JOURNAL OF MODERN SCIENCE
TOM 2/51/2023
www.jomswsge.com

DOI: https://doi.org/10.13166/jms/168314

Aleksandra Klich
University of Szczecin, Poland
aleksandra.klich@usz.edu.pl
ORCID: 0000-0002-2931-712X

PERSONAL DATA PROTECTION IN THE ENERGY SERVICES MARKET – SELECTED ISSUES

Abstract

The article deals with the protection of consumers' personal data in the energy services market, considering the penalties imposed by national supervisory authorities between April 2018 and December 2022. The publication discusses Principles of personal data processing in the energy sector and Innovative technological solutions and technical safety in the policy of sustainable development. The author focuses on administrative fines imposed in the energy sector in Europe. The article recognizes the role that administrative fines can play in defining a new category of state revenue.

Keywords: *smart meters, personal data protection, GDPR, consumer data, energy sector, administrative fines*

Introduction

It seems that energy sector is an area where investment in digital transformation took place faster and more willingly than in other socio-economic sectors. It was linked to the desire to develop the current activity. The energy sector is undergoing a "digital revolution", where information and communication technologies (ICT) are increasingly used throughout the energy infrastructure, leading to the increasing digitization of production, storage, and consumption processes (Barichella, 2019, p. 1). Each investment and development, while using modern technological solutions, is not only an organizational and economic challenge, but is also burdened with the need to build mechanisms and use tools that guarantee a high level of security of processed data, including personal data. The rapid development of digital technologies, observed since the late 1970s, resulting in the expansion of the catalog of traditional threats to physical security, currently provides the basis for defining new digital threats resulting from the interconnectedness of physical and virtual services, and recently also from the exploitation of huge data sets (Eriksson, Giacomello, 2007, pp. 14-15; Schneier, 2015, p. 244). Popularization of the issue of personal data protection, is becoming an inseparable element of a modern model of a consumer using services offered by entities from the energy sector. With the increase in society's dependence on digital technologies, many methods of ensuring security have been improved. Currently, they address issues such as control over data, resilience of IT systems and overall capacity for technological development. It is possible to say that security has been digitized (Rajavuori, Huhta, 2020, p. 353-367).

The impact of EU regulations imposing obligations regarding the need to ensure the security of processed personal data on the activities of regulatory authorities is very large. The extra-territorial scope of the 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 ("GDPR") is significant. There is no doubt that energy companies are increasingly becoming data companies, while using data concerning not only energy, but above all personal data, which are tools for energy efficiency

mechanisms. For this reason, the impact of personal data protection rules on the energy sector is extensive.

Among the many areas in which entities from the energy sector are obliged to pay particular attention to the protection of consumer personal data, the following areas can be distinguished:

a. areas related to the actual use of energy and used to perform the transmission contract;
b. areas related to the use of online platform that facilitates ongoing control of expenses, monitoring of energy consumption in connection with the installation of a remote reading meter;
c. areas related to marketing and promotional activities.

The implementation of smart meters is associated with complex personal data processing operations. The vast majority of data subjects may not be aware of the nature of these operations, the organizations that use their data, and the potential impact this may have on their privacy. The consequence of the lack of awareness of the processing of personal data is that these persons are not able to make informed decisions in this regard. In practice, once a connectivity-enabled smart meter is installed, it may be difficult for consumers to prevent meter data collection. It is necessary to focus on the impact of the changes observed in the energy sector on the obligations related to the need to securely process personal data of consumers on this market. This is expressed not only in the need to determine whether data from measuring devices can be qualified as personal data, but also what obligations rest on energy distributors towards persons whose data is processed.

Literature Review

From the perspective of the subject of this study, it is important to establish a catalog of personal data in a way that allows to determine the status of the so-called measurement data. The term "personal data" is generally defined as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly,

in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. The literature points out that identifiability depends on whether, taking into account the factors listed above, it is possible to identify the person to whom the data held by a given company or institution relates. Both in the literature on the subject and in the jurisprudence, a subjective and an objective concept can be distinguished in relation to the concept of personal data. According to the first concept, identifiability depends on the circumstances: a good example can be a PESEL number – for one person it may be only a sequence of eleven digits, especially when that person does not know that it is indeed someone else's PESEL number and does not have any additional data identifying the person to whom the number relates, for another person (who has additional information), the same PESEL number may be personal data. According to the second concept, there is a presumption that any information about a person is personal data (Mednis, 2020, p. 934 et. seq). This concept is valid from the perspective of measurement data.

The literature also emphasizes that in order to determine whether a particular method can be used with reasonable probability to identify a person, all objective factors such as the cost and time needed to identify the person, as well as the technology available at the time of data processing and technological progress should be taken into account. Such an approach and reference to the criterion of "technological progress" makes it possible to conclude that the scope of the concept in question may change over time, because information which currently cannot be connected to a specific person, in the perspective of progressing civilization and technological development, can potentially be classified as personal data in the future (Sakowska-Baryła, 2018, p. 23 et. seq). Personal data may therefore take various forms, such as: photos, videos, recorded voices (Mednis, 2020, p. 35), so-called biometric data, pupil features, fingerprints, facial features, hand geometry (Drozd, 2007, p. 41), messages expressed and saved in any way, regardless of the manner, scope, and freedom of their sharing, and regardless of the way they were obtained (Barta, Fajgielski, Markiewicz, 2004, p. 370). It is not possible to determine in advance a catalog of information, even of an open nature,

which may be considered as personal data. This catalog is open, and the representatives of the doctrine emphasize that any attempt to close it is doomed to failure due to the ongoing technical and technological development. It is popular in the literature to state that any information, regardless of the way and form of its expression, may be assessed from the point of view of the concept of personal data and any information may be considered as information of a personal nature. Specific information does not have to be universally understood either (Sibiga, 2003, p. 33). The legal nature of this information will be assessed individually for each of its holders. It does not have to be true either (Barta, Fajgielski, Markiewicz, 2004, p. 371). This should be understood in such a way that it may refer to circumstances that objectively do not exist, but it can be assigned to a specific, identifiable natural person. The status of personal data can therefore potentially be granted to any information relating to a natural person, including data of an economic nature, relating to work life, etc. (Dammann, Simitis, 1999, p. 109).

In addition to the obvious data identifying persons (e.g., name and surname), contact details (e.g., telephone number, e-mail address), or address data (e.g., mailing address, address of residence), a modern catalog of personal data processed in the energy sector is extended with measurement data, which is related to the policy of installing smart metering systems. Energy consumption patterns obtained from smart meters can reveal much more than just the amount of energy used. A smart meter can record every fifteen minutes (or less) what someone is doing in their home in terms of energy consumption (Knyrim, Trieb, 2011, p. 121-128). The use of household appliances is an indicator of human behavior and allows individuals to be identified. Smart meter data can also reveal if someone is away from home and what household appliances the consumer is using (Huhta, 2020, pp. 5-22). Finally, such frequent data collection can reveal consumers' daily habits, which can affect their privacy (Tonyali, Akkaya, Saputro, Selcuk Uluagac, Nojoumian, 2018, pp. 547-557). Therefore, the operation of smart meters involves the processing of "personal data" and must comply with the EU General Data Protection Regulation (GDPR) (EDPS TechDispatch, 2019). The fact that data from smart meters constitute personal data is also confirmed by the Article 29 Working Party in its opinion. It is clearly indicated that the use of smart meters makes

it possible to process personal data such as: unique smart meter ID and/or unique property reference number, metadata referring to the configuration of the smart meter, a description of the message being transmitted, for example whether it is a meter reading or a tampering alert, a date and time stamp, or the content of the message itself. All this information can increase the level of identifiability of the smart meter user; therefore, it must be qualified as personal data within the meaning of EU Regulations.

Principles of personal data processing in the energy sector

The basis of processing

The GDPR defines several basic rules for their processing so that this action is lawful. The dominant legal basis for the processing of personal data in the energy services sector is the contract to which the data subject is a party. The subject of the contract also defines the purpose of personal data processing. In the energy sector, it is not possible to use energy without clearly defining the rules of access to it (of course, assuming that the use of energy is legal). For this reason, each entity of the energy sector concluding an energy transmission contract with a consumer has a clear legal basis for the processing of personal data.

However, it should be remembered that the subject of the contract defined as, for example, "enabling the distribution of energy" does not entitle the personal data controller to use the data provided in the contract, e.g., for marketing purposes or to automatically enter them into mobile applications. Such actions require a separate legal basis. Signing an energy distribution contract cannot be treated as consenting to receive commercial information, a newsletter, or the obligation to use the mobile application. Each processing of personal data resulting from or related to the use of online platform facilitating ongoing control of expenses or related to marketing and promotional activities requires the consent of the consumer of the energy services market. This consent should be expressed by means of an unambiguous, confirmatory action,

which expresses the voluntary, informed, and unambiguous consent of the data subject to the processing of personal data concerning the data subject for the purposes of that specific situation and take the form of a written (including electronic) or oral statement. If the data subject is to give consent in response to an electronic inquiry, the inquiry must be clear, concise, and not unnecessarily disruptive to the use of the service to which it relates. An exception to the need to obtain consent may be a situation where we are dealing with the monitoring of energy consumption in connection with the installation of a remote reading meter. It seems necessary to determine that in this case the dominant basis will be the fulfillment of the legal obligation imposed on the controller.

The principle of minimalism and the purpose and time of personal data processing

The basic obligation of entities in the energy services sector is to correctly define the purpose of data processing and the time of their storage. This means that the controller should not process more personal data than it is necessary for a specific purpose. The concept of adequate data is not synonymous with the concept of their necessity. When concluding an energy distribution contract, information about the number and age of the consumer's children can be obtained. This information is not necessary to conclude an energy distribution contract, but it is adequate for the purpose for which it is collected. It can be assumed that a client who has children in early school age will consume less energy than a client with children in their teenage years who play computer games every day. However, the Polish translation of the GDPR says that the data must be e.g., limited to what is necessary in relation to the purposes for which they are processed. The purpose will be different in the case of performance of the transmission contract, and different in the case of using the mobile application or newsletter by the consumer. Each time, the controller is obliged to specify this purpose and adapt the process of data processing actually necessary to its implementation. For example, in the case of performance of a transmission contract, the scope of data processed will certainly include identification and contact details (such as, for example,

name, surname, date of birth, tax identification number, postal address, e-mail address, telephone number, place of residence, cadastral data, permit for construction), but also data on energy consumption and environmental data as well as bank data. In turn, in the case of processing data related to the use of a mobile application, home automation or newsletter service, the scope of processed data may be extended. It may include, for example, information collected from devices installed at the customer's premises, such as: room temperature, brightness, peak power, humidity, total electricity consumption, total heat consumption, motion alarms, on the basis of which it is possible to determine information identifying a given natural person.

It is important that the data from smart meters are not used in a way that could lead to the conclusion that they are processed in violation of the law. In particular, the exact purposes for the processing of personal data should be clear, legitimate, and specified at the time of collection. The purpose of processing the data of a customer of the energy services market is most often related to the functioning of a given website and services. By specifying this goal in detail, it is possible to isolate tasks related to the need to ensure the smooth functioning of the website, explain the circumstances of unauthorized use of the website, as well as create internal reports and analyzes (including statistics on the views of subpages of a given website), improve the quality of services provided, and possibly – send the service recipient a newsletter to the indicated e-mail address. While the purposes resulting from the provision of transmission services are clear and unambiguous, in the case of marketing and information activities, it is necessary to have separate consents to document a valid basis for data processing. It is worth emphasizing that the purpose of processing personal data by entities guaranteeing the supply of energy is primarily the performance of the contract for the supply of energy. In this regard, the purpose of processing, depending on the stage at which the collection and further processing of data takes place, may be both preliminary activities (such as those related to connection, switching, commissioning and termination of energy supply) and directly related to the implementation of an already concluded contract (e.g., consideration of any requests for information, complaints). The secondary goal is to ensure energy efficiency and other actions related to this, such as intervention in the furnace or central

heating installation, installation of photovoltaic panels, insulation, handling of all information requests, consideration, and handling of complaints, etc. In turn, in the case of data processed in connection with the installation of smart meters, the purpose of processing may be the performance of a contract for the supply and possible installation of devices at the user's premises, including home automation, as well as processing and sending reports on energy consumption and environmental data.

Almost every controller processes personal data also in order to pursue legitimate interests, as well as to fulfill the legal obligation incumbent on the controller.

Information obligation

When collecting data, the so-called information obligation must be met, i.e., it is necessary to inform the persons whose data are collected about who will process them and for what purpose, what rights those persons have, to whom the data will or may be made available, etc. It is particularly important to precisely define the purpose of data processing at the beginning, because its change during the processing may sometimes turn out to be impossible, which results from the content of Article 5(1)(b) of the GDPR, which specifies that personal data is collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The purpose of the information obligation is to draw the attention of the person whose data are processed to the entire process related to the specific use of this personal data. Organizing this area of personal data processing is an extremely important element of a properly implemented policy of secure personal data processing. Although it seems that the implementation of this obligation does not contribute anything to the everyday functioning of the consumers, in fact it gives them the opportunity to control the areas in which their personal data are processed. Importantly, a large part of the administrative fines imposed in Europe relates to non-performance or partial implementation of this obligation, which will be the subject of the further part of the study. The installation of remote reading meters is associated with increased fulfillment of information obligations towards consumers. The operator of the electricity

distribution system provides the final customer with information about the meter during or before the installation of the remote reading meter, including, inter alia, information about the processing of personal data of this recipient (Act of 10 April 1997 – the Energy Law Act (uniform text, Journal of Laws of 2021, item 716).

Application of appropriate security measures

When discussing security measures, the focus is naturally on the security of smart meters. However, it should not be forgotten that this issue relates to the processed personal data as a whole and the way of organizing work and the area in which personal data is processed in order to minimize the risk of personal data breach. Nowadays, it is inevitable to keep records with the use of electronic data carriers, ICT systems or applications. In order to ensure proper security of the above tools and protection of personal data, three types of organizational security measures may be implemented.

Firstly, in terms of physical threats, the buildings where the headquarters of entities from the energy services sector are located should be protected by an alarm system, and the rooms where personal data processing takes place must be adequately protected. Moreover, the rooms in which data are processed should not be accessible directly, and during the absence in the room, it should be locked in the presence of third parties. Computer printouts with personal data must be stored in closed rooms. In turn, in the case of installing computer network systems, network cabling should be laid in protective covers so that the section connecting the computers is as short as possible.

Secondly, in terms of threats resulting from access to data by unauthorized persons, it is worth introducing solutions according to which only authorized employees and members of the personal data controller may be allowed to operate the IT systems in which personal data is processed. Access authorization systems must be used in all IT systems where personal data are processed, and computer printouts or information carriers containing personal data which are intended for liquidation must be destroyed.

Thirdly, in terms of threats resulting from the actions of users, all persons authorized to process personal data should be obliged to keep the processed

data secret, also after the authorization expires. In addition, all persons authorized to process personal data must be trained in the provisions on the protection of personal data, and individual access rights to personal data must be established for individual persons authorized to process personal data, if technically and organizationally possible. One of the important safeguards is also the prohibition of copying databases or printouts from databases for purposes other than archiving and/or transferring data to an authorized entity.

At the same time, it should be remembered that smart meters must be secured with solutions that minimize the risk of cyber-attacks. These products cannot be exposed to any manipulation, which means that data exchange should be encrypted and go directly through the electricity and telephone network, avoiding the vulnerabilities of the Internet. Hardware resistance to potential tampering should be associated with the ability to generate private encryption keys for use in transferring data (Desarn-Luksaud, 2017, p. 32). Importantly, these entities must also ensure that appropriate safeguards are implemented to minimize the risk of third parties gaining access to data. There is no doubt that consumer data can be processed for clearly defined purposes and in accordance with applicable data protection laws. The use of smart metering can lead to the tracking of persons' daily lives in their homes and buildings. For this reason, an important obligation of entities processing personal data is the need to inform the person whose data are processed about this fact. This information should be broad and include all information related to the processing of personal data. The energy services sector is threatened by digital security issues ranging from cybersecurity of energy systems (Sun, Hahn, Liu, 2018, p. 45) to privacy in smart systems (Véliz, Grunewald, 2018, p. 702) and ultimately geostrategic competition in the field of energy technologies (Goldthau, 2019, p. 29) that have infiltrated the public and private domains both at home and abroad.

Implementation of appropriate technical solutions minimizes the risk not only of unauthorized use of personal data, but also of access to them by unauthorized persons, and consequently – reduces the risk of imposing an administrative fine. The analysis of administrative decisions leads to the conclusion that the contemporary consumer model is characterized by high legal awareness. In many cases, the fines imposed resulted from a complaint filed

by an individual entity, not a group of persons seeking to determine whether a personal data breach had occurred. For this reason, vigilance of entities from the energy services sector should be particularly maintained.

Innovative technological solutions and technical safety in the policy of sustainable development

One of the major challenges faced by energy sector enterprises is the implementation of innovative technological solutions that will not increase the risk of unauthorized disclosure or leakage of processed personal data. Currently, a trend related to the climate policy of the EU countries can be observed, the aim of which is to replace 80% of electricity meters with smart meters. This requirement stems directly from the EU Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, imposing an obligation for each Member State to replace 80% of traditional electricity meters with smart meters by 2020. From the point of view of metering data protection, this is an extremely beneficial solution that can affect electricity costs, as well as time optimization due to the fact that they enable remote reading and analysis of energy consumption. Their introduction involves the implementation of not only technical, but also access facilitations. The reason for this is that the recipients with access to the Internet can check how much energy they have used so far at any time. In the situation of introducing such facilitations, the issue of protecting the collected data and ensuring their privacy is often forgotten. Focusing on savings caused by the fact that billing is based on actual energy consumption may negatively affect the need for parallel implementation of technological solutions ensuring the security of data processed in the network. The implementation of energy-saving solutions in the industry, services and households is a response to the development and improvement of technology.

The policy of ensuring security requires continuous improvement of technologies for detecting and forecasting the development of threats,

ICT information processing, protection and counteracting threats and liquidation of their effects (Zborowski, 2010, p. 19). Environmental protection and sustainable development policy must be implemented in parallel with the policy of safe processing of personal data. This position was also confirmed by forecasts and strategic documents, in which key areas for technical security issues in the years 2015-2020 were indicated (FuTMaN), such as: teleprevention, teleservice, monitoring of products and materials, smart identifiers and access cards, personal data protection, preventing the possibility of a serious industrial accident, minimizing the effects of a major accident in relation to people, the environment and material values, designing technologies, machines and devices in a way that ensures their safe use, automation of management in the event of crisis threats. It seems that ensuring sustainable development in the field of personal data protection (Zborowski, 2010, p. 22) requires improving the effectiveness of limiting the risk of unauthorized access or unlawful sharing and disclosure of personal data by coordinating activities in the effective implementation of new technologies and applying the best practices in the field of technical and organizational solutions focused on prevention.

Both smart grids and smart meters are devices that help both consumers and suppliers to adjust their energy consumption by providing real-time information on energy consumption and automatically turning certain devices on and off to optimize grid load. Smart meters have two key functions. On the one hand, smart meters can empower consumers by providing information on their energy consumption and/or generation, allowing them to adjust their consumption patterns and participate in demand response programmes and other services so that their energy costs can be reduced. On the other hand, smart meters are also a means for Distribution System Operators (DSOs) to keep track of energy demand and the functioning of their networks so that they can fine-tune their system operation to lower operation and maintenance costs (Lavrijssen, Espinosa Apráez, Caten, 2022, p. 1088). Although technical solutions are extremely attractive, it is necessary to remember about the risks related to the privacy of persons whose data would be collected. The collection of information on electricity consumption in each household may involve the collection of data about an identifiable natural person, and consequently – the collection of personal data. "Smart metering systems" and their spread across

Europe increases the amount of collected and processed personal data. The concept of security plays an important role in the strategy of sustainable development. It is regarded as a key factor for business success and is an integral part of technical activities. Technical safety has a progressive and measurable impact on reducing not only the number of accidents at work, road accidents, occupational diseases, environmental disasters and incidents, and losses related to accidents, but may also involve minimizing the situations justifying the imposition of various administrative fines (e.g., due to breach of security of personal data processing).

With the increasing digitization of the energy sector, it faces an increasing number of threats that require a careful cybersecurity risk assessment in order to take appropriate countermeasures. Social and technological innovations play an important role in achieving the energy transition (Hoppe, de Vries, 2019, p. 141). This is due to the fact that the existing solutions used in older systems were designed at a time when cyber security was not taken into account by entities processing personal data both in the energy sector and in other areas. In terms of technical security in the area of personal data protection, the need to use various types of tools can be distinguished. These are: a) technical systems supporting the security of personal data and processing processes, b) systems for monitoring and diagnosing data processing procedures, and c) systems increasing the security of processed personal data. Currently, there is a need to define new approaches to security in the field of detecting and preventing threats and building protection of personal data against cyber-attacks.

Administrative fines imposed in the energy sector in Europe

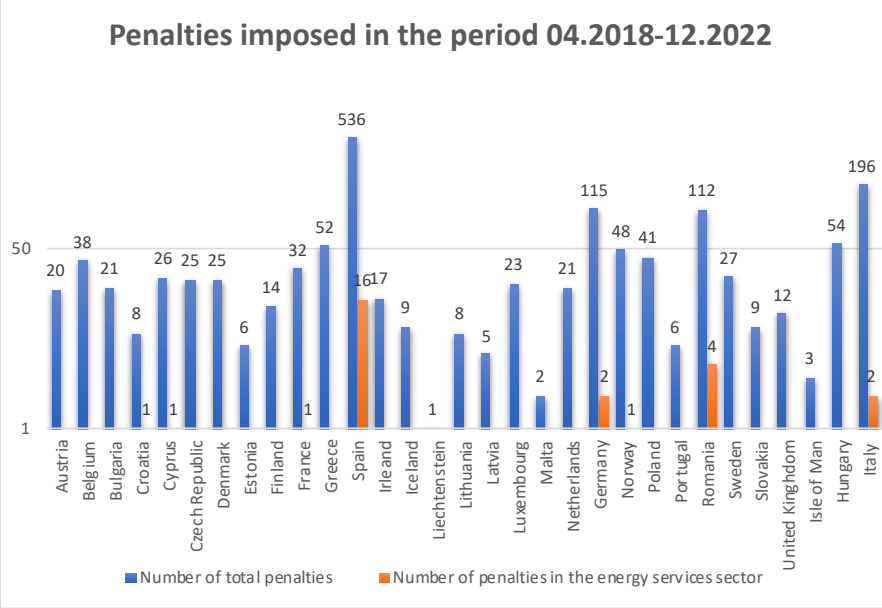
In order to increase the degree of enforcement of the provisions of the Regulation, the EU legislator introduced the possibility of imposing administrative fines on entities obliged to comply with the provisions of the EU Regulation. At the same time, it was stressed that in most countries the institution of an administrative fine is known. In those countries where such an

institution is not known (e.g. Denmark and Estonia), such penalties are replaced by a fine with an effect equivalent to an administrative fine. An administrative fine should be equated with the monetary sanctions specified in the law. They are imposed by a public administration body, by decision, following a violation of the law involving either a failure to fulfill an obligation or a violation of a prohibition incumbent on a specific entity. These fines may be imposed in addition to or instead of the relevant measures imposed by the Regulation by the national supervisory authority. Moreover, if the infringement is minor or if the imminent fine would impose a disproportionate burden on a natural person, a warning may be issued instead. However, supervisory authorities should pay due regard to the nature, gravity, and duration of the infringement, the intentional or negligent character of the infringement, the actions taken to mitigate the damage, the degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures imposed on the controller or processor, adherence to approved codes of conduct, and any other aggravating or mitigating factors.

Article 83 of the GDPR provides for three types of fines (and two ceilings). Two types of fines, i.e., higher and lower, are independent, and their maximum amount depends on the type of violation found by the authority. The third type, on the other hand, is successive to the legal measure already applied by the authority in the form of corrective powers specified in Article 58(2) of the GDPR (Litwiński, 2021, p. 545 et seq). A dependent fine is imposed in the event of non-compliance with the orders under Article 58(2) of the GDPR. It amounts to a maximum of EUR 20,000,000, and in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Independent fines are fines, the imposition of which is determined by the findings of the supervisory authority that the infringement took place. The independent lower fine is up to a maximum of EUR 10,000,000, and in the case of an undertaking – up to 2% of the total worldwide annual turnover of the preceding financial year. Secondly, the independent higher fine, which is up to a maximum of EUR 20,000,000, and in the case of an undertaking – up to 4% of the total worldwide annual turnover of the preceding financial year. In both cases, the higher of these

amounts applies. Clarification of the rules for determining the amount of fines in individual European countries is left to national legislators to decide.

In Poland, the funds from the administrative fine are income to the state budget. They do not contribute to the Office for Personal Data Protection itself. Thus, the Polish legislator ultimately decided to make the proceeds from these fines entirely state budget income, even though at the stage of drafting the national law, it was considered that 1% of the funds from these fines should be allocated to the activities of a new special purpose fund (the Personal Data Protection Fund) (Łuczak, 2018, p. 1059; Antonów, 2020, p. 33). The maximum penalties set by the GDPR reach maximum limits incomparable to any other administrative penalties imposed so far in Poland.



The analysis of administrative fines imposed in the European Union and other European countries for the purposes of this study is based on the analysis of information collected on the website http://safelog.pl, including information on fines imposed from 12 April 2018 till 3 December 2022. The list also includes information on decisions imposing fines without indicating their dates. The analysis covered 1,480 fines imposed in the indicated

period, of which only 28 fines were imposed on entities from the energy services sector, which is only 1.89%. In my opinion, this is because entities in the energy sector are consciously implementing the process of digitization of services, with full respect for the personal data of the recipients of the services they provide.

The penalties that have been imposed on entities in the energy sector concern several basic areas. First – they concern the principles of personal data processing and the legal basis for processing, i.e. Article 5 and Article 9 of the RODO. The combination of both bases for the financial penalty is justified, as one of the key principles of data processing is to act in accordance with legal regulations. On the other hand, processing data without a legal basis or with an erroneously designated legal basis is incompatible with legal regulations. Therefore, combining the two bases is most reasonable. The Spanish Data Protection Authority (esp. Agencia Española de Protección de Datos) found the largest number of violations in this area. The violations included the transmission of an electricity bill containing personal data such as the name, address and bank account of another customer (penalty of €24,000) (Procedimiento Nº: PS/00102/2020), whether an error in changing the applicant's personal data resulting in its deletion and the entry of a third party's data, which resulted in a breach of confidentiality (penalty of 60,000 euros). In another case, there was a change of electricity supplier without the consent of the data subject (penalty of €50,000) (Procedimiento Nº: PS/00232/2020). Norway's data protection authority (nor. Datatilsynet) imposed a fine of €14,900 for camera-based surveillance, which resulted from the installation of a 24/7 webcam on the roof of an office building with the ability to view the recordings via a live video stream on Youtube and the administrator's homepage. This penalty did not directly relate to a violation through unauthorized disclosure of data, but was related to creating the possibility of identifying what kind of car the respondents were driving, what kind of clothes they were wearing, what color hair they had and other personal characteristics. It became possible for those watching the live broadcast to identify and follow co-workers, colleagues, friends, family or other acquaintances. In this case, the violation affected not service recipients, but de facto employees due to the fact that the illegal camera surveillance involved a significant number of employees and that many of them were monitored

repeatedly, some daily. Live broadcasting was considered a violation. The highest fine imposed for violations of data processing rules and the basis for processing was imposed in Italy by the data protection authority there (it. Garante per la protezione dei dati personali) – €3,000,000. This was related to the unlawful processing of personal data in the context of advertising activities and the conclusion of unsolicited contracts for the supply of electricity and gas in a market economy. As indicated in the decision, many people only found out about the conclusion of a new contract after receiving a letter terminating the contract with the previous supplier or the first invoices (Provvedimento correttivo e sanzionatorio nei confronti di Eni Gas e luce S.p.A).

Not all fines were related to violations of the rules on the processing of personal data of consumers in the energy services market. A fine of €40,000.00 imposed by the Cyprus Supervisory Authority (Grafeío Epitrópou Dedoménon Prosopikoú Charaktíra) related to the use of an automated system based on the so-called Brad-Factor to manage, monitor and control employee sickness absence using a tool-based assessment. The regulator found that such an evaluation mechanism was not covered by Cypriot labor law and was therefore used illegally. Another group of violations is related to the need to implement the information obligation and the rights of data subjects. The Spanish authority imposed a fine of €1,500,000.00 for failing to implement the information obligation of data subjects whose data was being processed (Procedimiento Nº: PS/00236/2020). In the European arena, there has been a tendency to impose high fines for failing to comply with information obligations. A French authority (fr.: Commission Nationale de l'Informatique et des Libertés) imposed a fine of €1,000,000.00 for failing to provide during a telephone contact conducted for advertising purposes the information that is within the scope of this obligation, also failed to respect people's objections to the processing of their personal data for marketing purposes, and even failed to respond to data subjects' requests in a timely manner (Délibération SAN-2022-011). The Croatian authority (cr. Agencija za zaštitu osobnih podataka) imposed a fine of €124,245 on the fuel distribution entity. In this case, the consumer was denied access to the surveillance footage, arguing that there was no written request, and no legitimate purpose. Failure to secure the recordings resulted in the fact

that after a certain period of time (in this case – 7 days) the recording was erased, which had a decidedly negative evidentiary impact on the further course of the proceedings. On the other hand, in terms of violations of security procedures or their non-application in the European arena, decisions are discernible that were based on a finding of failure to take adequate technical and organizational measures to protect personal data. In the case of Romania, in a fairly short period of time (i.e., on March 25, 2020, June 18, 2020 and August 22, 2022), three decisions were issued stating that appropriate technical and organizational measures were not implemented to ensure an adequate level of information security. The most shocking penalty in terms of amount is that imposed by the Italian regulator in December 2021 in the amount of 26,500,00.00 euros. The amount of the fine was based on numerous data breach reports to the authority. After receiving hundreds of reports and complaints from users, the DPA found that the data controller illegally processed the personal data of millions of users for telemarketing purposes. Among other things, the DPA found that data subjects received unsolicited promotional phone calls (Ordinanza ingiunzione nei confronti di Enel Energia S.p.a.).

It is indisputable that the activities of the entities on which the administrative fine was imposed were related to the processing of personal data. Entities in the energy sector are energy supply companies, thus having numerous customers with whom contracts are signed. This means that these entities process personal data on a large scale. The precision with which they should process personal data is special. Therefore, each of the penalties imposed, in addition to their penalizing dimension, have a repressive and preventive character. Due to the large-scale processing of data, these entities are obliged to process the personal data of their contractors with special care. The Polish model of qualifying fines as state budget income can serve as a model for those countries where dues resulting from imposed fines feed into the budget of the supervisory authority. The placement of administrative fines for violations of personal data protection in the category of public funds determines the processes related to their collection, management (Antonów, 2020, pp. 31-50).

Conclusions

Energy companies increasingly rely on data processing technologies using modern technological solutions. The modern standard is the processing of personal data in the cloud in order to store large amounts of data. Storing all the data collected through new information and communication technologies (such as smart meters) in their own data centers becomes very problematic for enterprises. The popularization of issues regarding the security of personal data affects not only the awareness, but also the implementation of solutions that minimize the possibility of acting inconsistently with the currently applicable regulations. It seems that the energy sector and the entities operating in it are aware of these restrictions. This is evidenced by the analysis of administrative fines imposed on entities operating on the energy services market. The percentage ratio of fines imposed on energy distribution entities to the total number of fines is very low. Perhaps the reason for this state of affairs is greater technological and, consequently, legal awareness related to the need to implement tools and solutions that take into account the need not only to minimize cyber risks, but also to create functionalities that ensure the security of processed data.

References

Antonów, D. (2020). „Administracyjne kary pieniężne za naruszenia ochrony danych osobowych". Prawo Budżetowe Państwa i Samorządu, vol. 8. https://doi.org/10.12775/PBPS.2020.016, Google Scholar: https://apcz.umk.pl/PBPS/article/view/PBPS.2020.016

Barichella, A. (2019). "The US-EU Rivalry for Data Protection: Energy Sector Implications", Édito Énergie, Ifri, 19 February 2019, Google Scholar: https://sciencespo.hal.science/hal-02066832/

Barta, J., Fajgielsk, P., Markiewicz, R. (2004). Ochrona danych osobowych. Komentarz, Cracow, Google Scholar: https://books.google.com/books?hl=pl&lr=&id=n2NSAwAAQBAJ&oi=fnd&pg=PA5&dq=J.+.+Barta,+P.+Fajgielski,+R.+Markiewicz,+Ochrona+danych+osobowych.+Komentarz,+Cracow+&ots=Wq8SvQGAcr&sig=SOlE_CzpwNniRHTTOyFcYdstsDQ

Dammann, U., Simitis, S. (1999). EG-Datenschutzrichtlinie, Cologne, Google Scholar: https://doc1.bibliothek.li/aaw/FLM9111606.pdf

Desarn-Luksaud, G. (2017). "Cyber Attacks and Energy Infrastructures: Anticipating Risks", Études de l'Ifri, Ifri, January, p. 32, https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf (accessed on 26 December 2022).

Drozd, A. (2007). Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warsaw.

Eriksson, J., Giacomello, G. (2007). International Relations and Security in the Digital Age, Routledge, Google Scholar: https://scholar.google.com/scholar?oi=bibs&cluster=10730905561722326458&btnI=1&hl=pl

Goldthau, A., Westphal, K., Bazilian, M., Bradshaw, M. (2019). "Model and Manage the Changing Geopolitics of Energy", Nature, vol. 569, no. 7754, Google Scholar: https://www.nature.com/articles/d41586-019-01312-5

Hoppe, T., de Vries G. (2019). "Social innovation and the energy transition", Sustainability, vol. 11, No. 141, https://www.mdpi.com/2071-1050/11/1/141

Huhta, K. (2020). "Smartening up while keeping safe? Advances in smart metering and data protection under EU law", Journal of Energy & Natural Resources Law, vol. 38, https://doi.org/10.1080/02646811.2019.1622244, Google Scholar: https://www.tandfonline.com/doi/abs/10.1080/02646811.2019.1622244

Knyrim, R., Trieb G. (2011). "Smart metering under EU data protection law", International Data Privacy Law, vol. 1, https://doi.org/10.1093/idpl/ipr004, Google Scholar: https://academic.oup.com/idpl/article-abstract/1/2/121/664439

Lavrijssen, S., Espinosa Apráez, B., ten Caten, T. (2022). "The Legal Complexities of Processing and Protecting Personal Data in the Electricity Sector", Energies,

vol. 15, No. 1088, https://doi.org/10.3390/ en15031088, Google Scholar: https://www.mdpi.com/1480212

Litwiński, P. (ed.) (2021). Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, Warsaw, Google Scholar: https://ruj.uj.edu.pl/xmlui/handle/item/271804

Łuczak, J. (2018). [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa, s. 1059; Google Scholar: https://research-portal.vub.be/en/publications/gdpr-general-data-protection-regulation-commentary

Mednis, A. (2020). Ochrona danych osobowych w systemie ochrony zdrowia. Zasady prowadzenia, udostępniania i archiwizowania dokumentacji medycznej [in:] Organizacja systemu ochrony zdrowia. System Prawa Medycznego. Vol. 3, D. Bach-Golecka, R. Stankiewicz (eds.), Warsaw.

Rajavuori, M., Huhta, K. (2020). Digitalization of security in the energy sector: evolution of EU law and policy, The Journal of World Energy Law & Business, Volume 13, Issue 4, August, https://doi.org/10.1093/jwelb/jwaa030, Google Scholar: https://academic.oup.com/jwelb/article-abstract/13/4/353/5983698

Sakowska-Baryła, M. (ed.) (2018). Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warsaw.

Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons; Google Scholar: https://books.google.com/books?hl=pl&lr=&id=OT6kBgAAQBAJ&oi=fnd&pg=PR9&dq=18.%09B.+Schneier,+Secrets+and+Lies:+Digital+Security+in+a+Networked+World&ots=N5y-WRDi06F&sig=1N7Jr2JsrNRp4HzObUkmNuUzYpI

Sibiga, G. (2003). Postępowanie w sprawach ochrony danych osobowych, Warsaw, Google Scholar: https://bibliotekanauki.pl/articles/620414.pdf

Sun, CC., Hahn, A., Liu, CC. (2018). "Cyber Security of a Power Grid: State-of-the-Art", International Journal of Electrical Power and Energy Systems, vol. 45, https://doi.org/10.1016/j.ijepes.2017.12.020, Google Scholar: https://www.sciencedirect.com/science/article/pii/S0142061517328946

Tonyali ,S., Akkaya, K., Saputro, N., Selcuk ,Uluagac, A., Nojoumian, M. (2018). "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems", Future Generation Computer Systems, Volume 78, Part 2, https://doi.org/10.1016/j.future.2017.04.031

Véliz, C., Grunewald, P., (2018). "Protecting Data Privacy Is Key to a Smart Energy Future", Nature Energy, vol. 702, https://doi.org/10.1038/s41560-018-0203-3, Google Scholar: https://www.sciencedirect.com/science/article/pii/S0167739X17306945

Zborowski, A. (2010). Systemy bezpieczeństwa technicznego w polityce zrównoważonego rozwoju, „Bezpieczeństwo i Technika Pożarnicza", No. 3, Google Scholar: https://bibliotekanauki.pl/articles/372790.pdf

Legal Acts and Netography

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0072&from=EN (accessed on 19 December 2022).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter as: GDPR.

Act of 10 April 1997 – the Energy Law Act (uniform text, Journal of Laws of 2021, item 716.

EDPS TechDispatch 02/2019 on Smart Meters in Smart Homes, https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en (accessed on 26 December 2022).

FuTMaN. The Future of Manufacturing in Europe 2015-2020. The Challenge for Sustainability, Final Report. March 2003; Activity Report 2008. Submitted to the EC for the Annual Reporting. September 2008. http://www.industrialsafety-tp.org/filedown.aspx?file=1223; The Future of Manufacturing in Europe 2015-2020 The Challenge for Sustainability. March 2003. Institute for Prospective Technological Studies. ftp://ftp.jrc.es/pub/EURdoc/eur20705en.pdf.

Second Status Report on European Technology Platforms, Moving to Implementation, Report compiled by a Commission Inter-Service Group on European Technology Platforms. May 2006. ftp://ftp.cordis.europa.eu/pub/technologyplatforms/docs/ki7305429ecd.pdf.

Decyzja rumuńskiego organu nadzoru (rom. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal), skutkująca nałożeniem kary w wysokości 4.000 euro, https://www.dataprotection.ro/index.jsp?page=Amenda_pentru%20incalcarea_RGPD_Enel_iunie2020&lang=ro

Délibération SAN-2022-011 du 23 juin 2022, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045975295?init=true&page=1&query=San-2022-011&searchField=ALL&tab_selection=all

Ordinanza ingiunzione nei confronti di Enel Energia S.p.a. – 16 dicembre 2021 [9735672], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9735672

Procedimiento Nº: PS/00102/2020 , https://www.aepd.es/es/documento/ps-00102-2020.pdf (dostęp w dniu 30.01.2023 r.)

Procedimiento Nº: PS/00232/2020, https://www.aepd.es/es/documento/ps-00232-2020.pdf (dostęp w dniu 30.01.2023 r.)

Provvedimento correttivo e sanzionatorio nei confronti di Eni Gas e luce S.p.A. – 11 dicembre 2019 [9244358], https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244358 (dostęp w dniu 30.01.2023 r.)
Procedimiento Nº: PS/00236/2020, https://www.aepd.es/es/documento/ps-00236-2020.pdf