Adrian Szutkiewicz

System of Sanctions in Regulation 2016

Roczniki Administracji i Prawa 17/1, 215-231

2017

Annuals of the Administration and Law no. 17 (1), p. 215-231

Review article

Received: **25.03.2017**
Accepted: **05.05.2017**
Published: **30.06.2017**

Source of funding: **author's own resources**

Authors' Contribution:
(A) Study Design
(B) Data Collection
(C) Statistical Analysis
(D) **Data Interpretation**
(E) **Manuscript Preparation**
(F) Literature Search

Adrian Szutkiewicz*

SYSTEM OF SANCTIONS IN REGULATION 2016/679- GENERAL OBSERVATIONS AND REMARKS REGARDING EMPLOYMENT

INTRODUCTION

Currently we are living in the world in which information itself became the subject of trade. It is the information that very often decides about the success or failure of an enterprise. The case is not controversial when mentioned information regards entities traditionally not perceived as having a personal and individual interest in protecting the private aspect of everyday life and functioning. Problems arise when the information that is of our interest regards human beings, who very often on a daily basis perform multiple roles- some of them are strictly private and some to a full extent are of a public character.

* M.Sc.; Trainee attorney at the District Chamber of Legal Counsels in Cracow.

Law acting as a postulating factor is supposed to create specific safeguards of this part of our life that is not directly meant to be revealed to the others. The current level of protection of information regarding human beings on the European level was to a huge extent insufficient when it came to performing its suggested role- ensuring that personal aspects of our lives were not processed in a way that was based on a legitimate interest of either person whose personal data is referred to or the society itself which took form of a provisions of law that were to be a basis for the processing of personal data.

It was this insufficiency of protection and anachronism of regulations that was the main factor which motivated the European Legislator to create a completely new piece of legislation- legislation taking into consideration the state of current technological development and way of conducting business, very often reaping benefits from systematic insufficiencies of the whole system of personal data protection applicable throughout the European Union. As a result there was adopted 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 (later referred to as GDPR).

The idea of unification and creating of the uniform standards of personal data protection in the European Union was a reason because of which the instrument of a regulation was chosen as the way of implementing new solutions. By doing so, the Member States of the European Union were given the smallest- if any- amount of place for individual activity in terms of implementing and changing the overall shape of European provisions of personal data protection. GDPR is about to enter into force on May 25, 2018.

The Polish personal data protection regulation is mostly based on the Personal Data Protection Act of August 29, 1997 (Journal of Laws of 1997 No. 133, item 883). The mentioned regulation came into force on April 30, 1998. Almost 20 years that have passed between its adoption and present time resulted in its outdating. That is why an 'update' of the whole system of protection of personal data from the point of view of the Polish legal system will be seen more like a revolution rather than evolution[1].

It is undisputable that employment is one of those legal relationships that accompany most of us through almost all of our adult years. It is safe to say that the labor law, together with the widely understood civil law are those areas of law that regulate our lives. In this article I would like to indicate the third- newly created- area of law that is to play a huge part in our everyday existence directly by giving us specified and precise rights with corresponding with them duties encumbering other entities. Due to the obvious limits of this work I would like to focus on chosen aspects of this part where the labor law meets the regulations regarding the personal

[1] http://tvn24bis.pl/z-kraju,74/maciej-kawecki-z-resortu-cyfryzacji-o-zmianach-w-ochronie-danych,743005.html

data protection with special attention paid to the potential sanctions that threat the entities processing personal data.

ISSUES CONNECTED WITH THE PRACTICAL APPLICABILITY OF DIRECTIVE 95/46/EC.

As it was mentioned before, before the introduction of the GDPR, common rules of processing and protecting of personal data within the European Union were based on the piece of legislation taking the form of a directive (Directive 95/46/EC, later referred to as: the Directive).

According to Article 288 of the Treaty on the Functioning of the European Union: '*a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods*'.

This situation resulted in the fact that all the Member States of the European Union were obliged to implement the provisions of the Directive into their national legal systems with reservation that those 'local solutions' have to be coherent with solutions and safeguards included in the Directive[2]. Thus, it was ensured that in every piece of national legislation implementing provisions of the Directive the minimum level of the personal data protection was always guaranteed.

However, the introduction of any additional regulations regarding the personal data protection by the Member States in the course of the process of implementation resulted in divergences in the system of personal data protection in the European Union. Solely by the way of example there can be mentioned differences in such areas as:

1. Criteria for the processing of personal data in accordance with the provisions of law – they tend to differ from one country to another (some countries have repeated in their national legislations criteria in the same way as the Directive, whereas some tend to specify particular rules of processing of personal data in a more detailed manner[3]),
2. General principles of liability for the violation of the provisions regarding personal data protection, together with the types of potential sanctions that can be applied (including types of damages and their height) were left to be regulated by the national legal systems[4] (chapter III of the Directive). Naturally this resulted in the significant differentiation of the potential severity of punishment. Some coun-

[2] List of national regulations implementing the provisions of the Directive can be found at: http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.html.

[3] D. Korff, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments,* 2010, p. 69, available at: http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_working_paper_2_en.pdf.

[4] Ibidem, p. 94.

tries were recognized as 'more favourable' for conducting activities that were causing a higher potential risk for the violation of the provisions regarding the personal data protection.

3. The status of the Supervisory Authorities tends to differ within the European Union[5]. As Member States were obliged to determine the status and powers of the Supervisory Authorities (Article 28 of the Directive) it is natural that their ability to successfully apply appropriate countermeasures in the case of the violation of the personal data protection is a matter of being explicitly authorized to do so by a particular Member State. This resulted in significant differences in effectiveness of ensuring that the provisions of law regarding the personal data protection are obeyed.

THE SYSTEM OF SANCTIONS IN THE GDPR

Regulation 2016/679 is introducing a completely new system of duties and obligations encumbering entities that process personal data. This whole change of attitude towards the protection of personal data is so different from what was practiced before that it would be naive for the European Legislator to assume that all the entities processing personal data of subjects located within the territory of the European Union would adhere to the new provisions of law only because of its relevance and authority of the body introducing the GDPR. That is why in the provisions of the GDPR there is included a completely new and complex system of sanctions that are to be applied in the case of violation of the provisions of the Regulation.

REGIME OF SEEKING FOR REMEDIES BASED ON THE CIVIL LAW

From the Polish point of view the additional novelty featured in the GDPR is the fact that now a piece of legislation regarding the protection of personal data expressly allows for simultaneous filing of concurrent claims regarding both the protection on the basis of the GDPR and the obtaining of the judicial remedy in the Court in the case of the violation of the provisions of the GDPR that caused infringement of the rights of a person seeking for the compensation.

From the analysis of Article 79 of the GDPR there comes the conclusion that the mentioned parallel claim shall be filed at a competent court and be reviewed on the basis of the provisions of the civil- not administrative- procedure with all its consequences, including the type of potential remedies that can be awarded to compensate the suffered damage. However, the GDPR is specific when it comes to compensating the suffered damage. According to Article 82 paragraph 1 of the GDPR, in the case of the suffered damage, both material and non-material, the per-

[5] Ibidem, p. 102.

son affected by the actions of the data controller or data processor shall be entitled to receive compensation (monetary) for the whole damage. Any other type of compensation can be pursued on the basis of the provisions of the civil law, e.g. Article 24 of the Civil Code[6].

What has to be mentioned is the fact that in the draft of the new Polish Personal Data Protection Act[7] proposed in its partial form on March 28, 2017 it is determined that it is the Regional Court that will be proper for deciding about the abovementioned cases (article 56 of the Act).

That is why it is justified to say that according to the GDPR, the liability of an entity in the case of the violation of its provision can be divided into the administrative and civil liability, each of them completely independent from the other.

ADMINISTRATIVE REGIME OF SEEKING FOR REMEDIES

As it was mentioned before, in the case of the civil liability possible damage can be compensated in accordance with the provisions of the civil law. However, when it comes to the administrative liability, the sanctions that potentially can be incurred by the 'wrongdoer' in the course of this proceeding are original and distinctive. Generally, they can be divided into 2 groups: **fines** (for the purposes of this article called: monetary sanctions) and **corrective powers** (for the purposes of this article called: nonmonetary sanctions). What has to be explicitly mentioned and underlined is the fact that monetary and nonmonetary sanctions can be imposed simultaneously (article 83 paragraph 2 of the GDPR). The fact of imposing a monetary sanction does not necessary mean that the caused 'wrong' is completely covered by it. The possibility of imposing all of the nonmonetary sanctions described in the GDPR also potentially exists.

Such an approach in the Polish reality is a complete novelty. Previously in the Personal Data Protection Act, the idea of the monetary compensation for the violation of the provisions of the law regulating the processing of personal data was not seen as a proper way of enforcing the desired behaviors of those processing personal data. Instead, Polish authorities took more criminal based approach in enforcing an appropriate level of protection when it came to the duties of data controllers and data processors as sanctions of such a character were (and still are- until May 25, 2018) to be imposed on those violating the provisions of the Personal Data Protection Act.

The mentioned administrative-based sanctions are imposed on the basis of administrative decisions. According to Article 78 of the GDPR, every legally binding decision of the supervisory authority can be subjected to the control of the respective (administrative) court.

[6] Civil Code of April 23, 1964 (Journal of Laws of 1964 No. 16, item 93).
[7] Available at: https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf.

In the draft of the new Polish Personal Data Protection Act of March 28, 2017 it is determined that there will be appointed a new administrative authority responsible for handling the proceedings regarding the violation of the provisions of the law regarding the personal data protection- President of the Personal Data Protection Office (Article 15 paragraph 1 of the Act). Also the abovementioned proceedings are projected to be only one-instance (article 15 paragraph 2 of the Act).

AUTHORITIES COMPETENT TO CONDUCT THE PROCEEDINGS

When it comes to establishing the appropriate administrative authority that is to issue the abovementioned decisions, article 4 paragraph 22 of the GDPR determines that:

'The supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

- *the controller or processor is established on the territory of the Member State of that supervisory authority;*
- *data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or a complaint has been lodged with that supervisory authority.*

The mentioned principle regarding the competent jurisdiction of a respective supervisory authority is subject to change in the case of the processing of personal data having a cross-border character, understood as (article 4 paragraph 23 of GDPR):

- *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
- *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect the data subjects in more than one Member State.*

In the case of the presence of the abovementioned circumstances, more than one of the supervisory authorities appointed in every Member State of the European Union normally would be seen as competent for issuing the decision imposing the sanctions. That is why in article 56 paragraph 1 of the GDPR there was introduced the institution of a lead supervisory authority understood as the *supervisory authority of the main establishment or of the single establishment of the controller or processor* and which *shall be competent to act as the lead supervisory authority for the cross-border processing carried out by that controller or processor.*

What can be troublesome in practice is the fact that the prerequisites of activating and determining the competence of the lead supervisory authority are based on imprecise terms, such as the substantial affect that can cause deeming processing personal data as having cross-border character or the main establishment of the controller or processor, according to which the respective national supervisory au-

thority shall be appointed as a lead supervisory authority.

In the case of determining the place of the main establishment of the controller or processor, helpful guidelines can be found in Article 4 paragraph 16 of the GDPR, according to which the 'main establishment' means:

- *As regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;*
- *As regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.*

When it comes to the examination whether the processing of personal data can be of a 'substantial impact', according to document no. 244 of Article 29 of the Data Protection Working Group[8] every single time the following should be taken into consideration e.g.:

- *Possibility or likeliness to cause damage, loss or distress to individuals;*
- *Likeliness to have an actual effect on individuals in terms of limiting the rights or denying an opportunity;*
- *Possibility or likeliness to affect individuals' health, well-being or peace of mind;*
- *Leaving individuals open to discrimination or unfair treatment;*
- *Creating embarrassment or other negative outcomes, including reputational damage; or*
- *Involving the processing of a wide range of personal data.*

NONMONETARY SANCTIONS FOR THE VIOLATION OF THE GDPR PROVISIONS

The nonmonetary sanctions are listed in article 58 paragraph 2 of the GDPR. They include powers of the respective supervisory (or leading supervisory) authority to:

- *issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of this Regulation;*
- *issue reprimands to a controller or a processor where the processing operations have infringed the provisions of this Regulation;*
- *order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;*

[8] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

- *order the controller or processor to bring the processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*
- *order the controller to communicate a personal data breach to the data subject;*
- *impose a temporary or definitive limitation including a ban on processing;*
- *order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed*
- *withdraw a certification or to order the certification authority to withdraw the issued certification, or to order the certification authority not to issue the certification if the requirements for the certification are not or are no longer met;*
- *impose an administrative fine, in addition to, or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case;*
- *order the suspension of data flows to a recipient in a third country or to an international organization.*

MONETARY SANCTIONS FOR THE VIOLATION OF THE GDPR PROVISIONS

The monetary sanctions are regulated by article 83 of the GDPR. The regulation itself provides that the violation of its provisions can be qualified as punishable by an administrative fine amounting:

- *up to 10 000 000 EUR, or in the case of an enterprise, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, or*
- *up to 20 000 000 EUR, or in the case of an enterprise, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.*

The qualification for the first or second type of sanctions directly depends on the kind of the provisions of the GDPR that were violated by the infringer.

Thus, e.g. the following violations (article 83 paragraph 4 of GDPR) are punishable by the "lower" fine:

- duty to cooperate with the supervisory authority;
- lack of the notification of infringement of the personal data protection to the supervisory authority;
- lack of the notification of infringement of the personal data protection to the person concerned;
- the processing of the data without the authorization of the data controller or data processor;
- precluding or impeding the data protection officer from performing his duties.

The following are seen as more detrimental and as such punishable by harsher sanctions e.g. (article 83 paragraph 5 of GDPR):

- violation of basic principles of the processing of personal data;
- processing of personal data without consent of the concerned person;
- improper form of obtaining consent to process personal data or creating obstructions in withdrawing consent;
- violation of the rights to correct the processed personal data;
- violation of the rights to delete the processed data;
- violation of the rights to restrict the processed data;
- violation of the rights to transmit or obtain the processed data in an appropriate form
- violation of the provisions of the GDPR in terms of the processing of personal data in the context of employment.

Additionally, the non-compliance with an order of the supervisory authority imposing the nonmonetary sanctions shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an enterprise, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (article 83 paragraph 6 of the GDPR).

Article 83 paragraph 3 of the GDPR provides that *in the case of a controller or processor intentionally or negligently infringing several provisions of the GDPR in the course of the same or linked processing operations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*. So if the processor or data controller commits several infringements of the GDPR provisions that are not in the relation to each other, sanctions for them can be imposed independently. It seems the most probable that the upper limit of the overall height of the fine should be designated by the objectives of the sanctions, as discussed below.

When it comes to the monetary sanctions, according to motif 151 and article 83 paragraph 1 of the GDPR, the imposed monetary sanctions are to be 'effective, proportionate and dissuasive'.

As for the effectiveness of the sanctions, it is safe to assume that they have to be imposed in such a height that would compensate for all of the 'wrong' that was caused by the violation.

In the case of the proportionality, a similar institution can be found in the doctrine of the criminal law, where the amount of fine (penalty) imposed on the one committing the crime cannot be lower than the social noxiousness of the act and at the same time cannot exceed the amount determined by the guilt of the wrongdoer[9]. Similarly, it would be logical for the authorities imposing fines mentioned in the GDPR to use a similar mechanism in determining the amount of monetary sanctions for the violation of the provisions of the GDPR.

[9] W. Wróbel, A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2013, p. 328, 504-505.

Finally, the dissuasiveness of the sanctions is something that especially at the very initial stage of functioning of the GDPR will cause a lot of troubles both for the authorities imposing the sanctions and the entities subjected to the duty of paying fines. Once again turning to the doctrine of the criminal law the ideas of general and individual prevention[10] are logical to be applied here. From the point of view of the personal data protection, the idea of individual prevention would mean that the sanction imposed on the subject violating the provisions of the GDPR is supposed to be of such a character and height that it would act as a deterring factor for the further violation of provisions regulating the protection of personal data. The sanction imposed at the lower height will be simply seen by the 'wrongdoer' as a mere inconvenience in conducting its business activity. General prevention in the field of sanctions imposed on the basis of the GDPR would mean that other subjects acting in the similar field to the one, in which our 'wrongdoer' acted upon receiving information on the height and character of the sanctions imposed for acts similar to those committed by them will correct their behavior thus starting to act in compliance with the GDPR.

In the course of establishing the height of the monetary sanctions for the violation of the provisions of the GDPR, according to the Regulation itself (article 83 paragraph 2 of the GDPR) the following should be taken into consideration e.g.:

- *the nature, gravity and duration of the infringement taking into account the scope or purpose of the processing concerned as well as the number of data subjects affected and the level of the damage suffered by them;*
- *the intentional or negligent character of the infringement;*
- *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
- *any relevant previous infringements by the controller or processor;*
- *the categories of personal data affected by the infringement;*
- *(…).*

PRINCIPLES OF THE PERSONAL DATA PROCESSING FORESEEN BY THE GDPR

The GDPR in article 5 expressly sets out basic principles, on which every single act of processing of personal data should be based. As a general rule, compliance with those principles should automatically render the mentioned processing consistent with the GDPR and make the processor or data controller safe from any potential sanctions threatening him.

Those principles state that personal data shall be:

- *processed lawfully, fairly and in a transparent manner in relation to the data*

[10] Ibidem, p. 41.

subject ('lawfulness, fairness and transparency');

- *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall (…) not be considered to be incompatible with the initial purposes ('purpose limitation');*
- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');*
- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');*
- *kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (…) subject to the implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').*
- *the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Below I would like to outline the key issues related to chosen principles of the processing of personal data that can have an impact on the whole system of the processing personal data and documents produced and gathered by employers in the course of employment.

PURPOSE LIMITATION

Employers usually obtain the information regarding the employees at the very beginning of employment on the basis of the provisions of article 22^1 of the Labor Code[11]. It is not uncommon that in the course of the employment within the company there are created procedures requiring the input of some of the information about the employees. A frequent practice is that the employers in the mentioned circumstances come into the conclusion that if they already possess the data of this kind, it is correct to use it in whatever manner they want. On the basis of the GDPR

[11] Labor Code of June 26, 1974 (Journal of Laws of 1974 No. 24, item 141).

this practice will be completely unacceptable. The further processing of this data without the provided compliance with the procedure of the proper gathering of it will be seen as a direct violation of the provisions of the GDPR.

STORAGE LIMITATION

This principle shall be applied in a way similar to the previous one. Data processors and data controllers should not keep personal data regarding persons concerned for a period longer than one initially justified by the purpose of gathering of the data. In terms of employment this principle can find its use e.g. for regulating the period of keeping CVs of candidates to work. As soon as the procedure of recruitment for a job they applied for is finished, the CVs containing the personal data should be destroyed or deleted unless there exists another basis for its processing, however the principle of storage limitation still will be fully applicable but this time for the purpose, other than the initial procedure of the recruitment.

DATA MINIMIZATION

It is a common practice, especially in big companies to create and keep documents solely for the internal, business or marketing related purposes. In reality there is possible a scenario, in which the same set of information regarding an employee is kept e.g. in the HR department, sales department and logistics department where as justification there is quoted the fact that such a practice makes functioning of a company easier as departments do not have to send requests to each other to obtain some of the information- it is simply easier for them to keep all the possible information regarding the employee 'just in case'. According to the GDPR this practice will be inadmissible. Relatively long '*vacatio legis*' set for by the GDPR to enter into force was meant exactly for the purpose of making it possible for everyone to provide the compliance of procedures regarding the processing of the personal data with its provisions. This includes a change in the way of operating within the companies in order to introduce such a system that would be both effective in terms of protecting personal data and convenient for the employers and employees when it comes to performing running processes in the company.

INTEGRITY AND CONFIDENTIALITY

Another novelty contained in the GDPR consists of the introduction of the principles named as 'privacy by design' and 'privacy by default'[12] that can be derived from article 23 of the GDPR. In terms of the practical application, the principle of 'privacy by

[12] http://www.eudataprotectionregulation.com/data-protection-design-by-default.

design' means that all the systems and procedures used to process personal data (including that in the course of employment) must be designed in such a way that would ensure the biggest possible safety of the processed data. The level of protection, however, does not have to be absolute. It is obvious that together with development of technology, new ways of obtaining of an illegal access e.g. to IT systems will be created. The mentioned 'privacy by design' has to guarantee that every single time a compromise between the provided safety of the data and practical applicability of the system will be found (e.g. in the hypothetical situation the absolute safety of the data can be guaranteed by restricting the access to it only to one employee, however, such a solution would render day-to-day operations of an enterprise impossible – that is why by design the access to data should be granted only to a verified and finite group of employees who at the same time possess all the necessary tools to ensure the safety of the data).

When it comes to the 'privacy by default'- this rule will find the widest range of applications in the IT systems. Essentially it means that systems and procedures regarding the processing of personal data should be created in such a way that would guarantee safety of the data without the need of any actions or interferences required from the part of persons concerned. Exemptions from the default protection of personal data, consisting of e.g. giving consent to process personal data or sharing some of the information should require positive and expressed actions (for instance sharing of the data included in the employee's timetable maintained in a digital form by default should be impossible, sharing this information with other employees e.g. in order to inform them about business trips should require performing specific actions by the person, whose information is included in the mentioned timetable).

GUIDELINES

One of the advantages that are attributed to the GDPR is that it is seen as an 'intelligent act'[13]. This quality was achieved by creating the provisions of the Regulation in such a way that they do not directly refer to certain and specific technical solutions or manners of handling the procedures of the processing of personal data. In the Polish reality one of the accusations made against the Personal Data Protection Act and the whole system of regulating the protection of personal data in Poland was that it was too specific and concrete. The Regulation of the Ministry of the Interior and Administration of April 29, 2004 on the documentation of the processing of personal data and technical and organizational requirements that should be met by the devices and IT systems used for processing of personal data (Journal of Laws of 2004 No. 100, item1024) is a great example of such an overregulation. In the mentioned regulation there are listed the requirements regarding even the length of

[13] http://gdpr.pl/rodo-iso-wywiad-dr-maciejem-kaweckim-koordynatorem-krajowej-reformy-ochrony-danych-osobowych.

a password used to enter the IT system where the personal data is processed. Such an attitude is impractical in such a way that in the case of change in the state of the technical development, meeting the requirements indicated in the regulation will not necessarily mean that the sufficient level of protection is provided. That is why the GDPR abandoned such an approach. Instead the Regulation outlined the general rules of the processing of personal data that is to be 'completed' by formally not binding recommendations and directions of the proper conduct. Every single time it is the data controller and data processor that have to assess whether their conduct is within the appropriate level of the protection of personal data. A great example of those 'tips' are documents issued by Article 29 Working Group[14], where key issues for personal data protection are explained and subjected to an analysis. Below I would like to quote some of the standpoints from the opinions of Article 29 Working Group that can be useful for the assessment of the correctness of the processing of personal data in the course of employment.

In the opinion 2/2017 on data processing at work adopted on 8 June 2017[15] the Working Group decided to complete and adjust its previous opinion 8/2001 on the processing of personal data in the employment context (WP48)[16], and the 2002 Working Document on the surveillance of electronic communication in the workplace (WP55)[17]. Such a decision was motivated by the significant change in the state of the development of technology, which also had a huge impact on technical measures available to employers to control their employees.

PROCESSING OF THE DATA IN THE COURSE OF RECRUITMENT

When it comes to the practice of using profiles of potential employees in social media as a source of 'input' information used for the process of selecting the best candidates for a job, the Working Group took a clear position that such a behavior is inadmissible. Employers have to clearly outline the private aspect of the life of employees and in no event interfere with it in the course of employment. This attitude is currently prevailing when it comes to the protection of personal data regarding employees and is repeated in the official positions of the Working Group regarding all the aspects related to processing of personal data in the course of employment.

[14] Those documents are available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[15] Available at: http://www.giodo.gov.pl/pl/file/12460.

[16] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[17] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

MONITORING OF THE EMPLOYEES

Currently, due to the almost indefinite range of measures available to the employers, the employees, understood as a 'weaker' party in the employment relationship should be covered by a special care in terms of the scope of the surveillance measures applied to monitoring the way they perform their work.

As currently most of the work that is seen as requiring some kind of monitoring and direct insight into requires using computers and different types of IT systems, the Working Group focused directly on issues that potentially have the biggest negative impact on the field of the processing of personal data regarding the employees. Summing up the position of the Working Group, it can be said that even though monitoring of an inbound and outbound traffic to the computer of the employee is possible and under some circumstances can be justified (e.g. when it is not possible to block the employee's access to some type of data and the same data is of a great importance to the employer) this solution is possible to a limited extent and should be applied only if the 'physical' blockage of transmitting the important data or access to the specified type of websites or parts of the IT system is not possible.

As a justification the Working Group quoted that it is better to stop employees from infringing of the employer's justified interest by simply not giving them measures to do so (e.g. by blocking their access to some webpages) rather than giving them free hand to do whatever they want with simultaneous restriction that their actions will be monitored all the time.

GPS TRACKING

It is a common practice to enable the employees to use company cars made available to them in order to perform their professional duties also in their private time. This fact itself does not raise concerns in terms of the protection of personal data of the employees. What is of a great importance in this field is the fact that those cars generally are equipped with devices monitoring the location of the vehicle, its speed, operating parameters and other extraordinary events. Gathering this information from the period of time when a person operating the vehicle acts as an employee is correct (after meeting specified requirements). Troubles arise when this information is gathered from the time when the vehicle is used as a private means of transport. According to the Working Group it is inadmissible for the employer not only to process this information but also even to come into its possession. In practice it means that there has to be implemented a technical solution that would completely turn off the transmission of the data from the monitoring device in the period of the private use of the entrusted vehicle. From a practical point of view and taking into consideration the fact that monitoring devices are implemented also in order to track a car in the case of a potential theft, the idea ac-

cording to which this device would have to be turned off in the time of a private use of a car would render installing GPS trackers rather troublesome.

SUMMARY

It is undisputable that after May 25, 2018 the whole system of the personal data protection in the European Union will be subject to a complete and significant change. The Regulation brings with itself not only new obligations and rights but also potential fines threatening the data controllers and data processors. Due to the frequency and scope of the processed personal data within the existence of the employment relationship, the employers are particularly exposed to the risk of bearing the liability for infringing the provisions of the GDPR. That is why they are those subjects that should to the full extent make use of the long '*vacatio legis*' provided by the GDPR and adjust their procedures of the processing of personal data to the requirements imposed by the provisions of the Regulation.

Bibliography

Civil Code of April 23, 1964 (Journal of Laws of 1964 No. 16, item 93).
Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Labor Code of June 26, 1974 (Journal of Laws of 1974 No. 24, item 141).
Personal Data Protection Act of August 29, 1997(Journal of Laws of 1997 No. 133, item 883).
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.
Treaty on the Functioning of the European Union.
Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Kraków 2013.

Internet sources:
http://tvn24bis.pl/z-kraju,74/maciej-kawecki-z-resortu-cyfryzacji-o-zmianach-w-ochronie-danych,743005.html.
http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.html.
Korff D., *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, 2010, s. 69, available at: http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_working_paper_2_en.pdf.
https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.
http://www.eudataprotectionregulation.com/data-protection-design-by-default.

http://gdpr.pl/rodo-iso-wywiad-dr-maciejem-kaweckim-koordynatorem-krajowej-reformy-ochrony-danych-osobowych.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
http://www.giodo.gov.pl/pl/file/12460.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

Summary: The aim of this article is to familiarize the Reader with the outline of the General Data Protection Regulation 2016/679 with a special emphasis put on its part that will be the most troublesome for the entities processing the personal data- monetary and nonmonetary sanctions. It is undoubted that never before have we faced a piece of legislation that can be of such a big importance not only because of the scope of its regulation but also because of its potential detrimental effects for the functioning of the market seen from the point of view of penalties threatening those processing the personal data. Due to the commonness of the employment relationships I decided to make them the basis for my reflections concerning the topic. It is even more relevant as the revolutionary character of the General Data Protection Regulation also results from the change in the attitude towards instructions and guidelines specifying the minimal scope of the protection of the processed personal data.

Keywords: personal data, General Data Protection Regulation 2016/679, sanctions, processing personal data, personal data in employment, personal data protection

SYSTEM SANKCJI W ROZPORZĄDZENIU 2016/679 – OGÓLNE SPOSTRZEŻENIA I UWAGI DOTYCZĄCE ZATRUDNIENIA

Streszczenie: Celem niniejszego artykułu jest zapoznanie Czytelnika z zarysem Rozporządzenia o Ochronie Danych Osobowych 2016/679, ze szczególnym naciskiem na tę jego część, która będzie najbardziej problematyczna dla podmiotów przetwarzających dane osobowe – sankcji pieniężnych i niepieniężnych. Niewątpliwie nigdy wcześniej nie mieliśmy do czynienia z regulacją, która może mieć tak duże znaczenie nie tylko z powodu zakresu swojego normowania, ale także z powodu potencjalnych negatywnych skutków dla funkcjonowania rynku rozpatrywanych z punktu widzenia kar grożących podmiotom przetwarzającym dane osobowe. Z powodu powszechności stosunków zatrudnienia zdecydowałem się, by oprzeć na nich moje rozważania dotyczące tematu. Zabieg ten jest jeszcze bardziej aktualny z uwagi na fakt, iż rewolucyjny charakter Rozporządzenia o Ochronie Danych Osobowych wynika również ze zmiany podejścia do instytucji instrukcji i wytycznych określających minimalny zakres ochrony przetwarzanych danych.

Słowa kluczowe: dane osobowe, Rozporządzenie o Ochronie Danych Osobowych 2016/679, sankcje, przetwarzanie danych osobowych, dane osobowe w zatrudnieniu, ochrona danych osobowych