http://dx.doi.org/10.12775/CLR.2017.005

Natalia Daśko*

THE GENERAL DATA PROTECTION REGULATION (GDPR)– A REVOLUTION COMING TO EUROPEAN DATA PROTECTION LAWS IN 2018. WHAT'S NEW FOR ORDINARY CITIZENS?

Abstract

This Article concerns the EU data protection reform which will come into effect from 25th of May 2018 and will be directly applicable in all Member States. The EU data protection reform aims to build a modern and comprehensive data protection framework for the European Union. The GDPR makes a number of changes in data protection laws, e.g. it introduces new obligations for data controllers and processors, brings new status and new tasks for Data Protection Officers (DPOs), gives more rights to data subjects and most importantly completely changes the perception of data protection law by introducing rules such as privacy by design, privacy by default. The Author describes selected changes, in general, from the viewpoint of an ordinary citizen.

Keywords

General Data Protection Regulation – data protection – processing – information society – privacy by design – privacy by default

* Natalia Daśko, Juris doctor (PhD), Assistant at the Cybercrime Research Centre, Faculty of Law and Administration, Nicolaus Copernicus University in Toruń, Poland; Advocate. E-mail: ndasko@umk.pl.

Introduction

The continuing development of new information and communication technologies is significantly changing our world and our life and creating a requirement for new legal solutions. In recent years we have witnessed the rapid development of the Internet and electronic commerce, the emergence and growth of social networks, cloud computing, mobile applications, geolocation etc. Development has given rise to a plethora of legal problems, particularly in data protection law.

Work on the Data Protection Directive 95/46/EC[2], the EU's most important piece of legislation in this area, started in the nineties of the last century, when the Internet did not exist in today's sense, there were no web search, and no smartphones. The use of the Internet was unthinkable! Today 76% of Poles have access to the Internet (the EU average is 83%)[3] and we use 58,84 million Smartphones[4]!

In this regard it was obvious that a change in data protection law had to come. The initial work on the new law was started in 2009. A new regulation was proposed in 2012 and after 4 years of preparation and debate in May 2016, the Official Journal of the European Union published the General Data Protection Regulation (GDPR)[5] which replaces the Data Protection Directive 95/46/EC/. The GDPR will come into effect from 25th of May 2018 and will be directly applicable in all Member States.

---

[1] 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. 31–50.

[3] Dostęp do Internetu w Polsce ma 76 proc. gospodarstw (In Poland 76 per cent of households have access to the Internet), https://finanse.wp.pl/dostep-do-internetu-w-polsce-ma-76-proc-gospodarstw-6114264429312129a/ [last accessed 20.72017].

[4] Ponad połowa Polaków korzysta z internetu, a smartfonów jest więcej niż obywateli (In Poland, more than half of the population uses the Internet; there are more smartphones than citizens), http://businessinsider.com.pl/media/internet/ilu-polakow-korzysta-z-internetu-raport-deloitte/f0wn6q4/ [last accessed 20.7.2017].

[5] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

The GDPR makes a number of changes in data protection laws, e.g. it introduces the new obligations for data controllers and processors, brings new status and new tasks for Data Protection Officers, gives more rights to data subjects, and, most importantly, completely changes the perception of data protection law by introducing rules such as *privacy by design*, *privacy by default,* or *privacy risk assessment* and *privacy impact assessment*. These rules constitute a totally new approach to data protection and therefore present a great challenge to data controllers or processors, whether they are operating in the private or public sectors.

I. Broader territorial scope of Regulation

The application of Directive 95/46 is based on territorial links. Crucial in this context is Article 4 which constitutes three conditions for the application of the national legislation transposing Directive 95/46. According to Article 4(1)(a) of Directive 95/46, each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the data controller on the territory of the Member State. If this first condition is met, it is unnecessary to examine the other two conditions. Where that condition is not met because the data controller is not established on Community territory, it is necessary to examine whether he, for the purposes of the processing of personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community[6]. The rather narrow territorial scope of the Directive 95/46 causes problems in today's world. From a technical point of view, the processing of personal data is becoming easier and easier. It does

---

[6] M. Czerniawski, *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (Territorial scope of application of Polish and EU data protection regulations in the context of the latest case law of the Court of Justice of the European Union*), [in:] E. Bielak-Jomaa, D. Lubasz (eds.), *Polska i europejska reforma ochrony danych osobowych (The Polish and the EU data protection reform)*, Wolters Kluwer, Warszawa 2016, p. 90.

not require any advanced knowledge or rare equipment and software. The physical location of the data controller and processor becomes less important. Personal data is available for use at any given moment, in any part of the world, moreover the physical locations of the processor may vary due to mobile devices. Two important judgments given by The Court of Justice are keeping pace with the times, pointing to the need to further extend the territorial scope of Directive 95/46[7].

The extension of the territorial scope of Directive 95/46 is regarded as a prerequisite for the proper protection of personal data in the current situation of constant technological progress. In the case C-131/12, *Google Spain*[8], The Court of Justice recognized the problem that national supervisory authorities have with jurisdiction over a data controller's operating in cyberspace. A strict interpretation of Article 4 of Directive 95/46 compromises the Directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the Directive seeks to ensure.

A Spanish national resident in Spain, Mr Costeja González lodged with the national supervisory authority a complaint against the publisher of a daily newspaper with a wide area of distribution and a high circulation, and against Google Spain and Google Inc. The complaint was based on the fact that by putting Mr Coasteja González's name into a search engine of the Google group ('Google Search'), one would obtain links to two pages of a Spanish newspaper which had published Mr Coasteja González's personal data. By that complaint, Mr Costeja González requested that the publisher be required to remove or alter the article with the personal data relating to him and that Google Spain or Google Inc. be required to remove or conceal those data so that they ceased to be included in the search results and no longer appeared in the

---

[7] M. Czerniawski, *Zakres terytorialny a pojęcie „jednostki organizacyjnej" w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu (Territorial scope vs the notion of „establishment" in the provisions of the General Data Protection Regulation – outline*), [in:] G. Sibiga (ed.) *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016 (General Data Protection Regulation. The current problems regarding the legal standards for the protection of personal data)*, C.H. Beck, Warszawa, p. 22-23.

[8] Judgment of The Court (Grand Chamber) of 13 May 2014 in Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317.

links to the newspaper. Agencia Española de Protección de Datos (AEPD) upheld the complaint against Google Spain and Google Inc. In reply to this Google Spain and Google Inc. brought actions against that decision before the Audiencia Nacional (National High Court) to confirm that AEPD has no jurisdiction over a private company incorporated under the laws of the State of California, USA.

The Court of Justice held that it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46. According to the Court of Justice "Article 4(1)(a) of Directive 95/46 it is to be interpreted as meaning that the processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State". A broad interpretation of Article 4(1)(a) of Directive 95/46 was confirmed in case C-230/14 *Weltimmo*[9].

With a view to the effective protection of individuals in terms of the processing of personal data, the GDPR changed the territoriality principle with regard to the application of EU data protection laws. Article 3 of the GDPR mostly repeats Article 4(1)(a) of Directive 95/46, confirming that the provision applies to the processing of personal data in the context of the activities of an establishment of a data controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The changes which considerably improve the system's efficiency and effectiveness are in Article 3(2) of the GDPR: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behaviour as far as their behaviour takes place within the Union".

---

[9] Judgment of The Court (Third Chamber) of 1 October 2015 in case C-230/14 Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.

With this provision the physical location of a data controller or processor becomes irrelevant: it is very important for a citizen of the EU due to the fact that giants of the net, like the previously mentioned Facebook or Google, are registered in third countries like the USA. But new regulations will not only apply to the big players of the internet but also to small and medium sized entrepreneurs from third countries, who sometimes might not be aware of the fact that they offer goods or services to data subjects in the EU[10].

II. New concept of consent

The new definition of assent to the processing of personal data is less rigorous – it might be not only a statement, but also clear affirmative action. Pursuant to the Polish regulations, the concept of assent varies – the assent shall be explicit and expressed intentionally, it may not be alleged or implied from the statement of intent with different content (Article 7 of Personal Data Protection Act)[11]. The new regulation diminishes the level of protection of data subjects by providing lower standards for consent.

The GDPR gives examples of potential forms of expression of an assent – it could be a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information 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. The GDPR clearly indicates that silence, pre-ticked boxes or inactivity should not therefore constitute consent[12]. For consent to be informed, the data subject should be aware at least of the identity of the data controller and the purposes of the processing for which the personal data are intended[13].

---

[10] See Czerniawski, supra note 6, p. 92.

[11] Act of 29 August 1997 o ochronie danych osobowych (on the protection of personal data) (Polish O.J. 1997, No. 133, Item 883).

[12] Recital 32 to the GDPR.

[13] Recital 42 to the GDPR.

Nevertheless it seems that the new definition of assets creates the risk of abuses such as the over-interpretation of individuals' behaviour, e.g. does visiting a website mean that the visitor agrees to the processing of personal data? Does installing the application or beginning to use the services automatically mean that consent was given? Even now a lot of entities operating in cyberspace, particularly those offering mobile applications, process personal data without the clear consent of data subjects, relying only on the implied consent. In such cases users very often are not aware of the fact that their personal data is being processed and they do not know anything about the scope and time of the processing. When it comes to their personal data, most individuals do not know their rights and this fact is often used by data controllers. With the new regulation we can be sure that the concept of consent will be abused in order to process personal data, and awareness levels will remain low.

A lot of emphasis is put on the voluntary nature of such consent. The GDPR indicates possible examples of situations when consent is not freely given, e.g. when the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. This is also the case when the data controller has a different legal basis for the processing, but nevertheless he gathers consent for the processing of the data (so called "illusion of consent"). Other situations are when the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Consent is presumed not to be freely given when there is a clear imbalance between the data subject and the data controller, in particular where the data controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Also, consent is not voluntary when it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.

However, none of this amounts to new insights. This is standard procedure at the moment when a court assesses whether consent is freely given, and takes these circumstances into account[14]. What is new is that for the first time these standards are clearly laid down in the legislation.

---

[14] The judgment of the Supreme Administrative Court of 6 September 2011 in case I OSK 1476/10, Legalis.

The situation is the same with the consent forms. The GDPR determines that 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 and that an abstruse and over-complicated consent form would be unacceptable and not binding. These requirements are well known and established in case-law[15].

Although we have the same new provision for internet users – 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[16].

The GDPR amends the terms of withdrawal of consent. The main difference is that prior to giving consent, the data subject shall be informed about the right to withdraw his consent at any time. This is very important, because now most people are not familiar with this right and believe that a given consent is permanently binding. The GDPR states that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The second innovation novelty is the obligation for data controllers to ensure that it will be as easy to withdraw as to give consent. How will this be done in practice? Simplicity of withdrawal must be assessed on a case-by-case basis and compare with the form of consent. For instance, if consent is given by ticking a box when visiting an internet website, withdrawal should be possible the same way. If consent may be given by an oral statement (e.g. via a phone hotline), withdrawal should be possible in the same manner. The essence of this solution is balance between the form of consent and the form of withdrawal: it cannot be as in the past, that one could give consent by simple ticking a box, but for withdrawal one must send a postal letter.

With the new concept of consent under the GDPR there is a question: do we need to give a new consent for the processing of personal data? Must data controllers gather new consents from data subjects? We find the answer to the questions in Recital 171 to the GDPR – it is not necessary

---

[15] The judgment of the Supreme Administrative Court of 4 April 2003 in case II SA 2135/02, Legalis; The judgment of the Supreme Administrative Court of 10 January 2013 in case I OSK 2029/11, Legalis.

[16] Recital 32 to the GDPR.

for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of the GDPR, so as to allow the controller to continue such processing after the date of application of this Regulation. In fact, data controllers who implement the provisions of Directive 95/46/EC/ and take into account the national supervisory authorities positions will not have to gather new consents. The processing of personal data on the basis of the consent of the data subject will not be possible when consent was not freely given, specific, informed, and unambiguous. This will concern checkboxes being chosen by default or very general consent form like „I give a permission to the process my personal data in accordance with the Act of 29 August 1997 on personal data protection".

III. Child's consent in relation to information society services

One of the most widely discussed subjects in the debates on new regulations, was the conditions applicable to a child's consent in relation to information society services[17]. According to Article 8 (1) of the GDPR where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. 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 authorized by the holder of parental responsibility over the child. What is important, Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. Initially, Poland was open to use this option, but after public consultation, concern has been expressed by representatives from the education sector, that this solution is too dangerous for minors.

---

[17] According to Article 4(25) of the GDPR, 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council. Article 1(1)(b) of Directive (EU) 2015/1535 states that 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services.

What should the data controller do to verify whether in fact he is dealing with a person over 16 years old? Asking about age is too simple, there's a high probability that the child will lie, and the same is true with putting the date of birth. Maybe a good option would be asking about the personal identification number (PESEL)? Although this option raises significant concerns as to its compatibility with the principle of data minimization.

Article 8(2) of the GDPR states that if a data controller is dealing with a person below the age of 16 years he must make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology. How to do this? Maybe children will have to send a scan of the written statement of the holder of parental responsibility? Or maybe they could indicate the e-mail address of the holder of parental responsibility who will receive an email with the activation link. The choice of appropriate mechanism is left to the data controller.

IV. Transparent information and communication

The data subject has a right to be informed about the processing of personal data concerning him or her. Under the GDPR, the scope of information to be provided by data controllers is much wider. According to Article 13 of the GDPR the controller must, at the time when personal data is obtained, provide the data subject with the identity and the contact details of the data controller (and where applicable also the contact details of the controller's representative and data protection officer), the purposes of the processing for which the personal data is intended, as well as the legal basis for the processing (in some cases also the legitimate interests pursued by the controller or by a third party). Successively the data controller must give information about the period for which the personal data will be stored, the recipients or categories of recipients of the personal data, if any, and, where applicable, the fact that the controller intends to transfer personal data to a third country or international organization. Other groups of information which must be provided concern the rights of data subjects, e.g. the existence of the right to request from the data controller access to and rectification or

erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability, the existence of the right to withdraw consent at any time, or the right to lodge a complaint with a supervisory authority. Where applicable, there is also an obligation to give information about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR as well as the significance and the envisaged consequences of such processing for the data subject[18]. This last one is very important when it comes to the advanced processing of a vast amount of data (big data), the creation of prediction profiles, or automatic data analysis[19].

So far, the vast majority of this information is provided only at the request of a data subject or the national supervisory authority. The aim of broadening the information provided by data controllers is to guarantee that the data subject will have the possibility to take a conscious decision about consent for the processing of his personal data. To facilitate this decision the GDPR states that all mentioned information shall be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child[20]. Moreover, according to Article 12(7) of the GDPR the information may be provided in combination with standardized icons in order to give in an easily visible, intelligible, and clearly legible manner a meaningful overview of the intended processing. Icons would be readable for citizens and also would help entrepreneurs to perform this information obligation.

The increased transparency and communication is very important for citizens. All the indicated information has an impact on any decision granting consent to the processing of personal data, but unfortunately so far most of it is not known to the data subject. Now, very often the data subject has no knowledge about basic issues such as the purposes

---

[18] Article 13 of the GDPR.

[19] K. Szymilewicz, *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony? (The reform of the European personal data protection law from the viewpoint of citizens' rights – more or less protection?)*, [in:] G. Sibiga (ed.) *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016 (General Data Protection Regulation. The current problems regarding the legal standards for the protection of personal data)*, C.H. Beck, Warszawa, p. 11.

[20] Article 12 of the GDPR.

and the period of the processing of his or her personal data, a situation which is unacceptable. Unfortunately Article 14 of the GDPR includes exemptions from the information obligation. In some circumstances, where personal data have not been obtained from the data subject, the data controller would not provide the data subject with the information e.g. when the provision of such information proves impossible, or would involve a disproportionate effort, or when obtaining it, is expressly laid down by Union or Member State law to which the controller is subject. These exemptions leave the door wide open to abuse. There is a risk that controllers may use Article 14 more often than it would be necessary. In this regard, a difficult task lies before Data Protection Supervisors[21].

V. The processing for a purpose other than that for which the personal data have been collected

The GDPR allows the processing of personal data for a purpose other than for which the personal data have been collected if, among other considerations, the processing is not based on the data subject's consent. The data controller shall ascertain whether processing for another purpose is compatible with the purpose for which the personal data is initially collected, taking into account, inter alia, any link between the purposes for which the personal data have been collected and the purposes of the intended further processing as well the context in which the personal data have been collected. This analysis and decisions would not be subject to the control of the Data Protection Supervisor, and thus the projected solution is potentially dangerous for data subjects[22].

VI. Right to data portability

For the information society, a new right to data portability could be very convenient. In the world of web apps, a solution which allows us to change from one service to another, with all our personal data, is very

[21] See Szymilewicz, supra note 19, p. 11-12.

[22] Ibid., p. 13.

welcome. According to Article 20 of the GDPR, data subjects have two options in the field of data portability. Firstly, a data subject can receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used, and machine-readable format, and has the right to transmit that data to another controller. In the second option the data subject will have the right to have the personal data transmitted directly from one data controller to another, where technically feasible. It is notable, that only personal data which the data subject has provided to a data controller is allowed to be transmitted – for instance, in the case of social media it can be debatable which data were provided by the data subject and which were created by the social service/controller[23].

Article 20(4) of the GDPR includes a clause which may limit the right to data portability and may be used by controllers to restrict competition on the cyber market, because it states that the right to data portability shall not adversely affect the rights and freedoms of others. The assessment of this problem is left to the data controller[24].

VII. Privacy by design, privacy by default

One of the most important changes that the GDPR brings is the establishment of the principles of p*rivacy by design* and *privacy by default*. The new regulation is beneficial to European citizens and transfers the responsibility for the protection of the privacy of personal information to the data controllers. However, from a commercial point of view, the new principle means a complete change in approach towards the processing of personal data.

The concept of *privacy by design* is well known in the doctrine and professional literature, often expressed by Data Protection Supervisors, notably in international fora[25], but the GDPR makes it a legal obligation.

---

[23] Ibid., p. 12.

[24] Ibid.

[25] At the 32nd International Conference of Data Protection and Privacy Commissioners in 2010 Resolution on Privacy by Design was adopted. According to the Resolution the foundational principles of *privacy by design* are: 1) Proactive not Reactive; Preventative not

The *Privacy by design* obliges data controllers, both at the time of the determination of the means for processing and at the time of the processing itself, to take into consideration the protection of personal data. The principle requires that, from the very beginning of its existence, any project involving the processing of personal data shall contain solutions to protect them. Initially, this principle referred to ICT (information and communication technologies) solutions and was meant to ensure the anonymity of the people using them, but now the term is used with a broader application, it refers e.g. to the creation of legislation, and more importantly to the creation of any applications, services, websites, business projects, electronic devices etc[26]. According to Article 25(1) of the GDPR, which refers to this principle, the data controller shall implement appropriate technical and organizational measures, such as pseudonymization, which is designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the *privacy by design* principle.

The *privacy by default* rule is one of the basic rules that constitutes *the privacy by design* principle. It assumes that the user's privacy is protected by default, and any changes to this setting may occur only at the user's explicit request. According to Article 25(2) of the GDPR the data controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing are processed. This means that, e.g. when we create an account on social network, fill in the contact form on the store's web site, or install apps for a mobile device, the data controller

---

Remedial; 2) Privacy as the Default; 3) Privacy Embedded into Design; Full Functionality: Positive-Sum, not Zero-Sum; 4) End-to-End Lifecycle Protection; 5) Visibility and Transparency; 6) Respect for User Privacy. See all Resolution: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf/ [last accessed 26.7.2017].

[26] M. Bienias, *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych (Data protection by design and data protection by default in the General Data Protection Regulation*), [in:] G. Sibiga (ed.) *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016 (General Data Protection Regulation. The current problems regarding the legal standards for the protection of personal data),* C.H. Beck, Warszawa, p. 53.

may ask us only for the data that really is needed to accomplish the goal. For instance, if you download a jogging app, it cannot automatically connect with your Facebook account and publish location, running time, rate etc. Also it should not be necessary to provide additional data about yourself. Similarly, when you create an account on a social network, it should not automatically be publicly available.

That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. The broader scope of access will depend only on the will of the user.

VIII. Profiling

The concept of profiling has been discussed since the early days of the preparation of the new regulation, where different positions have been taken, from acceptance, but only under strict conditions to general admission as any other processing[27]. 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, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement[28].

Generally, the GDPR prohibits automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her. There are, however, exceptions to this rule. This does not apply e.g. if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or when it is based on the data subject's explicit consent. Article 22(3) of the GDPR states guarantees for the protection of an individual's rights, such as the right to obtain human intervention, to express his or her point of view, and to contest the decision. However, compared to the

---

[27] See Szymielewicz, supra note 19, p. 14.

[28] Article 4(4) of GDPR.

existing regulations, like the Polish Personal Data Protection Act, these are rather general statements, not specific legal rights e.g. the right to a detailed explanation of the reasons for such a decision.

Potentially dangerous also is automated individual decision-making, including profiling, based on special categories of personal data ("sensitive data") referred to in Article 9(1), regulated in article 22(4) of the GDPR. Decision making based on sensitive data, like race, religion, sexual orientation, health status can give rise to discrimination, although the GDPR states that in such cases, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. However, lack of specific legal rights under the Regulation, mentioned above, allows us to doubt whether human rights will be totally respected[29].

IX. Final remarks

The substantial reform of the European data protection law is long-awaited. Data Protection Directive 95/46/EC was created in the nineties of the last century, when the Internet did not exist in today's sense, and there were no web searches, no smartphones, no apps, and no smart devices. This reform introduces many changes in the data protection system, e.g. it redefines the territorial scope for the application of personal data protection provisions, introduces the new obligations for data controllers and processors, introduces the institution of the Data Protection Officers, and specifies their new status and tasks. By introducing rules such as *privacy by design*, *privacy by default* or *privacy risk assessment* and *privacy impact assessment,* the GDPR constitutes a new approach to the issue of personal data security. One of the most important changes is granting more rights for the data subjects, which provides better protection in the digital world. However, some changes weaken the rights of citizens whose data are processed. Also, in some matters the GDPR leaves the Member States a degree of flexibility. Therefore, there is nothing we can do but wait for a final Polish project of a Personal Data Protection Act.

---

[29] Szymielewicz, supra note 19, p. 12.