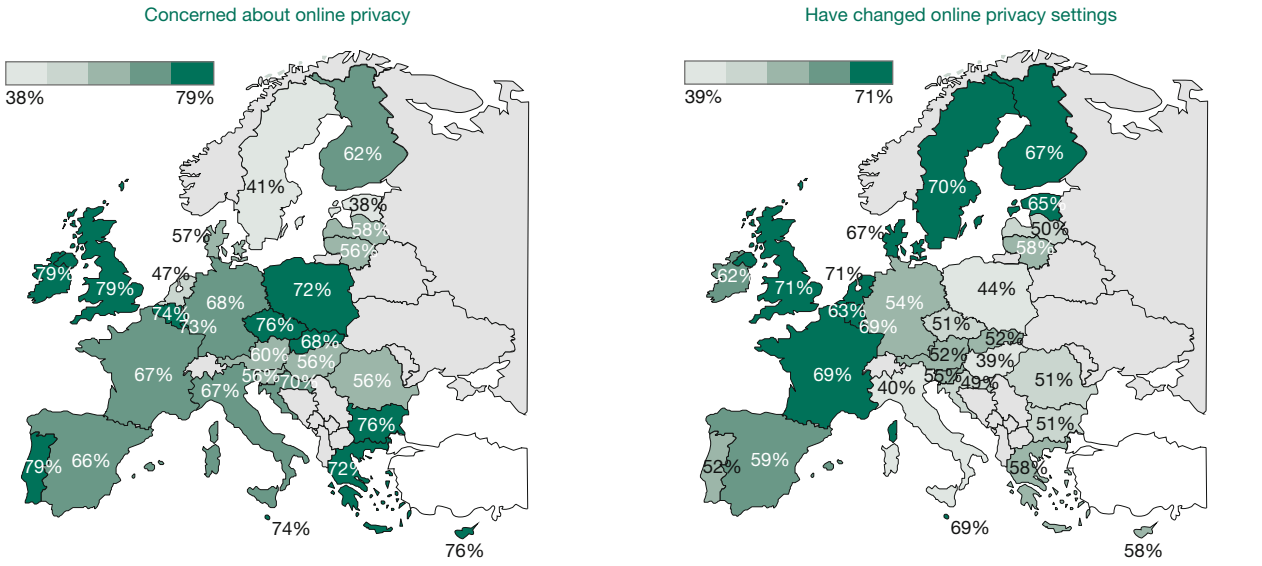
17 Ibid., p. 45.

18 Ibid., p. 39.

19 Ibid., p. 33.

20 Ibid., p. 46.

Figure 1
The privacy paradox across the EU



Note: Left pane: Concern about not having complete control over the information provided online (among respondents who feel that they do not have complete control over their personal data online). Right pane: Respondents who have tried to change the privacy settings of personal profile from the default settings on social networks (base: respondents who use online social networks). nleft = 16,244; nright = 15,339.

Source: Own elaboration based on data from European Commission: Special Eurobarometer 431. Data Protection, Wave EB83.1, 2015.

over this shared information.[21] However, Facebook CEO Mark Zuckerberg justified the privacy changes at that time by claiming that:

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.[22]

Is privacy in the digital era a thing of the past? The Exponential growth of online platforms fuelled by the utilisation of personal data and the development of predictive analytics, which eases the re-identification of anonymous individuals, support this statement.[23] Nevertheless, the European Commission still plans to extend oversight over companies that process the personal data of EU citizens, primarily through the GDPR – a regulation that aims to replace the outdated Data Protection Directive of 1995, implemented at a time when less than one per cent of EU citizens used the internet.[24]

Ambivalent attitudes towards online privacy

The Commission justifies the new data regulation to a large extent as a means to allay the privacy concerns of private individuals.[25] But do internet users really care about having control over personal information they share online? Surveys and polls show that online privacy is indeed an important concern for EU citizens. According to the results of the 2015 Eurobarometer comprehensive survey, more than eight out of ten respondents across the EU feel that they do not have complete control over their personal data online.[26] Among them, two-thirds are concerned about that fact (see Figure 1). On the other hand, studies indicate that individuals tend to reveal their personal data for a low level

21 See K. Bankston: Facebook's New Privacy Changes: The Good, The Bad, and The Ugly, Electronic Frontier Foundation, 9 December 2009, available at https://www.eff.org/de/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly. The privacy setting change gave users the ability to alter settings on items they upload to the site, such as photographs and videos, but all of their status updates were automatically made public unless specified otherwise.

22 B. Johnson: Privacy no longer a social norm, says Facebook founder, The Guardian, 11 January 2010.

23 See K. Crawford, J. Schultz: Big data and due process: Toward a framework to redress predictive privacy harms, in: Boston College Law Review, Vol. 55, No. 1, 2014, pp. 93-128, and A. Dix et al.: EU Data Protection Reform: Opportunities and Concerns, in: Intereconomics, Vol. 48, No. 5, 2013, pp. 268-285.

24 European Commission: Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World, COM/2017/0007, Brussels 2017.

25 Ibid. The document also contains other arguments pertaining to the benefits for businesses stemming from harmonisation of the legislation of 28 member states.

26 This includes e.g. the opportunity to correct, change or delete personal data. See European Commission: Special Eurobarometer 431. Data Protection, Wave EB83.1, 2015.

of remuneration.[27] Moreover, notwithstanding the stated concern and reluctance to share personal data online, Europeans often do not take basic actions to prevent unwilling disclosure, for example by changing the privacy settings on social networks (see Figure 1). Such inconsistency between declared concerns and actual behaviour marks the ambivalence in attitudes towards privacy. This "privacy paradox" is a well-established concept in the social sciences and has gained a lot of attention from empirical researchers in recent years.[28] The data in Figure 1 indicates the existence of a privacy paradox in the EU, particularly in central and southern member states.

In recent years, numerous studies have tried to explain the privacy paradox, providing logical explanations of the discrepancy between declared concerns and behaviour related to the management of personal data.[29] The most prominent from an economic perspective are based on privacy calculus theory and behavioural privacy economics. Both approaches make contrary assumptions regarding the users' rationality. The former is founded on the premise that agents make rational decisions. The level of online privacy protection is thus a solution to the trade-off between the expected risks and potential benefits of disclosure of personal data.[30] The voluntary disclosure of personal data by people who claim to be concerned about their privacy is justified by the fact that gains from revealing personal data are often intangible, such as peers' attention or social capital. When these intangible rewards are taken into account, they might outweigh the perceived risks and explain the seemingly paradoxical situations.[31]

The behavioural economics approach is based on the claim that users' decisions are to a large extent affected by heuristics and cognitive biases such as optimism and affection bias, overconfidence, fuzzy-boundary, benefit heuristics or hyperbolic discounting.[32] Studies in this field suggest that users are vulnerable to underestimation of future risks related to personal data disclosure but that they overestimate current benefits from its disclosure. Behavioural economics argues that since privacy concerns are often expressed generically, they may not correspond directly with the user's actual behaviour.[33]

Valuation of GDPR – empirical evidence

The economic analysis of privacy starts with the observation that personal data has been commodified into a tradeable asset.[34] Implementation of enhanced privacy control mechanisms will help to create a supply side of data markets, generating positive welfare effects for users. According to a recent empirical study undertaken on a sample of digital natives in Poland, this is indeed the case.[35] The gross consumer surplus implied by a combination of extended measures planned in the GDPR equals €6.50 per capita per month – roughly 50% of the monthly broadband subscription fee. Out of the tools provided by the new regulation, the one that individuals valued most highly was the right to be forgotten (€1.40 per month).

The next most highly valued tools were the extended scope of information obligations for providers and the right to object to profiling (each worth €1.00 per month). Interestingly, consumers do not acknowledge data portability as a valuable instrument, despite the fact that it plays a key role in GDPR reform as a potential game changer for the end-user-oriented data markets. The increase in the consumer surplus driven by the GDPR reflects the value of breaking the asymmetry of information and reducing the three major sources of user uncertainty: What data is used online? By whom? And for which purposes?

Conclusions

GDPR reform undoubtedly increases users' abilities to control their personal data online. Concepts such as privacy by design and privacy by default should lead to the more effective implementation of data protection tools. Information obligations on data controllers and processors could also raise end-users' awareness of to what extent and for which purposes their data is being processed. The right to be forgotten and the right to object to processing could play a vital role in allowing users to control the spread of their data on the internet. Therefore, taken as such, GDPR is surely a step towards a user-centric internet. There are,

27 See: Table X-B A. in A. Acquisti, C. Taylor, L. Wagman: The Economics of Privacy, in: Journal of Economic Literature, Vol. 54, No. 2, 2016, pp. 442-492.
28 H. Holland: Privacy Paradox 2.0, in: Widener Law Journal, Vol. 19, 2009, pp. 1-21.
29 In S. Kokolakis: Privacy Attitudes and Privacy Behaviour, in: Computers & Security, Vol. 64, January 2017, pp. 122-134, 18 studies are surveyed providing evidence supporting the privacy paradox hypothesis and 11 challenging it.
30 T. Dinev, P. Hart: Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact, in: International Journal of Electronic Commerce, Vol. 10, No. 2, 2006, pp. 7-29.
31 H. Lee, H. Park, J. Kim: Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk, in: International Journal of Human-Computer Studies, Vol. 71, No. 9, 2013, pp. 862-877.
32 J. Grossklags, S. Hall, A. Acquisti: When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information, in: Workshop on the Economics of Information Security (WEIS), 2007, pp. 7-8.
33 A. Acquisti, C. Taylor, L. Wagman, op. cit.
34 S. Preibusch: The Value of Web Search Privacy, in: IEEE Security and Privacy, Vol. 13, No. 5, 2015, pp. 24-32.
35 M. Sobolewski, M. Palinski: How much do consumers value online privacy? Welfare assessment of new data protection regulation (GDPR), WNE Working Paper No. 17/2017 (245), forthcoming.

however, some risks and impediments ahead, and it is hard to foresee how big this step will actually be.

First, there are still some reasons to suspect that legal practice will not lead to the absolute unification of data protection levels in the member states. The exemptions allowed in the GDPR, the procedural autonomy of the member states and the fact that some of the newly implemented solutions will eventually be shaped by the CJEU will influence the everyday practice of data protection in the EU.

Second, it is hard to tell today whether data portability will become an important instrument that encourages users to move their data between different service providers. Currently, users seem to underestimate its role. However, from a policy perspective, this mechanism is of great importance as a potential game changer which could shift the control over personal data from service providers to end-users and lower barriers to entry for innovative services.[36] The failure of end-users to acknowledge the importance of data portability is an early warning sign with regards to the effective implementation of the GDPR. Hence, keeping this instrument unrestricted and user-friendly to the broadest possible extent is of particular importance.

36 A good example of such services are privacy management platforms, such as Hub-of-All-Things (HAT) or Cambridge Blockchain. They enable users to manage personal data from multiple accounts and services by storing it in a virtual container.