Annales. Ethics in Economic Life 2018
Vol. 21, No. 7, Special Issue, 27–44
doi: http://dx.doi.org/10.18778/1899-2226.21.7.02

Ewa Kulesza
University of Lodz
Faculty of Law and Administration
Department of Social Security Law and Social Policy
e-mail: ekulesza@wpia.uni.lodz.pl

The protection of customer personal data as an element of entrepreneurs' ethical conduct*

Abstract

The right to the protection of personal data, which is part of the right to privacy, is a fundamental human right. Thus, its guarantees were included in the high-level regulations of the European Union as well as the legal norms of the EU Member States. The first Polish law regulating the protection of personal data was adopted in 1997 as the implementation of EU Directive 95/46. The law imposed a number of obligations on public and private entities which process personal data in order to protect the rights of data subjects and, in particular, to guarantee them the ability to control the correctness of processing of their personal data. Therefore, the law obliged data controllers to process data only on the basis of the premises indicated in the legislation, to adequately secure data, and to comply with the disclosure obligation concerning data subjects, including their right to correct false or outdated data or to request removal of data processed in violation of the law.

However, as complaints directed by citizens to the supervisory body—the Inspector General for Personal Data Protection—showed, personal data controllers, especially those operating in the private sector, did not comply with the law, acting in a manner that violated their customers' rights. In the hitherto existing unfair business practices of entrepreneurs, the violations of the data protection provisions that were the most burdensome for customers were related to preventing them from exercising their rights, including the right to control the processing of data, as well as the failure to provide the controller's business address, which made it impossible for subjects whose data were used in violation of the law or for the inspecting authorities to contact the company, a lack of data security and a failure

* The article is an updated version of the paper published in Polish in the *Annales. Ethics in Economic Life, 13*(1), 97–105.

to follow the procedures required by law, the failure to secure documents containing personal data or their abandonment, a lack of updating customer data, the use of unverified data sets and sending marketing offers to deceased people or incorrect target recipients, and excessive amounts of data requested by controllers.

The violations of the rights of data subjects recorded in Poland and other EU Member States—among other arguments—provided inspiration for the preparation of a new legal act in the form of the EU General Data Protection Regulation (GDPR) (which entered into force on 25 May 2018). The extension of the rights of people whose data are processed was combined in the GDPR with the introduction of new legal instruments disciplining data controllers. Instruments in the form of administrative fines and the strongly emphasised possibility to demand compensation for a violation of the right to data protection were directed in particular against economic entities violating the law.

Keywords: personal data protection, rights of data subjects, right to information, duties of personal data controller, GDPR, administrative fines, criminal liability, compensation for a violation of the right to personal data protection

JEL Classification: D18, M14

1. Introduction

The right to privacy and the right to the protection of personal data constituting its part, though distinguished as a separate right later, are basic human rights. Their significance is emphasised by the fundamental norms of international law, such as the Convention for the Protection of Human Rights and Fundamental Freedoms, as well as European law—including the Treaty on the Functioning of the European Union (Article 16) introduced by the Treaty of Lisbon or the Charter of Fundamental Rights of the European Union (Article 8).

The right to the protection of personal data has also been included—alongside the separately formulated right to privacy in Article 47—in the Constitution of the Republic of Poland, guaranteeing in Article 51 the right to "informational self-determination" for every person. Article 51 of the Constitution stipulates that no-one may be obliged, except on the basis of the statute, to disclose information concerning his person and that everyone shall have the right to access official documents and data collections concerning himself, as well as the right to correct and delete information which is untrue, incomplete or collected by means contrary to the statute. The data subject has the right of access to the data as well as the right to verify the truthfulness and correctness of the processed data along with the right to request a data correction, which constitutes the essence of personal data protection.

Due to the nature of the right to privacy and personal data protection, the legal norms regulating these issues acquire special significance, as they are an instrument to protect people's rights when they are violated by both public entities and private (business) entities that use personal data in their activity.

The importance attached to the protection of personal data is demonstrated by the significance of legal acts regulating the issue of data protection as well as a continuously extended catalogue of legal instruments guaranteeing everyone the right to this protection and the corresponding scope of responsibilities of the so-called personal data controllers.[1]

This extension of the rights of data subjects and the obligations of data controllers can be clearly seen when comparing European provisions regulating the protection of personal data, i.e. Directive 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 (Directive 95/46), and the Act of 29 August 1997 on the Protection of Personal Data, which is the manifestation of its implementation into the Polish legal system, with the currently binding Regulation of the European Parliament of 27 April, 2016, on General Data Protection (hereinafter referred to as the GDPR), repealing the Directive and the 1997 Act.

At the same time, despite numerous legal guarantees of data protection, in the practice of the functioning of public and private entities, there are cases in which controllers do not comply with the applicable laws, which leads to a gross violation of the rights of the data subjects.

The aim of the article is to show violations of personal data protection provisions by private sector entities in the previous legal environment, which constituted not only a breach of the law but was also unethical behaviour towards customers, and to present new instruments aimed at protecting the right to privacy and personal data, which hopefully will be a more effective means of controlling compliance with the law.

2. The right to the protection of personal data and the observance of the right by private sector entities under the 1997 provisions on personal data protection

The Act on the Protection of Personal Data, which was adopted in Poland in August 1997, imposed on all entities using personal data in their professional activities specific obligations related to their protection, and it guaranteed data subjects the right to control the processing of such data.

[1] The term personal data controller, defined in the same manner in both the previous and current provisions on personal data protection, means a natural or legal person, public body, unit or other entity that independently or jointly with others sets the purposes and methods of processing personal data.

The adoption of the Act on the Protection of Personal Data constituted the implementation into the Polish legal system of the philosophy and principles of protecting personal data detailed in Directive 95/46. It was also the fulfilment of Poland's obligations under the accession agreements to adapt the legislation to the European Union standards, as well as the implementation of the constitutional provision guaranteeing the right to personal data protection.

The Directive explicitly stressed that economic and social integration must lead to a significant increase in the flow of personal data between all entities involved privately or publicly in economic and social activities, and political integration must also lead to an exchange between individual national authorities—under Community law—of personal data for the purpose of performing duties and the implementation of tasks specified by law. However, pursuant to the Directive, the condition for the free exchange of data was the guarantee of the fundamental rights of every data subject: the right to privacy and personal data protection. This meant that the exchange of data had to take place with adherence to confidentiality principles and provide the guarantee of protection against illegal data processing, unauthorised data disclosure, alteration or loss, as well as the guarantee of data subjects' fundamental rights that constitute the essence of data protection: the right to information and the right to control data processing. A lack of these guarantees of the fundamental rights or differences in the degree of the protection of privacy and personal data in individual countries could lead to limiting data exchange due to discrepancies in the level of protection of individuals' rights and freedoms. It could even prevent economic projects from happening and make it difficult for public authorities to fulfil their legal obligations. Thus, the level of protection of individuals' rights and freedoms with regard to privacy and personal data protection needed to be equivalent in all countries which operate in the common market and which cooperate in the implementation of specific political and social activities.

The Directive, therefore, identified two basic pillars of economic and political cooperation: the admissibility and even necessity to exchange personal data in cooperation between states, especially in business transactions, as well as the obligation to protect data and guarantee certain rights to people whose data are processed (used) by public and private entities (data controllers).

Among the obligations of data controllers related to the protection of personal data, apart from processing data only on the basis of legal premises and with adequate data protection, the Directive required data subjects to be guaranteed the right to information about the processing of data as well as the right of access to and verification of their data. Data controllers' obligations corresponded to the rights of people whose data were processed, including the fundamental rights to information, to object to data processing, as well as to correct, delete or block data whose processing was incompatible with the provisions of the Directive, in particular, due to their incompleteness or inaccuracy.

2.1. Guarantees of the right to the protection of personal data in the light of the 1997 Act

The Act on the Protection of Personal Data, which was the implementation of the provisions of the Directive and Article 51 of the Constitution of the Republic of Poland,[2] did not limit the possibilities of using data in the activities of public entities of entities belonging to the private sector, but only imposed specific obligations on those entities. In accordance with the provisions of the Act, each entity collecting, maintaining, storing, changing or deleting, i.e., processing[3] personal data, was the so-called data controller,[4] obliged to exercise due diligence to protect the interests of data subjects. Pursuant to Article 26 Paragraph 1 of the APPD, this particular due diligence should consist in ensuring that data were processed in accordance with the law, collected for specified, legitimate purposes and not processed in a manner that was incompatible with those purposes, as well as in guaranteeing that data were factually correct and adequate for the purpose of processing, and stored in the form enabling the identification of the people whom they concerned, no longer than it was necessary to achieve the purpose of processing. The rules referred to in Article 26 of the APPD took on special significance for controllers from the private sector (entrepreneurs). In their case, the basis for the collection of data was not—as in the case of state authorities—a legal provision, but another of the premises indicated in the APPD, defining the lawful grounds for data processing. In the case of private sector entities, such a basis could be, for example, a contract between an entrepreneur and data subjects, or the consent of such people to use their data for marketing purposes.

The legislator, stressing in the provisions on the protection of personal data the obligation of the data controller to exercise due diligence in protecting the interests of data subjects and indicating that data were to be processed in accordance with the law, required compliance with the principles set out in the Act. This meant that the collection and use of data should only take place on the basis of one of the premises mentioned in Article 23 Paragraph 1 or Article 27 Paragraph 2 of the APPD, for specified, legitimate purposes, that data could not be processed in a manner incompatible with those purposes, and that the data controller was obliged to fulfil the obligations specified in the Act, providing data security and guaranteeing the rights of data subjects, described in detail in the

[2] Article 51 Paragraph 5 of the Constitution which stipulates that "principles and procedures for collection of and access to information shall be specified by statute" indicated the adoption of a separate act specifying all particular issues related to the implementation of the right to personal data protection formulated in the Constitution in a general manner.

[3] The term "processing" was defined in Article 7 Paragraph 2 of the APPD and is understood as "any operations performed on personal data, such as collecting, recording, storing, developing, altering, sharing and deleting, in particular those performed in information systems." An analogous definition of processing, although slightly extended to incorporate new forms provided as examples (such as "organising, structuring, adaptation or alteration, retrieval, consultation, combination, disclosure"), can be found in Article 4 Paragraph 2 of the GDPR, which means that the term "processing" will always mean any operations on personal data.

[4] The definition of data controller is provided in Article 7 Paragraph 4 of the APPD; currently the definition of data controller is defined in Article 4 Paragraph 7 of the GDPR.

provisions on the protection of personal data. In this respect, the Polish Act on the Protection of Personal Data, analogically to the then applicable EU Directive, emphasising the possibility of using personal data, provided their controllers with certain obligations, including the condition of guaranteeing data subjects their rights. This meant that the protection of personal data did not prevent the use of personal data to conduct business, but it stipulated that every entity processing personal data should act in accordance with the provisions of the Data Protection Act and with the principles set out in it, without violating the rights of data subjects.

It should be emphasised that the provisions on the protection of personal data did not specify only abstract and burdensome duties on the part of the controller. Fulfilling the duties was not solely intended to guarantee data security or appropriateness (adequacy) of data for the purpose of their collection and use but also to enable the data subject to control data processing, including the right to correct or update personal data in the case of incompleteness, a lack of timeliness, or redundancy for the fulfilment of a specific purpose, or collection in violation of the law. It was, and still is, extremely important that the entity collecting and using data should process data only to the extent necessary to achieve set objectives, but it should also guarantee that the data will not be used against the will of the data subject or without the data subject's knowledge for other purposes or by another entity, and that data will be true and current. This non-use of data for a purpose other than the purpose of the processing was to be guaranteed also by requiring the storage of data in a form enabling their identification only until the fulfilment of the set objective.

2.2. Examples of breaches of the right to data protection by private sector entities under the 1997 Data Protection Act

The fulfilment of obligations specified in the provisions on the protection of personal data has become particularly important in the case of data processing, i.e., data collection and data use by private sector entities. While public entities have a constitutional duty to act on a legal basis and within the law, which means that the legislator determines both the scope and purpose of data processing by these entities, controllers belonging to the private sector obtain data primarily in the framework of concluded contracts or on the basis of customers' consent to data processing, often based on trust in the data requester.

Thus, it was extremely important for the entity requesting data to fulfil the information obligation towards the person from whom the data were requested or whose data were obtained from another entity. This allowed the person whom the data concerned to make an informed decision on making the data available or it enabled the person to exercise his or her rights when the controller obtained data from another entity. In particular, it was important to provide information about the future data controller whose specification could determine whether or not the consent to the sharing and processing of data was given and the information about the obligatory or voluntary manner of data disclosure.

Providing information about the data controller could not be limited to giving the company name or the name with the post office address, but it had to include the full name of the company and its exact address which should allow the person whose data were used to contact the economic entity if ever the person wanted to check how the data were actually used, or in order to exercise his or her rights, including the right to object to the use of personal data or request their removal.

The information obligation also included specifying the purpose of data collection and entities that were data recipients, or at least a category of such entities. Finally, the information obligation required the indication of the right of access to the data content and the right to correct data, as well as the right to request the deletion of data or the non-use of data for marketing purposes.

The obligations of the personal data controllers, pursuant to the Act on Personal Data Protection of 1997, should be perceived not only through the prism of implementing applicable provisions but also as guarantees of the right to privacy and data protection of people whose data the controller processes, ensuring the security of data entrusted to the entity (data controller) by a person for a specific purpose, adequate (relevant) for the purpose of processing.

The Act required that the controller should be obliged to provide detailed information about the purpose of data collection and the obligatory or voluntary manner of transfer or collection of personal data, since knowledge passed in the course of performing the information obligation to the person whom the data concerned (even if the data came from another source than the person to whom the data pertained) determined whether the person would consent to the processing of data. The controller was also obliged to inform about the possible transfer of data to other entities, with an indication of at least the category of these entities. The person whose data were to be processed could only knowingly consent to that if he was aware of his rights and had comprehensive knowledge about the purpose of the processing, the obligatory or voluntary manner of data sharing, and the potential possibility of transferring data to other entities.

Providing this information was equally important for the data controller (entrepreneur) who could use the data within the limits that the person providing the data was informed about. The fulfilment of the information obligation was therefore equally valid and binding for the person providing the data as for the controller (entrepreneur).

Meanwhile, the general practice of entrepreneurs was non-compliance with the information obligation by not providing the purpose of data processing, misleading data subjects by giving a different purpose than the actual one or providing incomplete information, and then freely using the customer data. In particular, marketing companies avoided providing customers with information about the source of data or the full name and address of the company's headquarters, which prevented customers from exercising their rights, e.g. the right to object to the further use of their data for marketing purposes.[5] However, even if the information

[5] Cf. cases investigated by the Inspector General for Personal Data Protection (Polish: GIODO): GI-DS-430/150/06, GI-DS-430/167/06 (Generalny Inspektor Ochrony Danych Osobowych, 2007, pp. 37–38).

identifying the company (e.g. a marketing one) was given, the people to whom a parcel was addressed could not effectively exercise the right to object to the processing of their data—the objections made were not respected or were taken into account only after the intervention of the data protection authority.

A breach of customers' rights also involved the inability to disagree to the use of data for various purposes (e.g. providing data to so-called cooperating entities) due to the construction of the consent form that did not provide for the possibility of choice; no objection to the free use of data—in the absence of the possibility of not giving consent by the customer—provided a pretext for the free use or even sale of data to other entities.[6]

Datasets processed for the purposes of concluding a given contract were used to create subsets sold to other business entities, most often to marketing companies, and the multiplicity of additional information about customers facilitated the creation of such subsets according to various criteria (e.g., age, place of residence, education). The data controller believed that since the data were processed on the basis of customers' consent, the controller became their "owner" and could, therefore, use them freely, regardless of the purpose of collecting the data that customers had been informed about. The controller also recognised that such a dataset could be treated as an additional source of profits from the sale of data. The verdict of the Supreme Administrative Court of February 2008, prohibiting one of the telephone network operators from selling subsets created from its customers' dataset, offered for sale to other companies, may prove that this is not an example of a hypothetical reprehensible activity on the part of the data controller.[7]

The collection by a business owner of large amounts of unnecessary, detailed information about customers—under the threat of failure to conclude the contract—was a violation of not only the Act on the Protection of Personal Data, but also the privacy of customers. A classic example was the demand made by salespeople working for telephone network operators that people should present two or even three documents confirming their identity, and then photocopying them. Another action which violated privacy was making a photocopy of the entire (at the time in the form of a booklet) identity card containing information completely unsuitable for establishing the identity of the customers, such as previous places of employment, former places of residence or dates of birth of their children.[8] After changing the provisions of the telecommunications law, clearly specifying the scope of customer data processed, it turned out that employees of telephone network operators no longer needed to confirm a customer's identity and photocopy many documents containing different customer data, although the data contained in the new identity card are relatively limited. However, the problem of appropriateness (adequacy) of data for the purpose of processing continued to appear in the activities of banks. They demanded a great deal of information, not only confirm-

[6] Cf. cases investigated by the GIODO in 2006: GI-DS-430/224/06, GI-DS-430/250/06 (Generalny Inspektor Ochrony Danych Osobowych, 2007, p. 37).
[7] The judgement of the Supreme Administrative Court II SA/Wa 1252/07.
[8] Cf. cases GI-DIS-130/99/539, GI-DIS-245/99/654, GI-DP-445/99/451 (Generalny Inspektor Ochrony Danych Osobowych, 2000, p. 118).

ing the creditworthiness of the customer, but also family relationships or events from the past, which significantly violated customers' privacy. From the point of view of the provisions on the protection of personal data, this activity was a breach of Article 26 of the Act, requiring the controller to protect the interests of data subjects, and from the point of view of customers it was an unjustified violation of their privacy, and thus unethical conduct on the part of the entrepreneur.

Another form of violating customers' rights was the processing of data without complying with the information obligation in any respect. In cases submitted to be investigated by the Inspector General for Personal Data Protection, business entities registered abroad (most often in the USA) promoted products and services in the mail-order sale system, without informing customers about their status and address, the purpose of data processing or the data source. This prevented the claimants not only from filing a request to delete data or, for example, not forward data to other entities, but also from determining where the data were obtained from. The activities of such entities were combined with the offer of "cash prizes" provided under the condition of the purchase of a specific product or goods "at a discount price". Despite the purchase or a transfer of money, however, customers did not receive the goods, or the offers turned out to be unfavourable for the buyers (Case GI-DS-430/465/04). Letters from companies were also formulated as "a decision on the awarding of a grant", "a payment decision" or they contained information on high winnings being awarded. However, to collect it, the recipient had to meet several conditions, for example, call a given phone number (the cost per minute ranged from a few to over ten Polish zlotys).[9] Such activities were classified as fraud to the detriment of the customers.

The lack of verification and updating of data at the controller's disposal is also a flagrant violation of customers' rights. The processing of substantively correct data, adequate for the purposes resulting from the Data Protection Act, was not only the responsibility of the data controller but also an important instrument to protect the interests of customers. Meanwhile, complaints addressed to the data protection authority indicated that even entities that should exercise special care in protecting customers' interests (banks and other banking institutions) processed outdated data (e.g. about borrowers), which subjected such people to specific losses in the form of, for example, the refusal to grant loans, since they were considered to be in debt. The reasons for such actions were not only related to technical problems with the functioning of the IT system, for example, a lack of compatibility of the banks' IT systems with the Credit Information Bureau system, but also simple omissions on the part of the banks, which led to the relevant data being updated after many months. An example could be the case in which a data update—in the form of the transfer of information on the repayment of a loan to the register of the Credit Information Bureau—took place only after 18 months and concerned 55,000 customers (Generalny Inspektor Ochrony Danych Osobowych, 2007, p. 32).

[9] Cf. cases GI-DS-430/91/04, GI-DS-430/130/04 (Generalny Inspektor Ochrony Danych Osobowych, 2005, p. 199).

Cases regarding the use of non-updated datasets by marketing companies were of a different nature and were associated with moral losses. If, in accordance with the Act on Personal Data Protection, when collecting data not from the data subject, companies first complied with the information obligation after obtaining the data, and subsequently undertook marketing activities, they were able to verify and update relevant data, removing not only information about the people that did not consent to the use of their data, but also the data of deceased people. Failure to comply with statutory obligations meant that marketing offers were sometimes directed to the deceased, which was a particularly unpleasant experience for family members, especially when the loved one had been dead for some time, and the marketing offer, formulated in a fairly direct form,[10] suggested that the deceased had actively participated in recent weeks in a "game," and "had just gone to the third stage," and therefore a prize awaited that person.

A separate problem was the fulfilment of the obligation to secure data properly. A lack of data security could lead to unauthorised access to the data by those who could use such information to the detriment of the data subjects. This failure to fulfil the obligation to secure data could take the form of a lack of appropriate technical devices (e.g. the failure to secure the IT system), failure to comply with the procedures and documents related to data security specified in the Act and the implementing regulations, but it could also result from a lack of knowledge of employees of economic entities about the need to protect data or from disregarding employee duties. Occasional cases of finding customer information, e.g. in the form of printouts from banking information systems in the garbage or in public places, indicated a disregard for the issue of data security and, consequently, a disregard for customers.[11] A particularly drastic example of negligence was the abandonment of customer documentation in the event of the liquidation of a company or one of its branches. This could indicate a lack of professionalism of the employees of a given economic entity, especially when the data provided not only included information identifying the person but also information related to the person's health status (cases of throwing out medical documents without its anonymisation) or financial status (bank printouts). Cases of using business IT systems to conduct private correspondence via the company's Internet access can be explained by the employees' lack of professionalism, but also—as can be surmised—by the failure to train employees or the failure to apply appropriate procedures. The effect of such actions could have led to facilitating hackers' access to the company's IT system and, as a result, to access to large amounts of customer data, data theft or theft of money from customers' bank accounts.

[10] The offers used the names of people, e.g.: "Dear Peter, you have reached the next stage of the competition and won 50,000 Polish zlotys."

[11] Such cases were particularly frequent in the initial period of the Act on the Protection of Personal Data, as evidenced by cases described in the 1999 GIODO report (Generalny Inspektor Ochrony Danych Osobowych, 2000, pp. 136–137). Even nowadays, the media continue to report on documents containing personal data being abandoned, e.g. of bank customers.

Violations of customers' rights were particularly glaring when the business activity conducted was based on the assumption of the mutual trust between entrepreneurs and customers. Customers perceived a lack of banking system security or marketing activities being conducted by banks for other business entities as being particularly unethical due to the universal perception of banks as public trust entities.

The manifestation of actions violating ethical standards also included providing the media with information about customers, including information covered by another form of secrecy, such as telecommunications secrecy. For example, a journalist was informed by a telephone network operator about calls and the content of conversations between a person in proceedings before a parliamentary committee of inquiry and other people, and the content of these conversations was later published in the newspaper "Rzeczpospolita".

3. Special protection of the rights of data subjects in the provisions of the GDPR and the new Act on the Protection of Personal Data

Violations of the provisions on the protection of personal data concerned not only business entities operating in Poland, but they were also observed in other EU countries,[12] as indicated by complaints to the European Court of Justice concerning the refusal to delete data from files kept by private entities, despite such requests being made by data subjects.[13] The European Commission was inspired to adopt a new legal act introduced into the legal systems of all the EU Member States—i.e. the General Data Protection Regulation (GDPR)[14]—by the disregard for the applicable provisions on the protection of personal data manifested by private sector entities, non-uniform and inconsistent interpretations of the provisions of the Directive in various EU countries, and diverse ways of implementing the Directive into national legislations.

[12] As evidenced by the justification for the first draft of the Regulation of the European Parliament of 2nd January 2012.

[13] The most well-known case was that of Schrems v. Ireland's Data Protection Commissioner (reference no. C-362/14), settled by the verdict of the Court of Justice of the European Union of 6 October 2015, which concerned the request to delete Facebook user M. Schrems's data from the company's data collection. Although the issue itself was multi-faceted, and its significance had a broader dimension than only in relation to the protection of the rights of data subjects (in the ECJ judgement, among others, the basis for transfer of EU personal data to the USA was negatively assessed), it was a symbol of the behaviour of private sector entities disregarding their customers' rights.

[14] The EU regulation is an instrument of harmonising law in the European Union, a generally applicable legal act entering the legal order of a Member State. This means that since its entry into force, it has been part of the national law of each Member State and is directly applicable without transposition into national law (cf. Barcz, Górka & Wyrozumska, 2015, pp. 283–284).

The new provisions create new disciplinary instruments for data controllers as well as strengthen the rights of data subjects and expand the responsibilities of data controllers, especially those who process data based on people's consent, which is the basic premise for data processing by entities belonging to the private sector (entrepreneurs).

3.1. The GDPR extension of the rights of data subjects

In addition to the extended right to obtain information from the data controller and the right of access to data and the right to correct data already guaranteed in earlier provisions on the protection of personal data, based on the GDPR, everyone has been granted new rights, such as the right to delete data ("the right to be forgotten"), the right to limit data processing, the right to data transfer, the right to object and the right to be informed of a breach of data security.

In the framework of this article, it is difficult to discuss all the rights of people whose data are processed. However, it is worth drawing attention to two examples of the provisions contained in the Regulation extending the rights of data subjects.

In the course of the work on the GDPR, it was assumed that extending the scope of information provided to data subjects by the data controller at the moment of data collection, as well as the scope of information provided if data were obtained from another source (not from the data subject), should strengthen the rights of data subjects. It was also intended that the fulfilment of the information obligation by the data controller should take place in a concise, transparent, understandable and accessible form, in clear and simple language.

Supplementing the information clause with additional information provided to people whose data are collected or already processed and obtained from a source other than the data subject, is supposed to give data subjects the opportunity to make a rational decision, based on wider than ever knowledge, regarding consent (or lack of consent) to data processing. In addition to information already provided to identify themselves, as well as information on the purpose of data processing and possible data recipients or categories of data recipients, and the rights of the data subject, data controllers are obliged to indicate the period during which data will be processed. When this is not possible, they should provide criteria determining this period, along with information about the right to withdraw consent at any time, or about other rights of the data subject, including the possibility to lodge a complaint with the supervisory body or the right of access to personal data.

The right to obtain copies of processed personal data, apart from the provisions existing in the earlier legislation on the right to obtain information at the request of the data subject, complements the right to information. The controller's obligation to supply a copy of data to the person whose data are processed provides the opportunity to control the scope of the information processed.

The importance that the EU legislator attaches to granting individuals real access to data, and not only the information about the categories of data being processed, is demonstrated by a broad discussion of this right in the Preamble to the Regulation (recital 63). In this recital of the Preamble, it is clearly emphasised that every natural person should have the right of access to the data collected "in order to be aware of, and verify, the lawfulness of the processing", and if possible, the data controller should provide "remote access to a secure system which would provide the data subject with direct access to his or her personal data".

The new provision, which is worth noting, propagated as the "right to be forgotten", is the right to demand the immediate deletion of data from the files kept by the data controller, and if the controller has publicised the data, this right is extended to other controllers whom the "primary" controller should inform about the fact that the person requests that they should remove all links to these data, copies of personal data or their replications (Article 17 of the GDPR). "The right to be forgotten" applies in the cases mentioned in Article 17 Paragraph 1, including when one of the premises stipulated is met, i.e., when personal data are no longer necessary for the purposes for which they were collected, when the person withdrew the consent which was the basis for data processing, when the person objects to the processing of data, and when there are no reasons justifying data processing, if the data were processed unlawfully or should be removed in order to comply with legal obligations under the law.

"The right to be forgotten" is not absolute, as it has been weakened by the exceptions of its application mentioned in Article 17 Paragraph 2 and 3, and is therefore perceived as the law "which promises more than it gives" (cf. Barta & Kawecki, 2018, p. 410). There is also doubt about the possibility of the effective deletion of data that have been made public on the Internet due to the universal access to such data and the possibility of using them by undefined people (entities) who have obtained the data from this generally available source.

When discussing the newly established rights of people whose data are processed, one should also point out the right of the data subject—and the obligation of the data controller—to be informed about a breach of data security in the event of a violation of data protection provisions and a high risk of violating the rights or freedoms of people that the data concern (Article 34 of the GDPR). The notification should be made without undue delay and should include a description of the nature of the breach along with information on the possible consequences of the breach and measures taken by the controller to remedy the breach, including measures taken to minimise its effects. The notification should also include the name and contact details of the data protection officer from whom more information can be obtained.

The justification for granting data subjects the right to be informed about an event constituting a breach of data protection is the protection against the effects of such an event and the possibility of taking preventive actions.[15]

[15] In annotations to the GDPR, examples of preventive measures, such as changing passwords for access to a specific service, are provided (cf. Bielak-Jomaa & Lubasz, 2018, p. 719).

3.2. Strengthening the instruments for disciplining data controllers in their compliance with the provisions of the GDPR and the new Act on the Protection of Personal Data

The purpose of amending the provisions on the protection of personal data was to protect data more effectively by guaranteeing individuals better control over data processing. It was also designed to force data controllers to protect data more effectively as well as observe the rights of the data subjects.

Instruments which are intended to "force" data controllers to follow the data protection rules are the GDPR provisions that allow fines to be imposed of on personal data controllers. It also allows people whose data protection rights have been violated to demand compensation. Additionally, the new Act on the Protection of Personal Data of 10 May 2018 includes criminal provisions.

3.2.1. Administrative fines

The Regulation makes it possible for the supervisory authority to impose administrative fines on data controllers that violate provisions on the protection of personal data (Article 83 of the GDPR). Fines should be effective, proportionate and dissuasive, imposed on a case-by-case basis, in addition to or instead of "corrective" measures that the supervisory authority can use based on Article 58 Paragraph 2 of the GDPR.[16]

The provisions of Article 83 Paragraph 2 determine the conditions that must be taken into account when imposing administrative fines. In any event, the imposition of a fine must be individualised by assessing the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing, the intentional or unintentional nature of the violation, the category of personal data affected by the breach, and by evaluating the effectiveness of the technical and organisational safeguards applied by the controller to the processed data. The assessment that forms the basis for the determination of the administrative fine is also to be influenced by the attitude of the data controller to the protection of personal data, and, in particular, the existence of previous violations on the controller's part.

At the same time, the EU legislator recognised that breaches of the right to data protection when controllers are entities belonging to the private sector deserve special condemnation. With regard to these entities, the legislator provided for the possibility of imposing a fine of up to EUR 10 million or 2% of the total yearly global turnover from the previous year in the case of minor offenses listed

[16] Pursuant to Article 58 Paragraph 2 of the GDPR, each supervisory body is endowed with "corrective powers" towards a data controller who may have violated or who did violate the provisions of the GDPR by planned or performed processing operations. These powers include issuing warnings and reprimands, ordering the controller to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation, ordering the controller to bring processing operations into compliance with the provisions of this Regulation, ordering the controller to communicate a personal data breach to the data subject, imposing a temporary or definitive limitation including a ban on processing, or ordering the rectification or erasure of personal data.

in Article 83 Paragraph 4 of the GDPR, or fines of up to EUR 20 million or 4% of the total annual turnover in the case of more serious violations listed in Article 83 Paragraph 5 of the GDPR. They include, among others, the violation of the rights of data subjects (Article 83 Paragraph 5 b of the GDPR), leaving national legislators with the discretion to determine the admissibility of imposing fines and their amount in relation to public sector entities.[17]

3.2.2. Facilitating the pursuit of civil claims for compensation for a violation of the right to data protection

Article 82 of the Penal Code provides for the possibility of claiming damages for a violation of the provisions on the protection of personal data by any person who has suffered material or non-material damage as a result of an infringement of the Regulation.

The right to claim compensation pursuant to Article 82 of the GDPR is not a new solution—a similar provision was included in Directive 95/46. However, this right was not repeated or developed in the existing Polish provisions on the protection of personal data. This meant that people who considered that their right to data protection had been violated could apply to a civil court with a claim to award damages based on the provisions of the Civil Code. Such cases did occur;[18] however, the burden associated with going to court rested with those people.

Chapter 10 (articles 92–100) of the Act on the Protection of Personal Data currently in force highlights the possibility of pursuing claims for a breach of personal data protection provisions, creating the legal basis for special support from the supervisory body for people who would decide to file a suit, and imposing obligations unknown in the former provisions on the district courts competent to deal with such matters.

Providing support in the pursuit of a claim for compensation for a violation of the right to personal data protection, the President of the Personal Data Protection Office may institute proceedings for the benefit of the data subject, and may also—with the consent of the plaintiff—enter the proceedings at each stage. Additioanlly, if notified by the court about pending proceedings, he is obliged to immediately inform the court about any matter regarding the same violation, if such a case is being adjudicated by the President of the Personal Data Protection Office or the administrative court, or if it has been concluded.

Courts conducting proceedings for compensation for the damage caused by a violation of personal data protection provisions are, however, bound by the findings of the enforceable decision of the President of the Personal Data

[17] With such high administrative fines that may be imposed on private sector entities, Article 83 Paragraph 7 of the GDPR leaves it to each Member State to decide whether and to what extent administrative fines may be imposed on public authorities and bodies; in the new Act on the Protection of Personal Data, the Polish legislator has provided for administrative fines of up to PLN 100,000 for state and local government cultural institutions (Article 102 of the APPD).

[18] For example, a case concluded with a court awarding compensation to former Petrobank customers in connection with the bank's violation of personal data protection provisions (www.parkiet.com/Wiadomosci/311149873-LG-Petro).

Protection Office regarding the violation of provisions on the protection of personal data or findings of a final judgement issued as a result of lodging a complaint with the administrative court.

3.2.3. Criminal liability of data controllers

Although the GDPR includes liability in the form of administrative fines imposed for a violation of provisions specifying the grounds for data processing in Article 6 and Article 9—which means that data processing without reference to any of these premises is a violation of the provisions on data protection—in Article 107, the new law additionally provides for criminal liability for the processing of personal data when it is not permitted or when the entity processes data which it is not authorised to do.

The Polish legislator decided that such a breach of the provisions on the protection of personal data should be punished with a fine, a restriction of liberty or imprisonment of up to two years—if the entity processes "ordinary" data—or imprisonment up to three years if the unacceptable processing concerns data subject to special protection.

The previous experience of the Inspector General for Personal Data Protection related to refusals to prosecute violations of the protection of personal data by the prosecutor's office, in particular, the reference to the negligible social harmfulness of the crime or a lack of crime, give grounds for the recognition that the threat of imposing an administrative fine will be taken more seriously by data controllers than penalties provided for in Article 107 of the Data Protection Act.

4. Conclusions

The practice of applying the no longer binding Act on the Protection of Personal Data provided many examples—of which only some have been presented in the article—indicating not only the non-performance of obligations resulting from previously applicable provisions but also a lack of ethical behaviour in dealing with customers. And while the past tense was used when discussing examples of violations of customers' rights in many cases, it should be stated that unethical and infringing practices of economic entities were not uncommon[19] and it cannot be ruled out that they will also happen nowadays, as evidenced by the fact that cases of violating customers' rights from the recent past are still being adjudicated by the administrative courts (cf. the case concluded by the Supreme Administrative Court's ruling of 18th of April, 2018, the reference number I OSK 1354/16).

[19] For example, the activities of law firms, described by the press, specialising in obtaining compensation for victims of road accidents that buy illegally the names of victims of accidents or use the state of shock that victims of accidents are in to swindle signatures on contracts authorising them to file claims for compensation for an excessively high commission (cf. e.g. article by Bojanowski, 2009, p. 2).

In the hitherto encountered unfair practices, the most burdensome legal infringements for customers included preventing their rights from being exercised, including the right to control data processing, not providing the company's address to prevent access to it by data subjects or the controlling authorities, a lack of data security and not applying the required procedures, not securing documents containing personal data or simply abandoning them, not updating bank customers' data in the register of the Credit Information Bureau, using unverified datasets and sending marketing offers to deceased people, or controllers requesting data inappropriate for the purposes stated or requesting an excessive amount of data.

The presented examples of actions taken to the detriment of customers undermined confidence in business entities and infringed personal rights, and even subjected customers to material damage. In turn, misleading as to the purpose of data processing, transferring data to other entities, selling datasets or trading data collected for another purpose were not only unethical activities but also activities that provided unjustified profits to entrepreneurs at the expense of customers' rights.

It is difficult to clearly determine the reasons for this type of behaviour on the part of business owners. Undoubtedly, these reasons stem from the disregard for the applicable law on the part of the people violating the law as well as the prosecuting authorities, which responded to the majority of notifications of suspected criminal offenses with information that they had failed to prosecute or they had dismissed cases due to the negligible social harmfulness of the perpetrator's act. The reaction of the prosecutor's office was so striking because it was related to a violation of the provisions protecting the constitutionally guaranteed right of citizens.

It can be hoped that the situation will change under the current GDPR, in particular, due to the entry into force of the above-mentioned provisions allowing for the punishment with financial penalties of data controllers who violate the law and providing a real opportunity to claim compensation for a violation of the right to personal data protection. However, the question arises whether unethical entrepreneurs will not risk making a profit over the threat of even a severe financial penalty or paying compensation to a person who had been put at risk by their personal data being used in a manner contrary to the law.

References

Act of 10 May 2018 on the Protection of Personal Data, *Journal of Laws* 2018, item 1000 [Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000].

Act of 29 August, 1997 on the Protection of Personal Data, *Journal of Laws* 2016, item 922 as amended [Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2016 r., poz. 922 ze zm.].

Barcz, J., Górka, M., & Wyrozumska, A. (2015). *Instytucje i prawo Unii Europejskiej. Podręcznik dla kierunków prawa, zarządzania i administracji*. Warszawa: Walters Kluwer.

Barta, P., & Kawecki, M. (2018). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz* (P. Litwiński, Ed.). Warszawa: C.H. Beck.

Bielak-Jomaa, E., & Lubasz, D. (Eds.) (2018). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: Walters Kluwer.

Bojanowski, M. (2009, July 23). Ucywilizować łowców nieszczęść. *Gazeta Wyborcza, 171*.

Directive 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. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

Generalny Inspektor Ochrony Danych Osobowych. (2000). *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999 r. – 31.12.1999 r.* Warszawa: GIODO.

Generalny Inspektor Ochrony Danych Osobowych. (2005). *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2004*. https://giodo.gov.pl/data/filemanager_pl/727.pdf

Generalny Inspektor Ochrony Danych Osobowych. (2007). *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2006*. https://giodo.gov.pl/data/filemanager_pl/1051.pdf

Kulesza, E. (2010). Ochrona danych osobowych klientów jako element działania etycznego przedsiębiorcy. *Annales. Ethics in Economic Life, 13*(1), 97–105.

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). *Official Journal of the European Union*, L 119, vol. 59. https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A32016R0679