

Łukasz Gołba

Consent for Personal Data Processing in Digital Environment According to GDPR

Roczniki Administracji i Prawa 17/2, 253-265

2017

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

Original article

Received: **25.08.2017**

Accepted: **25.10.2017**

Published: **20.12.2017**

Sources of funding for publication: **author's own resources**

Authors' Contribution:

(A) Study Design

(B) Data Collection

(C) Statistical Analysis

(D) Data Interpretation

(E) Manuscript Preparation

(F) **Literature Search**

Łukasz Gołba*

CONSENT FOR PERSONAL DATA PROCESSING IN DIGITAL ENVIRONMENT ACCORDING TO GDPR

INTRODUCTION

In recent years, with the development of new technologies, a change in the nature of personal data has been observed. This trend is most evident in the digital environment. Attention should be paid to the universality of the processing of personal data and the creation of new forms and ways of using it, which – as it should be emphasized – most often, entails economic benefits on the part of the entity that processes the personal data. It is obvious that there are significant risks to the protection of natural persons, in particular with regard to online activity¹. Meanwhile, personal data are becoming a new type of currency in digital environment². It may be noted that granting consent for data processing

* mgr

¹ See recital 9 of 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), hereinafter referred to as GDPR.

² See remarks stated in the introduction: C. Langhanke, M. Schmidt-Kessel, *Consumer data as consideration*, "Journal of European Consumer and Market Law" 2015, no. 6, p. 218-219; Compare: A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2017, no. 8, p. 9; Y. Hermstrüwer, *Contracting Around Privacy. The (Behavioral) law and economics of consent and Big Data*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2017, no. 8, p. 9; See also: W.D. Eggers, R. Hamill, A. Ali, *Data as currency*, "Deloitte Review" 2013, no. 13 p. 21; F. Zoll, *Personal Data as Remuneration in the Proposal for a Directive on*

may be perceived through the prism of a performance in a relationship, in which, in exchange for the possibility of personal data processing, the person to whom the data concern, has the opportunity to use a particular service or good, totally or partially free of charge.

Laws concerning the consent can be reconstructed both pursuant to the provisions of the Personal Data Protection Act,³ and of the special laws, which pursuant to Article 5 of PDPA, apply if they provide for protection that goes beyond the PDPA⁴. In terms of the European Union law, currently, in addition to Directive 95/46/EC⁵, and a number of other EU acts⁶, the most important act in the field of personal data protection is the so-called General Data Protection Regulation. GDPR shall enter into force on May 25, 2018 when it will be directly applicable. Hence, this will be the basis for the analysis in this publication. Considerations will focus primarily on mandatory elements of the consent and its form. The issues that have raised and continue to raise concerns are doubts about its legal nature, the issue of withdrawal of the consent⁷, the issue of granting it by persons who do not have full legal capacity. The issue of the consent in case it is granted in exchange for the possibility of using “free” services or goods will also be dealt with. It appears that the requirements posed by GDPR, in the scope of granting the consent, may be an obstacle in the context of functioning of numerous mobile applications, websites and social networking sites in the current form.

‘CONSENT’ OF THE DATA SUBJECT

GENERAL INFORMATION AND DEFINITION

One of the bases for authorizing the administrator to process data is the consent of the person to whom the data concern (the data subject). The premises of consent give rise to processing all (taking into account the common and sensitive data) categories of data to the fullest – as it seems – range of purposes and processing methods. In GDPR, consent is the condition for lawful processing,

Supply of Digital Content, [in:] *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, R. Schulze, D. Staudenmayer, S. Lohsse (ed.), 2017, p. 179.

³ Personal Data Protection Act of 29 August 1997 (Journal of Laws 1997, no. 133, item 883, Journal of Laws 2016.922 j.t.), hereinafter referred to as PDPA.

⁴ The scope of a conflict rule, which is expressed by the maxim *lex specialis derogat legi generali* was modified. Provisions of such acts shall apply only if degree of protection extending beyond that which arising under PDPA; Compare: P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warsaw 2016, pp. 64-65; Compare: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz Lex*, Warsaw 2015, pp. 298-301.

⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50, hereinafter referred to as DPD.

⁶ These are first and foremost: Directive (EU) 2016/680, Directive 2009/136/EC, (EC) No 2006/2004, Directive 2002/58/EC, Directive 2000/31/EC.

⁷ J. Byrski, *Odwolanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia*, „Monitor Prawniczy” 2011, no. 3, pp. 1014-1016; P. Fajgielski, *Odwolanie zgody na przetwarzanie danych osobowych – znaczenie dla praktyki gospodarczej*, [in:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, A. Mednis (ed.), Warsaw 2013, p. 64.

inter alia, for non-sensitive personal data, processing of special categories of personal data, automated individual decision-making, including profiling, for processing personal data after the data subject invoked the right to obtain from the controller restriction of processing, and finally for a transfer or a set of transfers of personal data to a third country or an international organization in the case of absence of an adequate decision pursuant to Article 45 par. 3 GDPR⁸.

Considerations on the consent should be started with defining it. For the purpose of this study the definition from GDPR can be quoted, and differences may be indicated between the definition adopted in that act and the definitions assumed in PDPA. In accordance with provisions of GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Regarding this definition, in contrast to PDPA, GDPR does not establish a prohibition that the consent shall not be presumed or implied from a declaration of intent with different contents. This, in other words means that according to GDPR consent to data processing may be given *per facta conclusio*⁹. However, it should be emphasized that there are other obligations arising from GDPR, that provisions of PDPA, the same as DPA did not provide for, which were discussed below.

LEGAL NATURE OF CONSENT

In the literature regarding the consent, there is a lot of analysis about its legal nature. Most of the doctrines are in favor of the position according to which the PDPA consent must be considered a declaration of will¹⁰. However, there are also different concepts¹¹, above all, those that state that the consent to the processing of data must also be assessed through the prism of a legal action. At this point, it should be analyzed if this dispute makes any sense at all, because especially taking into account the provisions of GDPR, we assume that this discrepancy in doctrine may turn out to be legally irrelevant.

It is said that comments made in regard to this issue on the consent to the violation of personal rights may apply. This statement is so justified that some authors postulate that the consent expressed in Article 7 item 5) of PDPA can be

⁸ Compare: Article 22 par. 2, letter c) GDPR and article 49 1. GDPR.

⁹ See: Article 7 point 5 *in fine* PDPA; P. Fajgielski, *Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych*, „Informacja w Administracji Publicznej” 2016, no. 4, p. 10.

¹⁰ P. Barta, P. Litwiński, *Ustawa o ochronie...*, pp. 137-138; Compare P. Fajgielski, *Zgoda na przetwarzanie danych osobowych*. [in:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, G. Sibigi, X. Konarski (ed.), Warsaw 2007, pp. 42-43; Compare: T. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce*, Wrocław 2013, pp. 90-91; L. Kępa, *Ochrona danych osobowych w praktyce*. Warsaw 2015, pp. 141; M. Ulasiewicz, *Prywatność jednostki w kontekście dostępu do informacji publicznej*, „Przegląd Prawa Publicznego” 2016, no. 11, pp. 45-46; A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warsaw 2008, p. 80; J. Byrski, *Odwolanie zgody...*, „Monitor prawniczy” 2011, no. 3, p. 1013.

¹¹ About the view according to which the consent for the infringement of personal rights should be assessed through the prism of a legal action, which was introduced by E. Zitelmann, and partly shared by German literature, was rejected by M. Sośniak; See: A. Szpunar, *Zgodauprawnionego w zakresieochronydobrosobistych*, „Ruchprawniczy, ekonomicznyisocjologiczny” 1990, LII no. 1, p. 46.

treated as consent for the infringement of personal rights, due to similarity of its legal nature.¹²In this case, a dispute has also arisen, as to whether the consent for the infringement of personal rights is a legal action or a declaration of will¹³.

Searching for the most far-reaching legal consequences resulting from the above described alternative approaches for the consent qualification, the most important criterion, i.e., the issue of legal capacity, should be pointed out. In fact, doubts are raised, right due to the issue of granting the consent by a person who does not have full legal capacity¹⁴. In the case of treating the consent as a declaration of will, according to some authors, the requirements in this area are mitigated, and in that case the person to whom the consent relates is required to hold it to the full extent¹⁵, and therefore for the assessment of the ability and effectiveness of granting the consent as creating a constitutional right to privacy, according to this concept, it is enough – as it seems – that a person understands the meaning of the statement that he/she makes¹⁶. While, if the consent is recognized as a legal action, one should directly refer to the provisions of the Civil Code¹⁷, which as a consequence would mean making the consent granting depend on the age and degree of potential incapacitation. What may lead to the assumption that every consent granting will require the consent of the statutory representative of a minor or guardian of a legally incapacitated person.

From the point of view of the above considerations, not assuming categorically one of the concepts as the most adequate, it can be pointed out that, from the perspective of civil law the consent to the processing of personal data can be seen as – firstly – a declaration of will not being a legal action, or – secondly – as a unilateral or bilateral legal action, where in both cases, the key element of this activity is the consent of the data subject¹⁸. It appears that none of these concepts can be applied in any case. It is rightly pointed out that the nature of relationships between the data controller and the person who grants such a consent is not strictly a civil law relationship, but a public law relationship. Therefore, the application of regulations on legal actions, in particular those relating to the invalidity of a legal action made without the consent of the statutory representative may not be justified¹⁹.

¹² J. Bryski, *Odwolanie zgody na przetwarzanie...*, p. 1013; See also: P. Fajgielski, *Zgoda na przetwarzanie danych osobowych...*, pp. 42-43.

¹³ See more widely: M. Gutowski, *Nieważność czynności prawnej*, Warsaw 2012, p. 12.

¹⁴ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, p. 341.

¹⁵ A. Szpunar, *Zgoda uprawnionego...*, p. 46.

¹⁶ S. Hoc, T. Szewc, *Ochrona danych osobowych i informacji niejawnych*, Warsaw 2014, p. 32.

¹⁷ Civil Code Act of 23 April 1964 (OJ.2017.459 j.t.) hereinafter referred to as PCC.

¹⁸ R. Adamus, *Zgoda na przetwarzanie danych osobowych osoby nieposiadającej pełnej zdolności do czynności prawnych*, "Gazeta Sądowa" 2005, no. 2, p. 23.

¹⁹ T. Szewc, *Zgodanaprzetwarzaniedanychosobowych*, „PaństwoiPrawo” 2008, no 2, pp. 87-88; According to article 17 PCC, Subject to exceptions provided for by the statute, the validity of a juridical act, by which a person limited in his capacity for juridical acts assumes an obligation or disposes of his right shall require the consent of his statutory representative.

The choice of the theoretical legal construction and analysis of the consent for data processing should be started with the considerations on axiological assumptions of the regulations on the protection of personal data, and not necessarily focus on civil law concepts in terms of the consent for the infringement of personal rights, or the crossing of notions of will and legal action. On the other hand, public or constitutional character of the rights to privacy or data protection cannot prevent referring to civil law instruments because similar mechanisms of their application to other rights – including – fundamental rights (e.g. ownership) are known²⁰. In this regard it is worth pointing out the opinion of the European Data Protection Authorities which explain the notion of consent and make recommendations on the revision of the general legal framework for data protection. 'Consent is also a notion used in other fields of law, particularly contract law. In this context, to ensure that a contract is valid, other criteria than those mentioned in the DPD will be taken into account, such as age, undue influence, etc. There is no contradiction, but an overlap, between the scope of civil law and the scope of the DPD: the Directive does not address the general conditions of the validity of consent in a civil law context, but it does not exclude them. This means, for instance, that to assess the validity of a contract in the context of Article 7(b) of the DPD, civil law requirements will have to be taken into account'²¹. In the light of the above comments it should be noted that granting the consent is a factual action whose legal consequences are determined primarily by the regulations on the protection of personal data. Therefore, criteria for the ability to grant it should be established – insofar as this is possible. As a rule, GDPR does not provide clear indications regarding the terms for granting the consent. Therefore, it can justify the attempt to apply strictly civil law construction. However, even the appropriate application of the criteria of performing legal actions by persons who do not have full legal capacity, provided for in Articles 17-20 of the PCC, does not necessarily reflect the assumptions behind data protection regulations, especially in the digital environment.

GRANTING AND FORM OF CONSENT

One of the most major difference is that the written form is not required by GDPR, without regard to sensitive or any other personal data²². Consent could take a form of a written, electronic or oral statement, or any other clear affirmative act. In compliance with recital 32 of GDPR this could include ticking a box when visiting an internet website, choosing technical settings for information

²⁰ T. Szewc, *Zgoda na przetwarzanie danych...*, p. 90.

²¹ According to the Opinion 15/2011 on the definition of consent adopted on 13 July 2011 the data subject's consent has always been a key notion in data protection, but it is not always clear where consent is needed, and what conditions have to be fulfilled for consent to be valid. This may lead to different approaches and divergent views of good practice in different Member States. This may weaken the position of data subjects. This problem has become more serious as the processing of personal data has become an increasingly prominent feature of modern society, both in on-line and off-line environments, often involving different Member States. [access on-line: 02.11.2017]: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

²² P. Fajgielski, *Zgoda na przetwarzanie danych osobowych w...*, p. 9.

society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. It should be indicated regarding to mobile apps, internet services and social networking services in many cases, user (customer) must turn off features related to data processing already at the stage of functioning of the service. On the ground of GDPR provisions, such situation would not be acceptable.

A declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms²³. Moreover, according to article 7 par. 2 of GDPR, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. What is important for digital environment, if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided²⁴.

In view of the foregoing considerations, it can be noted that the current practice of hiding provisions related to the consent would therefore be considered unlawful. In addition, it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. As an example, the phrase in privacy policy: "We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones [...]" might not meet expectations of GDPR. For reasons of transparency, it should be clarified in particular which data may be processed and exactly for what purposes. It seems that too general wording of such terms of privacy policy create a problem related to lack of proper level of awareness of the users. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended²⁵. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. In relation to mobile apps, internet services and social networking services, in addition to the above, it should be remembered that if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided²⁶.

²³ See: recital 42 of GDPR.

²⁴ See: recital 32 of GDPR *in fine*.

²⁵ See: recital 42 of GDPR.

²⁶ See: recital 32 of GDPR.

FREELY GIVEN CONSENT

Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for this performance²⁷. This last requirement would in particular have an impact on providers of mobile apps and social networking services. This is because a large number of providers of this type of service processes users' data for other purposes than the application itself, as discussed above – they benefit from processing. In many cases, without the consent of the user, the user cannot use the service. In this aspect, from the perspective of service providers, an additional doubt will also arise from the wording of the motive 42 according to which for consent to be informed about, the data subject should be aware of at least the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment²⁸. According to the GDPR standards, the user will have the right not to authorize the processing for purposes indirectly related to the supplying of the service. Any attempt to bypass these requirements may raise doubts from the point of view concerning the requirement regarding freely given consent.

ABILITY TO GIVE CONSENT FOR DATA PROCESSING

Looking for criteria for the ability to grant consent for data processing, the following would be undoubtedly worth considering – firstly – the circumstances in which it is granted, secondly, whether the consent is accompanied by a specific obligation, Finally, the age and level of consciousness and discernment of the person concerned should also be taken into account. In the digital environment's aspect, in particular, it refers to cases when the consent is part of a legal activity, (contract) for the provision of information society services²⁹. The problem under what circumstances and under what conditions the consent for personal data processing can be granted will be most important in the case of children. Currently many of them already at a very young age start enjoying the benefits of the digital world. Setting the limit of age after reaching which an individual can freely dispose of his/her privacy is undoubtedly a difficult task. We are provided with some guidance in this regard by recital 38 of GDPR, according to which, children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in

²⁷ See: recital 43 of GDPR.

²⁸ See: recital 42 of GDPR.

²⁹ Polish Supreme Administrative Court took a view on this matter. The court concluded that consent cannot be considered as clear, if the declaration of intention is an additional part of another obligation. See: Judgment of Polish Supreme Administrative Court of 4 April 2003 (II SA 2935/02), LEX no 149895.

particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counseling services offered directly to a child.

The EU legislator overcame this oppression, as it gave the states some freedom in this regard. In case if the consent, in relation to the offer of information society services aimed directly at a child, the processing of the personal data of a child shall be lawful when the child is at least 16 years old. Where the child is below the age of 16, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. However, Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years³⁰. In the Member States the methods of determining the age limit are based on different criteria, starting from setting a specific border, or by reference to criteria adopted by civil law, ending with a subjective approach, leading to a concrete case study a check of the circumstances of the consent³¹. In the Polish doctrine the question raises some doubts³². Checking each time the discernment of the person who granted the consent seems to be impossible in practice. Therefore, it seems that in order to avoid an inconsistent interpretation, the right direction for the laws of the Member States is a specific regulation of the terms for granting the consent, both by minors, as well as persons with a certain degree of incapacitation, taking into account the above mentioned GDPR provisions, considering the close relationship between the right to privacy and data protection with the person who provides the consent³³. It seems that such an operation consisting in creating a certain template in line with the criteria of legal capacity in PCC, would have a positive effect on the certainty of marketing, especially in the digital environment.

However, the postulate described above does not solve the problem of the relation of data protection provisions to the general provisions of contract law of the Member States *de lege ferenda*. Increasingly consent to the processing of personal data is part of the obligation, consisting in the fact that in return for using certain services (these include social networking sites, instant messengers, mobile navigation, and other data processing applications), the data subject is obliged to bear the fact of processing his or her data by the service provider. As a side note, it should be noted that work is also ongoing on the draft of a directive on digital content, where the position was presented according to which the provision of data would be treated as a mutual performance of the person to whom the consent relates³⁴. So,

³⁰ See: Article 8 par. 1 *in fine* GDPR.

³¹ See more: M. Macenaite, E. Kosta, Consent for processing children's personal data in the EU: following in US footsteps?, "Information & Communications Technology Law" 2017, vol. 26, no. 2, pp. 152-156.

³² J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, p. 341; J. Bryski, *Odwolanie zgody na przetwarzanie...*, p. 1014; Compare: Drozd, *Ustawa o ochronie danych osobowych...*, p. 81; P. Barta, P. Litwiński, *Ustawa o ochronie...*, p. 140. T. Szewc, *Zgoda na przetwarzanie danych...*, p. 90; S. Hoc, T. Szewc, *Ochrona danych osobowych i informacji...*, p. 33.

³³ Compare: R. Adamus, *Zgoda na przetwarzanie danych osobowych osoby...*, p. 24.

³⁴ See: Proposal for a Directive of The European Parliament and of the Council on certain aspects concerning

the question arises that, due to the fact that it is possible to assume, in the above cases, a certain commitment appears, then the conditions and the ability to grant the consent have to coincide with the conditions of a lawful and effective obligation, in accordance with civil law regulations. Assuming that the ability to grant the consent on the basis of the GDPR regulations does not match the criteria of the obligations by persons with limited or without any capacity for legal action, in the case of the services described above, there appears a necessity to adopt different criteria granting the consent for personal data processing in relation to the criteria for performing a legal action whose consent is a key element. Thus, assuming that, as a result of granting consent for the processing of personal data, in exchange for the possibility of using information society services, an obligation arises, Civil law of the Member States constitutes a barrier with regard to the mitigated terms of the consent given by the child referred to in Article 8 paragraph 1 of GDPR. In that case the mentioned provision (paragraph 1) would not be applicable due to wording of Article 8 paragraph 3 of GDPR. In this respect, the new regulation (GDPR) will not affect the general contract law of the Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

DEFECT OF INTENTION

A similar situation will be in the case of defects of the will declaration. Analyzing the definition of consent and its related motifs in GDPR, the terms freely granted, informed, allow to assume the assumption that the catalog of defects of will declarations adopted in civil law will apply. However, the consequences of granting the consent and the consequences of the validity of legal actions made under the influence of defects of the declaration of will are shaped differently. The effect of violation of the terms for granting the consent under GDPR will always be the absolute nullity. Meanwhile, in the case of a significant error, deceit or threat only the possibility of evading the legal consequences of such a declaration appears under the PCC³⁵.

In the case of assuming that by granting the consent for data processing a commitment is made, different legal consequences of such an action appear from the perspective of personal data protection law and civil law of the Member States.

WITHDRAWAL OF CONSENT

The ability to cancel the consent was introduced into the Polish act as a result of an amendment made on October 29, 2010³⁶. In European literature, the possibility of canceling the consent was derived by way of interpretation, although the

contracts for the supply of digital content, COM/2015/0634 final - 2015/0287 (COD); F. Zoll, *Personal Data as Remuneration...*, pp. 179-188; A. Metzger, *Data as Counter-Performance...*, pp. 2-8.

³⁵ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, p. 454; M. Giermak, M. Sofronów, *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, „Monitor Prawniczy” 2017, no. 2, pp. 94-95.

³⁶ See: Article 7 point 5 PDPA; See also: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, pp. 344-345.

DPD did not provide *expressis verbis* for such an institution³⁷. According to GDPR the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subjects shall be informed thereof. It shall be as easy to withdraw as to give consent³⁸. This last requirement shall require the digital service providers to adjust the contracts and forms to the new legal status³⁹. Similarly, the administrators will have to create appropriate mechanisms for easy withdrawal of the consent. In many cases, the withdrawal of consent will cause the impossibility to provide the service. But what is very unfavorable for digital service providers, is that in other cases revocation of consent may include only a specific processing purpose, that was most important for the controller, but was not being necessary for the functioning of the service.

As a side note, it should be noted that as was the case with PDPA and GDPR, the ability to cancel the consent under PDPA and GDPR is limited⁴⁰, or even sometimes excluded from other bases of data processing.

BURDENSOME REQUIREMENTS

Internet services providers as the controllers should be able to demonstrate that the users have given consent to the processing operation. The burden of proving that the strictly defined consent for processing data has been given, shall lie with the controller⁴¹. It should be also noted that DPD will be repealed by GDPR. According to recital 171 of GDPR processing already under way on the date of application of GDPR should be brought into conformity within the period of two years after which this GDPR enters into force. Where processing is based on consent pursuant to DPD, it is not necessary for the users to give his or her consent again if the manner in which the consent has been given is in line with the conditions of GDPR, so as to allow the controller to continue such processing after the date of application of this Regulation⁴². It should be indicated that the lack of fulfilling information obligations concerning *inter alia* informing about the possibility of withdrawal of consent may prove to be a problem for controllers. The question that arises is whether the data controllers would be forced to get the consent again or just inform the users of the rights to which they are entitled⁴³.

³⁷ J. Byrski, *Odwolanie z godynaprzetwarzanie...*, pp. 1014-1016; see also: C. Langhanke, M. Schmidt-Kessel, *Consumer data as...*, p. 219; see also: F. Zoll, *Personal Data as Remuneration...*, p. 184.

³⁸ See: Article 7 par. 3 GDPR.

³⁹ P. Fajgielski, *Zgoda na przetwarzanie danych osobowych w...*, p. 11.

⁴⁰ Compare: P. Fajgielski, *Odwolalność zgody na przetwarzanie...*, p. 64.

⁴¹ See: recital 42 of GDPR *in principio*.

⁴² See: Article 171 GDPR.

⁴³ See data policy on social networking service Facebook.com as an example: "You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates." It seems that this kind of clause meets GDPR requirements. But phrase: "Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account.", may raise some doubts., See: <https://www.facebook.com/about/privacy/>.

CONCLUSION

GDPR introduces new rules for lawfully consent for processing data. In many cases, in particular in digital environment, providers of mobile apps and internet services do not meet requirements arising from the new regulation. It should be noted that GDPR will be binding in its entirety and directly applicable in all Member States. Act of May 25, 2018, controllers (on-line service providers) processing European Union citizens' personal data will have to adopt new requirements in connection with the GDPR regulation. It will require introducing changes concerning technical aspects of the functioning of mobile apps, social network services, and other forms of internet services. However, as stated above, GDPR provisions raise a lot of doubts which need to be dispelled by the scholars and EU institutions.

Bibliography

- Adamus R., *Zgoda na przetwarzanie danych osobowych osoby nieposiadającej pełnej zdolności do czynności prawnych*, "Gazeta Sądowa" 2005, No. 2.
- Banyś T., Łuczak J., *Ochrona danych osobowych w praktyce*, Wrocław 2013.
- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz Lex*, Warsaw 2015.
- Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warsaw 2016.
- Byrski J., *Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia*, „Monitor prawniczy” 2011, No. 3.
- Drozd A., *Ustawa o ochronie danych osobowych. Komentarza. Wzory pism i przepisy*, Warsaw 2008.
- Eggers W.D., Hamill R., Ali A., *Data as currency*, “Deloitte Review” 2013, No. 13.
- Fajgielski P., *Odwołalność zgody na przetwarzanie danych osobowych – znaczenie dla praktyki gospodarczej*, [in:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, A. Mednis (ed.), Warsaw 2013.
- Fajgielski P., *Zgoda na przetwarzanie danych osobowych w przepisach ogólnego rozporządzenia o ochronie danych*, „Informacja w Administracji Publicznej” 2016, No. 4.
- Fajgielski P., *Zgoda na przetwarzanie danych osobowych*. [in:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, G. Sibigi, X. Konarski (ed.), Warsaw 2007.
- Giermak M., Sofronów M., *Zgoda na przetwarzanie danych osobowych dzieci w serwisach społecznościowych w kontekście zmian prawa europejskiego*, „Monitor Prawniczy” 2017, No. 2.
- Gutowski M., *Nieważność czynności prawnej*, Warsaw 2012, p. 12.
- Hermstrüwer Y., *Contracting Around Privacy. The (Behavioral) law and economics of consent and Big Data*, “Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2017, No. 8.
- Hoc S., Szewc T., *Ochrona danych osobowych i informacji niejawnych*, Warsaw 2014, p. 32.
- Kępa L., *Ochrona danych osobowych w praktyce*. Warsaw 2015.

- Langhanke C., Schmidt-Kessel M., *Consumer data as consideration*, "Journal of European Consumer and Market Law" 2015, No. 6.
- M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warsaw 2010.
- Macenaite M., Kosta E., Consent for processing children's personal data in the EU: following in US footsteps?, "Information & Communications Technology Law" 2017, vol. 26, No. 2.
- Metzger A., *Data as Counter-Performance: What Rights and Duties do Parties Have?*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2017, No. 8.
- Szewc T., *Zgoda na przetwarzanie danych osobowych*, „Państwo i Prawo” 2008, No. 2.
- Szpunar A., *Zgoda uprawnionego w zakresie ochrony dóbr osobistych*, "Ruch prawniczy, ekonomiczny i socjologiczny" 1990, LII No. 1.
- Ulasiewicz M., *Prywatność jednostki w kontekście dostępu do informacji publicznej*, „Przegląd Prawa Publicznego” 2016, No. 11.
- Zoll F., *Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content*, [in:] *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, R. Schulze, D. Staudenmayer, S. Lohsse (ed.), 2017.

OTHER SOURCES

- Civil Code Act of 23 April 1964 (Journal of Laws 2017.459 j.t.).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (OJ L 281, 23.11.1995, pp. 31–50).
- Judgment of Polish Supreme Administrative Court of 4 April 2003 (II SA 2935/02), LEX No. 149895.
- Opinion 15/2011 on the definition of consent of Article 29 Data Protection Working Party Adopted on 13 July 2011, 01197/11/EN, WP187.
- Personal Data Protection Act of 29 August 1997 (Journal of Laws 1997 No. 133 item 883, Journal of Laws 2016.922 j.t.).
- Proposal for a Directive of The European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, (COM/2015/0634 final - 2015/0287).

Summary: In recent years, due to the development of new technologies, we are dealing with an increased threat to the privacy of individuals, especially considering their on-line activity. The new General Data Protection Regulation ensures a high level of security of personal data and privacy protection. The paper focuses on issues regarding consent to the processing of personal data from the point of view of users and Internet service providers. The publication presents the differences between the Polish Personal Data Protection Act, the Directive 95/46/EC and the new Regulation, as well as analyzes the requirements for giving consent to the processing of personal data in a digitized environment.

Keywords: personal data, civil law, consent, General Data Protection Regulation

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH W ŚRODOWISKU CYFROWYM W ŚWIETLE PRZEPISÓW OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH

Streszczenie: W ostatnich latach w związku z rozwojem nowych technologii, mamy do czynienia z wzrostem zagrożenia prywatności osób fizycznych, szczególnie biorąc pod uwagę ich aktywność on-line. Nowe Ogólne Rozporządzenie o Ochronie Danych zapewnia wysoki poziom bezpieczeństwa danych osobowych i ochrony prywatności. Artykuł koncentruje się wokół zagadnień dotyczących zgody na przetwarzanie danych osobowych z perspektywy użytkowników i dostawców usług internetowych. W publikacji zaprezentowano różnice między polską ustawą o ochronie danych osobowych, dyrektywą oraz nowym Rozporządzeniem oraz przeanalizowano wymogi dotyczące udzielenia zgody na przetwarzanie danych osobowych w środowisku zdigitalizowanym.

Słowa kluczowe: Dane osobowe, prawo cywilne, zgoda, ogólne rozporządzenie o ochronie danych.