JUSTYNA TYBURSKA[1]

CRITERION OF LEGITIMACY OF CONSENT FOR PROCESSING PERSONAL DATA IN E-COMMERCE[2]

1. INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC[3] (hereinafter: DPREC) is the basic legal act for the protection of personal data in European legislation. The principles of personal data protection have been legislated on considering the scale personal data being collected and exchanged. The above results from technological progress and globalization, coupled with increase in fraud or offences related to unauthorized use of personal data. The legislation of personal data protection rules was aimed at preventing infringements of the free movement of personal data in the European Union (hereinafter: EU), having regard to the rights of individuals to the protection of their personal data[4]. For the sake of legislative coherence in personal data protection across the EU, the regulation has been chosen.

The paper examines and assesses the latest European legislation and solutions concerning personal data protection, including the rights and obligations of data subjects and data processors, in terms of intensification of inspection over the flow of personal data of various types.

2. LEGAL DEFINITIONS

Under Article 4(1) of the GDPR, personal data shall mean information about an identified or identifiable natural person. Personal data are divided into: ordinary personal data,

[1] Instytut Nauk Prawnych Polskiej Akademii Nauk.

[2] Artykuł przetłumaczony ze środków finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego na działalność upowszechniającą naukę (DUN), nr decyzji 810/P-DUN/2018. Article translated from funds financed by the Ministry of Science and Higher Education for the dissemination of science (DUN), Decision No. 810 / P-DUN / 2018.

[3] 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) (OJ L 119, 4.5.2016, p. 1).

[4] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, ed. M. KAWECKI, T. OSIEJA, Warszawa 2017, p. 12.

such as: name and surname, address of residence, Internet identifiers, telephone number, sex, eye colour, weight, height and specific (otherwise sensitive) personal data, which include, inter alia, data on sexual orientation, biometric data and genetic data, data revealing racial or ethnic origin or data from the register of convicted persons[5].

As defined in Article 4(2) of the GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Personal data processing is construed as any action on a personal data file, regardless of whether via a traditional technique or using information systems, and includes all possible forms of operation with regard to personal data[6].

In this regard, it is noteworthy that even consent may not legitimise an inadequate or excessive processing of data vis-à-vis the purpose of data collection.

3. CONSENT TO THE PROCESSING OF PERSONAL DATA IN TRADITIONAL TRANSACTIONS

Under Article 4(11) of the 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. The consent given by a clear affirmative action may be applied solely to ordinary personal data, because for sensitive personal data to be processed explicit consent is vital, that is expressed through a written declaration of will[7].

Freely given means that the data subject must be able to choose between consent or lack thereof, without affecting its relationship with the controller in areas not covered by consent[8]. Freely given consent shall be freely given on one's own initiative by a person in full mental health and without any coercion of a social, financial, psychological or other nature[9]. Respectively, a consent should not be considered freely given if the data subject has no real or free choice and cannot refuse or withdraw consent without adverse consequences.

Under Recital (43) of the GDPR, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority. Wherever the controller is an administrative authority, freely given consent would be illusory.

[5] *RODO. Ogólne rozporządzenie o ochronie danych*, ed. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2018, p. 171.
[6] GIODO, *Gotowi na RODO*, https://uodo.gov.pl/data/filemanager_pl/641.pdf (access: 22 June 2019, 20:48.).
[7] A. SAGAN-JEŻOWSKA, *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018, p. 24.
[8] Ibid..
[9] *RODO. Ogólne rozporządzenie…, op. cit., p.* 247.

The above premise of voluntariness is assessed against four criteria, that is the criterion of balance between the parties, necessary consent for the performance of the contract, characteristic performance and a reasonable alternative. The latter does not stem directly from the legislation. Quoting after E. Bielak-Jamaa and D. Lubasz, the provision of services by the controller should not be dependent on the consent to the processing of personal data, if the data subject will not be able to receive an equivalent performance at all or on reasonable terms in case of disagreement[10].

Importantly, consent is not considered freely given if it cannot be given separately for different personal data processing operations. While not necessary for contract performance, the consent determines it, including the provision of services. By way of illustration, where participation in a project depends on the consent to the processing of data for marketing purposes, the consent given in such a case will not meet the voluntariness requirement. Only splitting the purposes of data processing consent into: for contract performance and for marketing purposes will make data processing consent for marketing purposes freely given, unless the absence of consent does not prevent participation in the project.

Another premise of the criterion of lawfulness of consent for data processing, specificity, means that it must refer to the specific situation of processing personal data for the purposes and scope of processing. A specific consent should also be clearly defined, precise and objective and must refer to the purpose for which personal data will be processed. 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. The specific consent must explicate the purposes of the processing. A single consent may cover several processing operations, provided that they all serve the same purpose. 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 provided.

The unambiguity feature implies that the statement must indicate precisely that the data subject has given his or her consent, and therefore consent may not be implicit. Unambiguity as a characteristic of consent implies that there is no doubt about the data subject's intention to consent[11]. It should be pointed out here that consent according to the GDPR is based on an *opt-in* system, which requires a specific activity of the data subject and an unambiguous demonstration of will. Accordingly, any *opt-out* model is unacceptable as being based on inactivity, silence, carelessness or inertia, that is by means of a *checkbox* when using websites,

[10] Ibid., p. 4267.
[11] *RODO. Ogólne rozporządzenie…, op. cit., p.* 255.

or by acceptance of the terms and conditions of the service which determine the question of consent beyond the scope of service provision[12]. It is also appropriate to make another statement, expressed in recital (32) of the GDPR, which clearly indicates that the data subject has accepted the proposed processing of his or her personal data.

A fourth category remains to be discussed, namely awareness, which means that the data subject must be aware of what he or she agrees to and, furthermore, should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Freely given means that the data subject must be able to choose between giving his or her consent and not doing so without affecting his or her relationship with the controller in areas not covered by consent[13].

4. LAWFULNESS OF DATA PROCESSING

Under Article 6 of the GDPR, the processing of data is lawful provided that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[12] Ibid., p. 352.
[13] Ibid..

Consent may be given subject to a condition and may be valid after this condition has been fulfilled, and may also be a consent of limited duration in view of the determination of the term of validity of the consent, upon the expiry of which it will cease to be valid. The consent may also be territorially limited, that is apply to processing within the territory of a relevant State. The consent may also be granted with a subjective indication, that is with the proviso that processing may be carried out only by a designated person. According to J. Bart and P. Fajgielski, consent to data processing may also be a partial consent, that is it may apply not to all operations falling within the scope of the concept of personal data processing[14].

Consent to the processing of data is a legal act in accordance with Article 17 of the Civil Code[15] (hereinafter referred to as the Civil Code). In principle, consent is considered to be an activity similar to a declaration of intent, though the GDPR provides no guidelines in this respect[16]. However, this is of considerable practical significance, given that the plenipotentiary may make the declaration of will or the provisions on defects in the declaration of will may apply to consent. In this context, a person who initially consented to the processing of personal data and subsequently in mistake may evade the legal effects of the declaration of will by making a written declaration, as a result of which the previously given consent will be invalid from the outset. This has consequences for the controller as a result of the unlawful processing of personal data. The provision of Article 60 in conjunction with Article 84 § 1 of the Civil Code on defects of the declaration of will may underpin the evasion by the data subject of the legal consequences of consent to the processing of data, given by the data subject in a material mistake, tracked down to the provision of insufficient or untrue information by the data controller about the purpose of their collection, or about the recipients of the data. The ineffectiveness of evading the legal consequences of a data subject's consent to the processing of data given by the data subject in mistake is contingent on correct compliance with the obligation to provide information to the data subject. Consequently, consent will be invalid if the data subject is in a state excluding the free or informed expression of his will. Likewise, consent given in a material mistake, deception or an unlawful threat will be invalid[17].

[14] J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, p. 452-453.
[15] Act of 23 April 1964. - Civil Code (Dz.U.-Journal of Laws Issue 16, item 93 as amended).
[16] B. KACZMAREK-TEMPLIN, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia*, [in:] *Polska i europejska reforma ochrony danych osobowych*, ed. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2016, in. 104-105.
[17] Ibid., p. 454.

4.2. MEANS AND FORMS OF GIVING CONSENT TO DATA PROCESSING

Consent may be given in different forms. In practice, a written declaration in traditional trade or electronic form is most often observed. This may include ticking a check box when browsing the website, selecting technical settings for the use of the services (by way of illustration *online*), or it may take the form of an oral statement. Any other form of statement or behaviour is allowed which in the context clearly indicates that the data subject has accepted the proposed processing of his or her personal data. Where consent is given by e-mail, text message or instant messenger, it will be effective as long as the declarant's identity may be established. Hence, consent will solely be given if a clear affirmative action unambiguously demonstrates that the data subject consents to the processing of his or her data for a specific purpose, and such clear affirmative action is effected if, for instance, he or she gives a business card, fills in a contact form for a known purpose, or sends personal data to a specific controller for a specific purpose[18].

The provisions allow for consent to be expressed orally, yet in practice such consent must be recorded, and such evidence of consent would in principle be the recording of the interview, so other forms of consent prevail. At the same time, consent to the processing of data makes it necessary to comply with the information obligations stemming from Article 14(2) of the GDPR, while according to Article 12(1) of the GDPR, information on the rights of the data subject may be given orally if the data subject so requests, and the identity of the data subject can be established otherwise. Further, the controller shall be responsible for proving that data processing consent is in place.

As clear from the Preamble to the GDPR, where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 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, the important things being clear and plain language, both in written and oral form. In most cases, the statement of consent to the processing of data is developed by the controller and should not contain unfair terms. With a view to verifying these conditions the consent clause must be separate from the content of the contract.

[18] Ibid., p. 25.

As a rule, each natural person on its own gives consent for data processing producing legal effects. However, GDPR particularly protects children with regard to consent to information society services, that is services available and rendered online. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Only children over the age of 16 can give their own consent to the processing of data for information society services. Nonetheless, under the GDPR, no consent is required for preventive or counselling services offered directly to a child[19]. Relying on the available technology, the controller should pursue reasonable endeavours with a view to verifying whether the person exercising parental responsibility or custody has consented or approved the consent. The means of verification are not specified, but could be verification by means of penny transfers or by telephone to verify data. Doubts may be raised about verification by requesting confirmation of consent via e-mail.

GDPR does not provide for the conditions of consent to the processing of personal data given by minors for processing other than civil society services. Therefore, to the effectiveness of the consent of a natural person, the provisions of civil law on legal capacity to perform legal acts apply, since consent to the processing of personal data is a declaration of will. Under Article 12 of the Civil Code, a person under the age of 13 cannot make an effective declaration of will, and therefore the processing of his/her personal data requires the consent of the guardian given prior to the submission of the declaration by the minor. The situation is similar in the case of incapacitated persons[20]. Minors between 13 and 18, with limited legal capacity, may make effective declarations of will. Pursuant to Article 18 of the Civil Code, in some cases – such as confirmation of the validity of a contract concluded by a person with limited capacity - statutory representative must confirm the declaration.

4.4. WITHDRAWAL OF THE CONSENT FOR DATA PROCESSING

The consent shall in principle remain valid until withdrawn by the data subject. In other words, earlier consents - obtained under the previous regulations of the Act of 29 August 1997 on personal data protection, repealed on 25 May 2018, are valid, and as a result data may be processed based thereon. Nevertheless, the so-called *reconsenting* is recommended, that is

[19] A. SAGAN-JEŻOWSKA, *op. cit*., p. 34-35.
[20] J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ, *op. cit*., p. 452.

consents must be reiterated at times ensure the awareness of data subjects, even if the circumstances of this processing have not been significantly modified[21].

The data subject has the right to withdraw his or her consent at any time, whereas it shall be as easy to withdraw as to give consent. On the other hand, when withdrawing consent, no declaration of intent is required in the same form as consent, so that the form of withdrawal may be different as long as it originates from the data subject. It would be invalid to establish that registered letter is essential for revocation to be effective, as it imposes excessive obligations on the data subject. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. Furthermore, controllers should sensitise natural persons to the risks, principles, safeguards and rights involved in personal data processing and means of exercising their rights as regards processing, and are legally required to advise the natural person that they may withdraw their consent as part of the information obligations accompanying the collection of personal data. Withdrawal of consent has an *ex nunc* effect: it has effects upon submission. Consequently, the person withdrawing consent may not in any way challenge the lawfulness of the data processing during validity of consent.

Obviously, the data subject may only give his or her consent before the controller commences processing. Any consent must precede any new purpose of the processing, no follow-up form being allowed[22].

Consent to the processing of personal data issued under the effective earlier provisions of the Personal Data Protection Act repealed on 25 May 2018 does not expire. If issued in compliance with the GDPR requirements, that is to say, if the original expression of consent corresponds to the terms of the GDPR. When the GDPR comes into effect, each controller has had to assess whether the consents obtained by him or her met the criteria described in Article 4(11) (freely-given, specificity, awareness and unambiguity), Article 6(1)(a) in conjunction with Article 7 and Article 9(2)(a) of the GDPR.

5. CONSENT TO THE PROCESSING OF DATA IN EUROPEAN TRANSACTIONS

On 25 May 2018, the Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic

[21] A. SAGAN-JEŻOWSKA, *op. cit*., p. 32-33.
[22] *RODO. Ogólne rozporządzenie…, op. cit., p.* 356.

Communications)[23] (hereinafter: the ePrivacy Regulation) was to have entered into force. The provisions of this Directive complement 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[24] and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector[25].

Meanwhile, the level of security is assessed in the light of Article 17 of Directive 95/46/EC and its provisions complement and specify the GDPR with regard to the electronic communications data that qualify as personal data. The ePrivacy Regulation is intended to supersede Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[26], still, given the ongoing negotiations, the final wording of the regulation as of the date of drafting of this text was not known.

The ePrivacy Regulation has been designed to strengthen the protection of end-users of terminal equipment against undue intrusion into their privacy. It ensures the protection of personal data in the electronic communications sector. Whereas the recent years have brought material technological and economic changes to the market, the new rules are supposed to bring the rules into conformity with technological progress and current market realities and to boost confidence in digital services. It is important that the ePrivacy Regulation ensures online protection not only for private individuals but also for legal persons.

The ePrivacy Regulation commits providers of electronic communications services to be issued with end-users' consent to the processing of electronic communications metadata, which should include device location data generated to provide, maintain access to, and connect

[23] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final – 2017/03 (COD).

[24] 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, p. 31).

[25] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998).

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37) amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337, 18.12.2009, p. 11).

to, a service. End-users may consent to the processing of their metadata to access specific services, such as anti-fraud services, by examining their usage, location and account data in real time. Electronic communications metadata include: data processed in an electronic communications network to transmit, distribute or exchange electronic communications content; including those used to trace and identify the source and destination of a communication event; device location data generated in the provision of electronic communications services; and the date, time, duration and type of communication. Metadata thus provide sensitive information such as user location, browser history, time of communication or time of message transmission.

Under Article 6 of the ePrivacy Regulation, providers of electronic communications services may process electronic communications data to render a specific service to an end-user provided that the latter has consented to the processing of their electronic communications content and the service cannot be provided without the processing of that content or that all end-users concerned have consented to the processing of their electronic communications content for one or more purposes which cannot be achieved by the processing of anonymised information and the provider has consulted a supervisory authority.

For the purposes of the ePrivacy Regulation, the consent of the end-user, whether a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent. The ePrivacy Regulation highlights that consent can be given through the use of appropriate technical settings of Internet access software. Moreover, access to information about a photo on the phone or contacts will have to be preceded by the device user’s consent.

Under the ePrivacy Regulation, consent to the processing of data should meet the conditions set out in the GDPR, that is it must be freely given, unambiguous and informed. At the same time, consent to the processing of data related to the use of the Internet or voice communication will not be valid if the data subject has no genuine and free choice or cannot refuse or withdraw consent without detriment. Moreover, end-users may withdraw their consent at any time and electronic service providers should remind users of this option every six months throughout the processing period.

What is more, in electronic transactions, the ePrivacy Regulation provides for changes to *cookies* which remember preferences and personalise websites with regard to the content displayed. Indeed, natural persons using online services by means of cookie identifiers can be easily identified by the so-called 'electronic footprints' which, in combination with unique identifiers and other information obtained by servers, can be further used to profile and identify

individuals[27]. Browsers should be equipped with additional settings to obtain unambiguous consent to the use of *cookies* for the specific purpose of processing personal data. Solely for *cookies* that do challenge the end user's privacy no consent will be necessary. *Cookies* which are intended to facilitate the use of the website by the user, such as remembering the contents of the shopping cart, and those which count the number of visits by the users to a relevant website, will be exempt from obtaining the user's consent[28].

Under Article 5(3) of the ePrivacy Regulation, storing information or gaining access to information already stored in the user's device is allowed only if the user has consented to it; after receiving clear and complete information, inter alia, about the purposes of the processing. Further, the user may give his or her consent in any way that enables him or her free and informed expression of the user's wishes, in particular by ticking a checkbox when browsing the website. In concert with the ePrivacy Regulation, no consent is required for every operation to access or store information on a user device, as information and the right to refuse may be offered on a one-off basis for different types of tools installed on a user device during the same communication, and may also include any further use of these tools during subsequent communication[29]. However, consent may not be derived from the use of a service, since it must be explicit and not implicit or expressed *per facta concludentia*.

6. CONSENT TO DATA PROCESSING IN *CLOUD COMPUTING*

Cloud computing is a model of service provision for access on demand, through a network, to a shared pool of information technology resources (hereinafter: IT), and for accessing scalable and flexible IT services[30]. These resources may be ordered by customers and configured as appropriate, depending on the users' needs, delivered on demand and made available with minimal involvement of the service recipient. In other words, *cloud computing* includes data and software transfer to external servers, making them available to the user, whereas changes may be made and saved from any computer connected to the Internet. The above is a data collocation that may be of a different nature. In order to be available, the personal

[27] M. OLSZEWSKA, *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkownika Internetu*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny, 7(6)/2017, p. 42.
[28] Ibid., p. 46.
[29] Ibid., p. 50.
[30] E. DYBKA, D. FALKOWSKI, R. GAJDA i in., *Cloud computing w sektorze finansowym. Raport Forum Technologii Bankowych przy Związku Banków Polskich* p. 6, https://zbp.pl/getmedia/c6fc00fd-6f7e-4cd0-9965-e6f4d143377d/Raport_Cloud_computing_w_sektorze_finansowym_2013-_z_recenzjami (access: 24 June 2019, 22:36.

data is cloned between different locations but nearly always within a cluster or matrix. This also applies to backups with the service provider, which can keep copies of customer data in another server room, etc. A distinction is made between private clouds available to one organization, public clouds available online to different users, and hybrid clouds being a combination both, where some work in an organization's environment and some in a public environment. Data may be collected in any cloud, and businessmen massively use the space available to them in the cloud to store human resources records containing personal data of employees and candidates for work. Nevertheless, a cloud user does not purchase a specific carrier on which to store data, or a copy of computer software – is solely accedes distributed resources for use. From the perspective of personal data protection, in principle, cloud computing constitutes entrusting personal data processing to another entity or a network of entities. On the other hand, the cloud provider must ensure a cloud user, responsible for personal data processed in a cloud, with the processing under compliant with the rules binding on the cloud user. Personal data processing in a cloud will be lawful provided that the relevant provisions on the personal data protection are complied with, in the absence of separate legislation directly related to c*loud computing*. Accordingly, in order to carry out data processing in a cloud, an appropriate *cloud computing* service agreement must be concluded, for control of personal data bases and prohibiting illegal data transfer, being an agreement for entrusting personal data processing to a *cloud computing* service provider. Furthermore, the data subject must consent to the processing of personal data in this way, failing which, neither the cloud provider nor the service recipient can perform any operations related to personal data processing.

7. CONSENT TO DATA PROCESSING VERSUS VIEWS OF JURISPRUDENCE

The issue of consent to personal data processing is also reflected in the case law. In the light of the Polish jurisprudence, under the previous provisions of the Act of 29 August 1997 on the protection of personal data it was assumed that consent cannot be presumed, implicit or abstract, but the person expressing it must be aware of its essence, purpose and effects[31]. Moreover, consent to data processing must be explicit, whereas its placement as an additional element of another obligation not containing information about the purposes and scope of data processing misses this requirement[32]. The Supreme Administrative Court, in its judgment of 6 September 2011, I OSK 1476/10, OSP 2013/10/104, also emphasises the total freedom to grant

[31] Supreme Administrative Court judgment of 10 January 2013, I OSK 2029/11.
[32] Supreme Administrative Court judgment of 4 April 2003, II SA 2135/02, Wokanda 2004/6/30.

consent, which may be refused with no detriment [33]. On the other hand, the written consent of the employee to his or her personal data being collected and processed, expressed at the employer's request, in this respect violates the employee's rights and freedom of expression of will[34]. As assumed by Polish jurisprudence, consent may be given only in the form of a statement, and not by a clear affirmative action, as is the case in other European countries.

In Germany, the effectiveness of consent was at issue before a court in an action brought by the Federation of German Consumer Organisations *(Verbraucherzentrale Bundesverband)* against Facebook, which gained media interest. The complainant argued that the default privacy settings provided by the website fail to make users fully aware of the sharing of their data, and hence their consent is not fully informed.

At the same time, since the subject's consent to the processing of data must be informed, service providers must provide him or her with clear and intelligible information about the nature and extent of the purpose of the processing**.**

It is questionable whether the statement of consent must be limited to one purpose of the processing, views on this matter being divergent. The German legal academics and commentators takes the view that the statement of consent does not need to be limited to one purpose of processing, as follows from the wording of Article 6(1)(a) of the GDPR, consent covers the processing of personal data for one or more specified purposes. It has been assumed so far that a separate consent must be taken for each of the separate purposes of the processing, this fulfilling the condition of consent being specific[35]. Looking ahead, the Court of Justice of the European Union (CJEU) will probably rule on this issue with a view to ensuring the correct interpretation of the provision.

However, as follows from the CJEU case law, private life must be respected in the context of personal data processing, which is a fundamental right of every individual and pertains to all information on an identified or identifiable natural person[36]. Personal data include such information as a name, given name, date and place of birth, nationality, marital status, sex, record of entries into and exits from the country, residence status, particulars of passports issued to a person, record of one's previous statements as to domicile, reference numbers issued by

[33] Supreme Administrative Court judgment of 6 September 2011, I OSK 1476/10, OSP 2013/10/104.
[34] Supreme Administrative Court judgment of 6 September 2011, I OSK 1476/10, LEX nr 965912,
[35] *RODO. Ogólne rozporządzenie…, op. cit., p.* 355.
[36] Wyrok TSUE z 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 V. i M. Schecke, H. Eifert przeciwko Land Hessen, Zb. Orz. 2010, p. I-11063, pkt 52.

offices and authorities which supplied the data[37], and data on earned and unearned income or income from property of natural persons[38]. The CJEU also considered it to be processing to collect data as per official documents, to publish them in a comprehensive list or to make them available for commercial use.

The CJEU held that an exhaustive and restrictive list of cases sets out in which the processing of personal data can be regarded as being lawful and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending those grounds[39]. Furthermore, the right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society [40]. The latter thesis allows certain types of *cookies* to be exempted from the obligation of informed consent of the Internet user, as otherwise users would have difficulty in accessing many online services or could not use them at all, the mandatory consent being required.

8. CONCLUSION

The protection of personal data derives from the right to privacy, which is a fundamental right of every human being. More recently, the scope of the processing of personal data, the nature of the data collected and the way they are processed have showed a rapid change as a result of technological progress and globalisation. New technologies make it possible to process personal data on an unprecedented scale. Individuals make personal data available to a much greater extent publicly and globally, often not being fully aware of their consent.

The new legal acts, that is the GDPR and ePrivacy regulations, seek to provide individuals with the control over their personal data. The GDPR takes a more restrictive approach to consent. Amidst the new legislation, consent to the processing of personal data as a criterion for the legalization of data processing has been redefined. Consent to the processing of personal data must be freely-given, specific, informed and unambiguous, must be made in the form of a statement or a clear affirmative action, which agrees to the processing of personal data relating to him or her,, and must sometimes be clear. The effectiveness of consent shall be excluded in a situation of serious inequality between the data subject and the controller.

[37] Wyrok TSUE z 16 grudnia 2008 r. w sprawie C-524/06 H. Huber przeciwko Bundesrepublik Deutschland, Zb. Orz. 2008, p. I-09705
[38] Wyrok TSUE z 16 grudnia 2008 r. w sprawie C-73/07 Tietosuojavaltuutettu przeciwko Satakun-nan Markkinapörssi Oy i Satamedia Oy, Zb. Orz. 2008, p. I-09831.
[39] Judgment of the Court of 19 October 2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, CURIA.
[40] Wyrok TS UE z 9.11.2010 w sprawach C-92/09 i 93/09, *op. cit.*

It should be noted that the GDPR assumes a different nature of consent as a prerequisite for the legalisation of the processing of ordinary personal data and personal data of special categories. For special categories of data, the standard of consent has been raised by the obligatory explicit consent to the processing of specific data. As a result, clear affirmative action will not suffice in such a case, but a clear statement with the consent will be necessary[41]. Data controllers must obtain and keep records of consent in an appropriate manner so that, in case of a data subject's complaint, they can demonstrate that the data subject has actually consented to the processing of his or her personal data. Should the controller fail to demonstrate that he or she has obtained consent to the processing of data in a lawful manner, including through effective consent, he or she runs the risk of administrative sanctions and sometimes also will be held liable towards the injured person whose data have been unlawfully processed. Moreover, consent to data processing links to certain rights of data subjects, such as the right to erase data or data portability. At the same time, it is of essence for the data controller to properly construct a clause giving consent to the processing of data. The clause should clearly specify for what purpose, scope and by whom personal data will be processed, and these purposes must be properly defined. For a declaration of will regarding the different purposes of the processing, such consent should be given explicitly for each of these purposes of the processing. Furthermore, the clause must be properly distinguished from the rest of the contract or document.

The EU legislator highlights it that the subject may withdraw his or her consent at any time, whereas it shall be as easy to withdraw as to give consent. In this case, unless there is another ground for processing, such us performance of the contract or a specific legal ground, the controller must stop the processing. As a consequence of the withdrawal of consent, in the absence of a ground for processing the data, should be erased from all controller systems.

BIBLIOGRAPHY

BARTA J,, FAJGIELSKI P., MARKIEWICZ R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.

DYBKA E., FALKOWSKI D., GAJDA R. i in., *Cloud computing w sektorze finansowym. Raport Forum Technologii Bankowych przy Związku Banków Polskich*, https://zbp.pl/getmedia/c6fc00fd-6f7e-4cd0-

[41] *RODO. Ogólne rozporządzenie…, op. cit., p.* 242.

9965e6f4d143377d/Raport_Cloud_computing_w_sektorze_finansowym_2013-_z_recenzjami (access: 24 June 2019, 22:36.

GIODO, *Gotowi na RODO*, https://uodo.gov.pl/data/filemanager_pl/641.pdf (access: 22 June 2019, 20:48.).

KACZMAREK-TEMPLIN B., *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia*, [in:] *Polska i europejska reforma ochrony danych osobowych*, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2016.

Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, ed. M. KAWECKI, T. OSIEJA, Warszawa 2017.

OLSZEWSKA M., *Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkownika Internetu*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny, 7(6)/2017.

RODO. Ogólne rozporządzenie o ochronie danych, red. E. BIELAK-JOMAA, D. LUBASZ, Warszawa 2018.

SAGAN-JEŻOWSKA A., *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018.