PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE PROVISIONS OF THE GDPR DURING THE COVID-19 PANDEMIC

Łukasz Wojciechowksi, PhD
Department of Administration and Social Sciences
University of Economics and Innovation in Lublin
email: lukasz.wojciechowski@wsei.lublin.pl

Abstract:

The aim of the raport is to analyze the challenges related to the implementation of GDPR regulations and securing information during the COVID-19 pandemic, which is an important area of financial security of entities. The author points to the traditional application of the GDPR regulations, and then analyzes new challenges with particular emphasis on home office work. The conclusions presented in the report enable better preparation for the next stages of a pandemic or for similar crisis situations in the future.

Key words:
GDPR, personal data protection, COVID-19 pandemic, home office

1.INTRODUCTION

In 2020 and in the first half of 2021, the personal data protection system in the European Union was put to a special test due to the COVID-19 pandemic. The restrictions introduced in order to avoid the spread of the threat on the one hand were associated with the need to perform remote work on an unprecedented scale and transfer other activities to the Internet, e.g. education process in primary, secondary and higher education. On the other hand, not all activities could be transferred to the Internet. Hence the need for cumulative security and elimination

of potential threats (e.g. by measuring the temperature to all persons entering the premises of entities performing medical activities and the requirement to fill in appropriate questionnaires) and to ensure the security of personal data processed during activities aimed at ensuring security. Many of these activities aroused controversy and discussions in the scientific community regarding their legitimacy and legal aspects of individual activities, and the need to make quick and effective decisions due to the emergency situation additionally complicated individual processes.

The aim of the report is to analyze the challenges related to the implementation of GDPR regulations and securing information during the COVID-19 pandemic, which is an important area of financial security of entities. The author verifies the research hypothesis that the COVID-19 pandemic had a significant impact on the functioning of personal data administrators. The presented considerations regarding the personal data protection system in Poland are based on the applicable normative acts, as well as Polish and foreign scientific studies. The practical aspects of personal data protection during the COVID-19 pandemic have been presented largely on the basis of the author's practical experience, as the report was created during the COVID-19 pandemic. Hence, it was impossible to refer to other scientific studies dealing with similar issues. Scientific articles and other publications related to the processing of personal data during the pandemic were written in parallel with this study. Three research methods were used to conduct this analysis. The first of them is the institutional and legal method which enabled the analysis of normative acts regulating the functioning of the personal data protection system in Poland. The second research method is factor analysis, which enabled the selection of information related to the functioning of the personal data protection system and the selection of those that affect the functioning of the system during the COVID-19 pandemic. The third research method is the

comparative method. The use of this method was needed to compare the functioning of the system in public administration and business.

2.IMPLEMENTATION OF THE GDPR REGULATIONS IN THE PERIOD BEFORE THE COVID-19 PANDEMIC

The currently functioning system of personal data protection in Poland was finally shaped by actions at the level of all European Union countries. On April 14, 2016, the European Parliament adopted a legislative package regulating the personal data protection system in European Union countries. The package includes two legal acts. The first is the General Data Protection Regulation (GDPR). It is supplemented by Directive 2016/680, which regulates the protection of natural persons with regard to the processing of their personal data by competent authorities for the purposes of crime prevention, investigation, detection and prosecution of prohibited acts and the execution of penalties. Directive 2016/680, as in the case of the previously indicated Directive 95/46/EC, required implementation by individual states. In Poland, the law of the European Union has also been transposed in this area in an act adopted for this purpose.

In the case of the provisions of the GDPR, it was not necessary to implement them, because a legal act with the rank of a regulation of the European Parliament and of the Council of the European Union has been in force since its entry into force in all Member States. Due to the fact that the authors of the new regulations provided for a two-year transition period, the GDPR became mandatory in Poland from May 25, 2018. On the same day, a new act regulating the personal data protection system in Poland entered into force. It is worth emphasizing that it differed significantly from the Act of August 29, 1997, and this difference did not result from the development of new definitions or the adoption of other solutions in

the field of personal data processing. The new legal act was issued for completely different purposes. First of all, the specification of some GDPR standards and the appointment of a new data protection authority. The absolute applicability of the provisions of the GDPR meant that data controllers must apply the provisions of the regulation directly, and thus read its content. This is a significant innovation, as there was no need to read the provisions of Directive 95/46 / EC, the provisions of which were transposed into the Polish legal system in other normative acts, with particular emphasis on the Act of August 29, 1997 on the protection of personal data. Therefore, there was no need to repeat in the new Polish act the definitions of the concepts and rules for the processing of personal data contained in the GDPR. It is worth emphasizing that in accordance with the previously analyzed Article 51 par. 5 of the fundamental law "The rules and procedure for collecting and sharing information are specified by law". The enactment of the new act allowed at the same time to keep the personal data protection system in the constitutional order.

The provisions of the GDPR are intended to change the philosophy of personal data processing, which is to contribute to the observance of the rights and freedoms of natural persons. This philosophy is based primarily on preventive (proactive) protection, which was defined in the Regulation as privacy protection at the design stage. This approach implies the need to inventory potential datasets and processing processes before commencing a given project or activity. Moreover, each data controller must systematically analyze the risk of violating the rights and freedoms of natural persons. The risk-based approach is innovative and replaces existing solutions. It is worth emphasizing that on April 30, 2004, personal data administrators in Poland received a set of guidelines in the field of documentation and IT systems security in the form of the Regulation analyzed earlier. Currently, in accordance with the provisions of the GDPR, the administrator has a lot of freedom in the selection of technical and organizational security measures

(Marković, Debeljak and Kadoić, 2019). It must adapt these measures to the degree of actual threat. It is also important to significantly expand the rights of natural persons to whom the data relate. Examples include the compulsory nature of allowing complaints to be lodged with national data protection authorities free of charge, or the right to be forgotten which gives an individual the option to request deletion of data. The data processing entity is required to do so, if it is not in conflict with applicable law.

The new regulations also apply to employees of public administration and private enterprises dealing with the protection of personal data. The former function of an information security administrator has been replaced by that of a data protection officer. An important change is the obligatory nature of appointing an inspector in the case of public entities. In many cases, this will strengthen the internal system of personal data protection, however, it happens that public entities that employ one or more employees have a problem with finding an inspector among employees and with financing an external inspector. It is worth noting that the provisions of the GDPR do not specify the detailed qualifications of a person who may act as a data protection officer. The necessity to have professional knowledge was indicated, but it was not specified which certificates or certificates can confirm the possession of such knowledge. This is an opportunity for people who want to work as inspectors and gradually improve their qualifications. Due to the fact that it is possible to perform the function of an inspector in several entities at the same time, it is a good practice to appoint one person for this position in several entities with a similar profile, e.g. schools. Private enterprises do not have to appoint a data protection officer, but in the case of processing large amounts of personal data, appointing a person to this position is considered a good practice.

Among the changes resulting from the provisions of the GDPR, it is also worth paying attention to the issue of informing natural persons, e.g. about who

processes their personal data and for what purpose and what is the legal basis for it. The information obligation is not an innovation resulting from the GDPR, as it already functioned under the Act of August 29, 1997 on the protection of personal data. The priority nature of this action may be confirmed by the issuance of special guidelines by the Inspector General for Personal Data Protection on how this obligation should be fulfilled. Pursuant to Art. 13 and 14 GDPR, however, the information that must be provided by the data controller has been extended, including for contact details of the data protection officer, legal basis for data processing and information about the possibility of submitting a complaint to the national data protection authority. The extension of the information obligation should be regarded as a change of legal provisions that has a real impact on the protection of the legal interests of natural persons.

As a separate issue with the approach based on the risk analysis of violating the rights or freedoms of natural persons, and considered by some researchers and practitioners as part of the risk analysis, the data protection impact assessment should be mentioned (Mihăilă, 2020). In this case, the guidelines for this action were developed by the Art. 29 Working Party before the mandatory application of the new legal regulations. Thus, administrators were allowed to effectively prepare for the impact assessment when it was not yet mandatory. This assessment should be carried out primarily in two cases. The first one takes place when there is a high risk of violating the rights and freedoms of natural persons. Second if the activity is on a list kept by the supervisory authority.

3.THE SPECIFICITY OF THE IMPLEMENTATION OF GDPR PROVISIONS IN BUSINESS

The specificity of personal data protection in business, understood as private entities (companies whose ownership structure is private), significantly differs from

the protection of personal data in public administration. However, as a preliminary remark in this regard, it is worth presenting the conclusion that the legal regulations on the protection of personal data are not only the same in both sectors, but there are also examples of the real impact of the legislator's implementation of concepts related to the functioning of the private sector on the shape of legislation that regulates at the same time functioning of personal data protection in public administration. The basic principles of data security for natural persons are therefore the same. At the same time, both private entities and public institutions must implement the rights and freedoms of natural persons to the same extent.

A different specificity results mainly from the definition of the goals of private entities. Entrepreneurs operate in a creative way and their activity is intended to bring profits. Their actions are limited by law, but if there are no restrictions, they can freely make decisions as to the scope of operation. It is also worth emphasizing that public entities in most cases obtain personal data on the basis of applicable legal acts, thanks to which they have a de facto legal condition for their processing. On the other hand, in the case of companies, it is necessary to obtain personal data necessary to conduct business and look for such a premise. The solution that requires the use of the smallest resources and interaction is the reference to Art. 6 sec. 1 lit. f GDPR in the wording 'processing is necessary for the purposes of the legitimate interests pursued by the administrator or by a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject that require data protection personal data, in particular when the data subject is a child'. However, such a premise cannot be abused, and its application on a mass scale may be questioned by the supervisory authority. Therefore, the legal basis for the processing of personal data by private entities is primarily Art. 6 sec. 1 lit. b GDPR, according to which 'processing is necessary for the performance of a contract to which the data subject is party or in

order to take steps at the request of the data subject prior to entering into a contract' and art. 6 sec. 1 lit. a GDPR, according to which ‘the data subject has consented to the processing of his personal data for one or more specific purposes'.

It is worth noting that consent is an unfavorable premise from the point of view of the personal data administrator. The legal definition of consent has been indicated among the definitions of other key terms in art. 4. According to it, "the consent of the data subject means the free, specific, informed and unambiguous demonstration of the will to which the data subject, in the form of a declaration or a clear affirmative action, authorizes the processing of personal data relating to him". The mere acquisition of consent by a natural person, as well as the possibility of withdrawing it at any time, is a special area of the Regulation 2016/679. The standards in this respect are precise and have been included in the second chapter of this normative act, between such important aspects as the legal grounds for the processing of personal data and specific categories of personal data. Detailed regulations concern the conditions for giving consent and the conditions for giving consent by a child in the case of information society services. Restrictive regulations have been adopted, according to which there can be no doubt that a natural person has given direct consent, which is not implied in any way. At the same time, the personal data administrator may not in any case make it difficult for a natural person to withdraw his consent.

Another key aspect that belongs to the canon of factors shaping the specificity of personal data processing by companies is the possibility of losing a good image (reputation) in the event of a breach of personal data security. There is no doubt that this factor is also of great importance in public administration. The decline in trust in the state is an important phenomenon, but it has an abstract dimension that is difficult to measure and describe directly. In the case of private entities, the situation is different, because companies that have lost their good image

may at the same time lose customers and thus also financial liquidity. In some cases, this may lead to the bankruptcy of the enterprise. The clients of companies obviously do not take care of public affairs in them and do not have to use their services as they have to do in the case of public administration. At the same time, along with the growing awareness of the public in the field of personal data protection, it can be observed that the provision of services at a high level is synonymous with the provision of services in accordance with the principles of personal data security. It is also possible to forecast an increase in such a trend, especially in the case of the most competitive sectors of the economy. Currently, consumers have at their disposal, among others a large number of online stores where they can buy electronics and household appliances. If a personal data leak occurs in one of them and some customers lose their financial resources, then with prices shaping at a similar level, consumers will choose competitive offers in the future, fearing that their personal data may be at risk (Axinte, Petrica and Bacivarov, 2018).

An even greater difference between the private sector and public administration should be noted in the case of penalties imposed by the President of the Office for Personal Data Protection. The supervisor has much more power in this regard for companies. In art. 83 of Regulation 2016/679 specifies general conditions for imposing administrative fines. It is essential to adopt the principle that the supervisor must take into account a wide range of factors before imposing a sanction. This applies both to the decision to impose the fine, as well as to the determination of its amount. The maximum amount of the fine for a company was set at twenty million Euro or 4% of the total annual worldwide turnover from the previous financial year. Selected penalties imposed by the President of the Office indicate the priority importance of cooperation with the supervisory authority in the course of the proceedings.

The reform of the personal data protection system implemented in 2016-2018 provides for the introduction of preventive protection, also referred to as privacy protection at the design stage or proactive protection (Baldur et al., 2019). The essence of this mechanism is indicated in recital 78 of the preamble to Regulation 2016/679, according to which 'the protection of the rights and freedoms of natural persons with regard to the processing of personal data requires the implementation of appropriate technical and organizational measures to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which comply in particular with the principle of data protection by design and with the principle of data protection by default. Such measures may include, inter alia, on minimizing the processing of personal data, pseudonymization of personal data as soon as possible, transparency as to the functions and processing of personal data, enabling the data subject to monitor data processing, enabling the administrator to create and improve security'. According to this mechanism, the priority is to properly plan activities related to the processing of personal data before its commencement, and then to continue and implement the planned security measures during the processing.

4.IMPLEMENTATION OF GDPR REGULATIONS DURING THE COVID-19 PANDEMIC

The issues that took place in Poland and around the world in the first half of 2020 will be the subject of many studies related to all scientific disciplines. The spreading epidemiological threat has changed the functioning of most countries in the world in almost every area. The legal obligation to limit the mobility of people and transfer many activities to their place of residence, referred to as lockdown, was of particular importance. In Poland, it was decided to introduce many restrictions,

which was to protect citizens from the spread of the disease. At the same time, it was quickly realized that the restrictions would have a destructive effect on the economy and the condition of public finances. In Poland and in other countries of the world, a discussion has started on the need to find optimal solutions that will ensure the highest possible level of safety for people, and at the same time enable the functioning of institutions and companies. In this context, it is worth quoting the opinion formulated by German researchers from the Institut der deutschen Wirtschaft - M. Hüther and H. Bardt: 'The fight against the coronavirus pandemic has led to the isolation of social and economic life and will have serious economic consequences. Important areas of industry and services have been partially or completely closed. The resumption of activities should take place as soon as possible, after the medical conditions are established and fulfilled. This requires a clear exit strategy and a few steps to return to previous prosperity and growth indicators. After surviving the crisis through various liquidity lines and bridging loans, a relaunch of the economy requires a restart of public infrastructure, especially schools and kindergartens. Clear signals are needed according to a planned schedule to facilitate the coordinated and synchronized restart of complex industrial supply chains. A tax-driven exit signal and a demand-driven growth agenda can make a significant contribution to the new economic dynamism after the crisis". (Hüther, Bardt, 2020, p. 277-278)

From the personal data controllers' point of view, the events in question primarily required verification of the existing personal data processing procedures in terms of the new reality. In some cases, the transfer of activity to the Internet was a natural process that was gradually implemented anyway, and the pandemic caused the acceleration of these activities. In some areas, however, carrying out activities remotely was troublesome. In this context, education in primary and secondary schools as well as universities should be mentioned first of all. It is worth

emphasizing, however, that the process of modernizing the didactic process and increasing the use of modern technologies is not the same as the fact that all classes are held remotely. If not for the circumstances that forced such a process, such a solution would undoubtedly not be taken into account. This is mainly due to the fact that even with a well-developed system of online lessons, the school also fulfills a wide range of other tasks, and the socialization process also involves traditional contacts with peers and teachers. In the case of schools with specialized profiles and universities, the problem was primarily practical classes, which in some cases were difficult to adapt to this form of education.

These rules apply regardless of whether the work is performed in a traditional manner at the employer's premises or the head of the unit has commissioned the employee to perform work remotely. However, it is the personal data controller that is responsible for data security and the implementation of the rights and freedoms of natural persons. Therefore, it is up to the employer to assess the risk of the employee performing tasks on his own equipment.

In addition, other issues related to remote work, which can be classified as formal and personnel issues, were also regulated. The first is a record of activities performed. The employee is obliged to keep such records at the employer's request, taking into account in particular the description of these activities, as well as the date and time of their performance. It is the employer who decides the form and frequency of preparing the records. The second area is the specific right of the employer to determine the duration of remote work. He may at any time withdraw the order to perform such work and order the employee to return to work in the traditional form.

In addition to the indicated legal regulations for the remanded work, personal data administrators also expected guidelines developed by the President of the Personal Data Protection Office regarding the application of adequate data

security measures. However, the website of the supervisory authority provides only basic information in a synthetic form, which is divided into three areas:

- devices,
- e-mail,
- access to the cloud and the network.

Undoubtedly, it was properly prepared and valuable information, but from the point of view of the scale of transition to remote work, the supervisory body should take more actions in the educational dimension. However, it is worth paying attention to the numerous initiatives of private entities operating in the personal data protection industry, for which publishing valuable information on remote work has become a form of service promotion. As a result, valuable information and tips on the implementation of remote work in a safe manner have appeared on the websites.

One of the mistakes made by some administrators was the recognition that remote work consists primarily of on-line meetings through available applications and dedicated online platforms. Most of the employees did not have any problems with their operation, security was ensured by well-known software producers, meetings were usually not recorded, so it was considered that the risk of violating the rights or freedoms of natural persons in this case was low. Indeed, such activities did not generate many violations and difficult situations, but on-line conferences and meetings were only a part of remote work. Other activities in this area include the use by employees at their place of residence of official documents containing personal data. Additionally, when implementing various types of projects, employees had to consult them with other employees by sending them electronically. In addition, some remotely served clients by collecting their personal information. All these areas and others, the precise list of which could be created individually by almost every personal data administrator, were associated with the

need to select adequate measures for the correct and safe processing of personal data, avoiding breaches of their security and avoiding controls and penalties imposed by the President of the Office for Personal Data Protection. One of the ways to increase security, successfully used by some administrators, was just updating or creating from scratch the remote work procedure.

In the case of such a document, which most often constitutes an appendix to the existing procedures related to the implementation of the provisions of Regulation 2016/679, it was of key importance to anticipate various situations and plan adequate variants of action for them, and to properly define the dependent and independent variables. Repeated updating of the document could have a negative impact on its proper interpretation by employees, hence entering all relevant elements before the first presentation of the procedure to employees is a good practice. An example in this respect may be the dilemma of whether employees' private equipment will be used to perform remote work and whether employees will use their own equipment to work from home (Beňo, 2018). In the procedure, the administrator may describe the actual situation in which, for example, only employees' private equipment is used for the purpose of remote work. However, it is worth considering whether in the (near) future it will not be necessary to hand over work equipment for home use in the event of extending the scope of tasks performed as part of remote work. If there is a high probability of taking such actions, it is worth entering them into the procedure immediately and there will be no need to update it when it happens.

The development of a remote work procedure is an activity that does not result directly from the provisions regulating the functioning of the personal data protection system. Therefore, there is no single valid catalog of items it should contain. It is a good practice to include a comprehensive manual for the employee in the remote work procedure, in which the administrator specifies in the form of a

checklist a catalog of activities that should be performed in order to guarantee the security of personal data. It is also worth considering security measures in the procedure, with particular emphasis on those that were analyzed in Subchapter 4.4. At the same time, it should be emphasized that the remote work procedure alone is not sufficient to properly implement the provisions of Regulation 2016/679. The administrator should also carry out other activities, including review internal regulations in terms of taking into account new elements resulting from the change of the operating mode.

The situation of companies during the COVID-19 pandemic was different than in the case of public administration entities. It was conditioned mainly by the necessity to ensure financing of the current activity in the face of changing priorities of the majority of consumers. State-initiated instruments supporting entrepreneurs, incl. loans and subsidies are not analyzed in this study, but they cannot be omitted when examining issues related to the protection of personal data during the COVID-19 pandemic. Regardless of the assessment of the effectiveness of state aid referred to as the 'anti-crisis shield', there is no doubt that the additional funds, especially in those geographic areas of the country where they were efficiently disbursed, allowed the management staff to act more thoughtfully and over time. In some cases, they allowed, inter alia, at least postponing decisions on job cuts. This is important from the point of view of personal data protection, as there is a group of entities in the private sector where data security procedures are not prioritized and a job reduction involving the concentration of other employees only in areas that generate income in the short term would be negative. impact on the implementation of the provisions of Regulation 2016/679. At the same time, in the case of some companies, the discussion on the legitimacy of implementing the provisions and creating procedures for the protection of personal data has returned. The administrators tried to evaluate the personal data protection system in relation to

saving jobs, the existence of families and other areas commonly considered important in many dimensions, including the axiological dimension. Such a statement, however, is incorrect, because, as indicated in individual chapters of this monograph, the construction of an adequate internal system of personal data protection contributes to the effective functioning of entities, helps to organize other procedures, as well as increases the level of trust, while improving the company's image. Therefore, such argumentation should be considered as an attempt to reduce the number of tasks in the short term, which, however, may have negative effects in the long term.

It is worth emphasizing that some private entities managed to implement remote work mechanisms very quickly. This applies, of course, to entities operating in sectors where this was possible. The lack of such a possibility concerned primarily the service industry, but in the case of companies providing services that cannot be provided via the Internet, the creativity of some entities deserves special attention. An example would be hairdressers who sold hair care and dye accessories via websites and then communicated with their clients via instant messaging to provide remote instructions on their applications. Such action, of course, had a marketing dimension and made it possible to maintain ties with customers, but at the same time it was an extraordinary way of using remote work mechanisms. On the other hand, the most natural form of transition to remote work mode can be seen in the case of employees who worked in the office in the period before the pandemic on dedicated computer workstations. Regardless of whether their work consisted of performing data analysis and preparing reports, or dealing with customer service or other areas, in many cases it was possible to transfer these activities to their place of residence and perform them as part of remote work. The situation in which the employer was unable to continue running a business in a traditional form was a kind of compulsion to accept the use of modern technologies. It is also worth

emphasizing that this is a de facto obligatory test of the effectiveness of remote work and the organizational units in which this form of work works, and in which it is ineffective and should not be performed in the future. Therefore, it can be predicted that even if the pandemic period does not revolutionize the current functioning of companies, it will undoubtedly contribute to the evolution in terms of changing the current form of performing certain activities.

5.CONCLUSIONS

The presented considerations lead to the conclusion that the COVID-19 pandemic has permanently changed the functioning of private entities, but also public administration entities in the field of personal data protection. Currently, research in this area is at an early stage. Therefore, it is worth postulating an academic interdisciplinary discussion in this regard, because the changes that have occurred will not be reversed and business must prepare to function in the new reality.

The Polish experience of the functioning of business indicates lack of proper preparation to face the COVID-19 pandemic in terms of creating home office procedures and other changes in the protection of personal data. Therefore, it is worth postulating the creation of codes of good practice and transmission channels enabling information exchange.

The last conclusion is greater flexibility of business in relation to public administration in terms of introducing new solutions. This is due to other human resources, but also the possibility of faster implementation of legal provisions. Therefore, it can be predicted that the business will cope well with the COVID-19 pandemic in the area of personal data and overcome the difficulties.

The author points out that due to the lack of a sufficient number of sources, this report is largely based on his empirical experience. Therefore, conclusions should be verified during seminars and scientific conferences, as well as in the future with the effects of other scientific research in the form of literature on the subject.

REFERENCES

1. Axinte, S – D., Petrică, G., Bacivarov, I. (2018), *GDPR Impact on Company Management and Processed Data*, 'Quality - Access to Success', Vol. 19, Issue 165.
2. Baldur, K., Sahk, A. Berendsen, V. (2019), *Privacy by design in statistics: Should it become a default/standard?*, 'Statistical Journal of the IAOS', Vol. 35, Issue 4.
3. Beňo, M. (2018), *Working in the virtual world - an approach to the "home office" business model analysis*, 'Journal of Interdisciplinary Research', Vol. 8 Issue 1.
4. Hüther, M., Bardt, H. (2020), An Economic Policy Exit Strategy from the Corona Lockdown, 'Wirtschaftsdienst', Vol. 100(4).
5. Marković, Maja, G., Debeljak, S., Kadoić, N. (2019), *Preparing Students for the Era of the General Data Protection Regulation (GDPR)*, TEM Journal, Vol. 8 Issue 1.
6. Mihăilă, C., Mihăilă, M. (2020) *The legal interes, legal basis for the processing of personal data and the right to private life*, 'Fiat Iustitia', Issue 1.

Sources of law

7. The Constitution of the Republic of Poland of 2nd April, 1997, as published in Dziennik Ustaw of 1997 No. 78, item 483.
8. Act of 27 August 1997 on the protection of personal data, as published in Dziennik Ustaw of 2016, item 922.
9. Act of 10 May 2018 on the protection of personal data, as published in Dziennik Ustaw of 2019, item 1781.
10. 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), as published in the Official Journal L 119, Volume 59, on 4 May 2016.

Documents

Article 29 Working Party, Guidelines on Data Protection Impact Assessment and helping to determine if processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 04/04/2017, (WP 248 rev.01).