WROCŁAW UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF ELECTRONICS

FIELD: Computer science (INF)
SPECIALIZATION: Internet Engineering (INE)

MASTER OF SCIENCE THESIS

Personal Data Processing Support System for
the Company in the Face of New RODO
Regulation Requirements

System wsparcia przetwarzania danych
osobowych w firmie wobec nowych wymagań
wynikających z rozporządzenia RODO

AUTHOR:

Paweł Rymer

SUPERVISOR:

dr. inż. Jacek Mazurkiewicz

GRADE:

WROCŁAW 2018

Contents

Chapter 1

Purpose and scope of work

This work presents issues related to personal data processing in the face of General Data Protection Regulation (GDPR - Polish equivalent to this abbreviation is RODO and it stands for "*Rozporządzenie Ogólne o Ochronie Danych Osobowych*"). Upcoming changes in regulations oblige any entity that processes personal data to meet certain requirements. This entity is related to, among others, enterprises and companies. The more data is being processed in such entity, the more complex structure is required to manage this data. For medium and large enterprises, amount of data being processed requires the use of advanced IT systems. In the face of GDPR, such IT system should also support meeting new standard of personal data protection.

In this paper will be described the value which personal data represents, origins of personal data protection, legal state in European Union and Poland before GDPR and the risks associated with the processing of personal data on a large scale. In the following, the issue of the GDPR will be discussed. The question of what it is, what it stands for will be considered and scope of changes in regulations will be shown. The available solutions supproting GDPR requirements will be presented and analyzed to determine which provisions are necessary to be implemented in existing applications that process personal data so that they comply with the new requirements, and how the IT system is able to support the data controller on his legal obligations. Next, the existing IT system processing personal data, which required adaptation to the new regulations, will be briefly described. After this introduction, the changes implemented to this application will be presented, thanks to which it will become compliant with the new regulations. The prototype of the module developed in the application will also be discussed, which will support the data controller in his new duties resulting from GDPR.

1.1   Description of the problem

On the 25th of May 2018, GDPR become effective. Introduced changes can be divided in two ways, these more revolutionary, and these less revolutionary. These less revolutionary are basis legal concepts or rules of personal data processing which didn't actually change since current state. These more revolutionary are connected with rules to practical application [13]. These rules assumes increasing self-reliance, but also responsibility of data administrators.

The reason for the changes in the existing regulations is dynamic technological and social development, as well as the growing need for a fluid, but at the same time safe, transfer of data across national borders. The increasing scale of personal data processing

and the benefits derived from them create the necessity of introducing more advanced legal mechanisms that protect the privacy of users. The extending range of personal data processing requires not only increasing the user's security, but also his knowledge about puroposes of processing his data.

The scale of the impact of the processing of our personal data on our lives is hard to imagine. Especially, that we are not completely aware either of their consequences for us nor a multitude of areas they influence. The best example of this is the recent events related to the leakage of Facebook data for Cambridge Analytica. Facebook is a social networking site with a global range of about 2 billion people. The latter is, in a short, a consulting company that created software to analyze people's political preferences based on the data collected. The analyzed data is then sold to interested client, which was, among others, the election team of US President Donald Trump. With the help of external applications that could freely use data about Facebook users, this company came into possession of very sensitive information about political preferences of, estimated at least, 87 million people around the world. This data was used for targeted sending, profitably for Facebook, of political content to potential voters, and could significantly affect the result of US presidential elections in 2016.

At this point should be highlighted some very important things that have a fundamental influence on the development of these events. First of all Facebook's postion in obtaining data about its users. Over time, this portal took a dominant position in interpersonal relations. It allows us to both transfer our social life to the internet and express our views in public. Most importantly, however, it records and stores all of our account-related activities. Considering, in principle, unlimited access to the Internet, and hence our virtual personality on facebook, we allow to gather much more data about ourselve than we think.

Another important thing is the way Facebook manages its users data. After the Cambridge Analytica scandal, a public hearing of Facebook CEO Mark Zuckerberg was held before the US Congress and then before the European Parliament. In the course of the first hearing, it emerged that the data is processed not only in connection with the bussiness model, assuming the collection and payment of certain data about users attractive to advertisers, but also can be made available to Facebook client applications. That was the case with the applications that were later transferred to Cambridge Analytica. At this point, Facebook's CEO acknowledged that the data was downloaded without supervision.

The last thing to be highlightet here is the possibilities offered by broad access to personal data along with modern technology, and influence on our society. The Cambridge Analytica case is just an example. There are plenty of other enterprises, which bussiness model based on acquiring, processing and storing personal data. We know from elsewhere, that governments are also extensively collecting personal data about citizens. A sufficient example of this are the documents disclosed by Edward Snowden in 2013, which the press considered as the largest leak of information in US history.

As we can see, the current technological and social develpoment brings about the need to constantly adapt regulations to progress in order to provide citizens with privacy security. This is necessary to guarantee respect for fundamental human rights and liberties.

New regulation determines way of approaching to data processing called *risk based approach*. It assumes that first thing that should be done during gathering and using personal data is to analyze risk that could be caused for people which data concern. Another thing is *accountability rule*. It assumes that any data administrator has a duty to introduce appropriate technical and organizational mesures appling compliance with regulation

requirements, but at the same time it does not describe neither any best practices nor minimal technical standards. After the entry into force of GDPR, every administrator will have to independently decide which securities should be implemented. New regulation indicate instruments which may support administrator in making decision. This instruments are codes of conduct and certification mechanisms approved by state's main authority for the protection of personal data which is GIODO in Poland ("*Generalny Inspektor Ochrony Danych Osobowych*"), guidelines from European Data Protection Board or data protection officer. Besides, the ISO norms could be used as a source of practical knowledge [13].

Accountability rule also assumes demonstration by the administrator of compliance with the law. It could be realized, for example, by documentation of implemented legal instrumets described in regulation or by usage of approved codes of conduct mentioned above.

Chapter 2

Personal data protection

The emergence of new technologies, over time, totally replaced traditional, manual methods of data processing. The changes have come so far that they have caused a threat to the individual. This threat was difficulties to control the flow of information about this individual and its content. It led to the occuring a problem with entering to the scope of human privacy and dilemma how to protect a man against interference in his life.

2.1   Personal data as a value

In accordance with applicable, before GDPR comes into force, regulations, personal data are information allowing unambiguous determination of the identity of natural person [11]. The new GDPR regulation is defining personal data more detailed, because they not only defining concept itself, which is similar, but also it defines what identifiable natural person stands for. According to new definition, an identifiable natural person is one who can be identified, directly or indirectly, on the basis of specific phisical, geographic, economic, social, mental, genetic factors or virtual identities [2]. The second definition is much more specific, because it lists more exactly core characteristics of every natural person, considering also his virtual identity. What changed the most, over time, between these two legal acts is consideration of transferring a significant part of human life to the network and creating a copy of real identity there.

One can meet the therm that personal data is perceived as a new *"oil"*. This metaphor is appropriate because they can be used as a product in itself and as being a substance that is a basic to other activities. On the one hand, our personal data like name, surname, or telephone number are products in itself e.g. for direct marketing. Databases filled with such data are basis in this bussiness. The more precise these data are, the more valuable are they. For example, just name connected with phone number or address may cost around 0,50 and 0,80 PLN per record. They can be even cheaper for big orders. But in the same time, contact to the person initially interested in specific offer may cost between few and tens of PLN. On the other hand our data may be used indirectly e.g for political, economical or social purposes. There are many examples. In the 1950s and 1960s the FBI spied on the pastor of the First Unitaryan Church in Los Angeles due to his policy. For this reason members began to worry about internal unity and joint support of political goals. In 2013 the sued the NSA for internal espionage [23].

Another aspect of personal data is their storage. We live in the age of computers controlling every device. Thereby every day we are reacting with many computers. And the side effect of theirs operations are our personal data. Many service providers like, for

example telecommunication operators are storing these data. When we use smartphone, operator knows where we are, where do we call, what are we browsing in internet etc. Only storage of calls from every phone in the USA requires almost 300 milions petabytes or 30 milions of dollars every year [23]. Over the years 2011 and 2015 cost of storage 1 petabyte of data decreased from 1 million USD to 100 000 USD [23]. This fact combined with the growing speed of data processing by computers lets us deduce that nowadays storing data is far more profitable than their selection.

2.2   Genesis of personal data protection

Personal data protection is closely related with human dignity, which is basis of all human rights. This close relationship has its source in the concept of privacy, which appeared for the first time in a legal context due to two american law professors, Samuel D. Warren and Louis D. Brandeis. In the article they published in 1890 year, they used concept of *right to privacy*, which is defined as right to exclusivity, separateness, loneliness and right to be let alone [16]. Privacy in itself is referred to as the right of the individual to decide for itself when and how information about it will be shared for third parties [16]. Taking the above under consideration, right for privacy may be defined as ban on the interference of other entities, both private and public, in every field of live of the individual, unless special legal conditions are fulfilled [16].

Personal data protection from the legal side is relatively new. In the field of personal data protection, two acts are considered as to be pioneer - union law of the Hesse Pariliamen from 1970, on the union level, and Swedish law from 1973 on the state level [15]. They initiated regulation of legal provisions in Western Europe in 20th century. The next acts that appeared were the first federal law of Federal Republic of Germany from 1977 which introduced personal data protection in public and private institusions, French law on informatics, files and civil liberies from 1978, two Danish laws concerning data registers from the same year, also in the same year Austria enacted law which gave to all citizens basic right for demanding confidentiality, and Luxembourg law from 1979 on use of data in informatic systems [15].

2.3   Historical acts of international law

Among international sources of law, definitely more emphasis was placed on regulating privacy issues, which is broader meaning than protection of personal data in itself. None of the documents issued by the United Nations was entirely dedicated to the regulation of this problem. These documents, however, emphasizing the protection of privacy, indirectly influenced the increase of awareness about protection of personal data.

Universal Declaration of Human Rights, enacted by General Assemlby of United Nations in 1948, includes three important provisions. Article 12 of Declaration introduces the right of human to protect correspondence as well as family, home and private life. At the same time it prohibits entering into anyone's private, family and home life as well as correspondence. Finally it grants everyone right to legal protection against interference in privacy [15]. However, Declaration is not binding on the Member States. Another important document was the International Covenant on Civil and Political Rights. This pact in the article 17 states that no one can be the target of unlawful influence on his private life, home life, family life or correspondence. In contrast to the Declaration, this document may be the basis for drawing legal consequences for the state that ratified it.

Althoug these two documents regulated much wider aspects of human rights protection, they significantly influed the legal basis for the protection of personal data [15]. The most important UN resolutions from the point of view of personal data protection are rosolutions 34/169 from 1979 and 45/95 from 1990. The first one recommends the rules of dealing with personal data collected by a public order officers and their sharing. The second resolution refers to rules of gathering data in data banks, including personal data.

An extremely important document in the field of human rights protection was written on 4th of October 1950 in Rome, European Convention for the Protection of Human Rights and Fundamental Freedoms. In article 8 it provides everyone with the right to respect for their private and family life, their home and correspondence. It prohibits the power of interference in the life of a given person's excluding cases justified legally, socially or economically from the point of view of the state [15].

The provisions of the Convention 108 of the Council of Europe are considered as the first international act in the field of personal data protection. They concerned protection of persons due to automatic personal data processing. The convention strictly defines what personal data is, and what an automated data set is and also specifies the rules regarding the quality of data being processed. Very important thing that this convention introduces is the requerement that data processing has to be carried out only for specific and justified purpose. Data cannot be stored more than specific purpose needs to. The exemplary obligations that the Convention introduced are fulfilling the information obligation, the right to demand the correction of data about yourself, possibility of limiting protection only on grounds of security or defense of the state justified. [15]. Prior to the effective date of the GDPR, this Convention is only, by a legally binding, international act concerning protection of personal data, ratified by all countries belonging to the European Union [15].

2.4 Status in Poland before GDPR comes into force

The basic legal document regulating the protection of personal data in Poland is the Constitution of the Republic of Poland and derives from the right to privacy. Directly refers to this problem article 51 of the Constitution. This article provides the individual's right not to disclose data about himself, prohibits public authorities from collecting and sharing information other than necessary in a democratic state of law, introduces the right to demand correction or removal untrue or incomplete information, or information acquired in a manner inconsistent with the Act, the rules and procedure for collecting and sharing information are specified in the Act [10]. At this point, it is worth noting that the Constitution only partially regulates the protection of personal data, and as to the procedure of acquiring and sharing infromation, it refers to the act.

The legal Act that regulates the processing of personal data as a whole is the Act of 29 August 1997 on the protection of personal data. However, this Act does not regulate the processing of personal data in complete manner. The scope of application covers specific categories of processed information (e.g. classified information, or data on persons belonging to the Church or other religious association [15]) and sepecific activities (e.g. from natural persons which are processing data for personal or home purposes or entities with their registered office or place of residence in a third country [15]). Application of this Act does not cover press journalism or literary and artistic activity, unless they violate the rights and liberties of a person, the data refers to. Moreover the Act defines the basic principles of dealing with personal data, indicates the conditions for their processing

and the principles of caring for their safety. Specifies legal mesures to prevent fraud and liability for violations of these provisions. Finally the Act determines competences of the authority for the issues of protection of personal data, which is General Inspector for Personal Data Protection (GIODO).

The right to the protection of personal data is regulated also by other specific provisions. Article 5 of the Act provides that if the provisions of other laws refer in more detail to the protection of personal data, the provisions of these laws shall apply.

The accession of Poland to European Union resulted in necessity to adapt national regulations to those binding in the Community. Wherefor, in 2001 and 2004 two amendements where introduced, which implemented the current European Directive 95/46/WE [15]. After these changes, three more amendements took place, one in 2014 and two in 2016. These changes were connected with supporting the creation of unified digital market, improving work of personal data administrators and the GIODO immunity.

Chapter 3

GDPR

On the 27 April, 2016 was passed the regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movment of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The main purpose guiding the creation of this resolution is given in the second point of the preamble to this regulation, and states that it aims to influence the development of zones of security, freedom and justice, tightening economic relations in the internal market, socio-economic progress and the well-being of people [14]. By analyzing the remaining points, we can find more detailed reasons that led to creation of this legal document, as well as indications regarding the adaptation of new provisions to existing regulations in Member States. Among sources of inspiration should be mentioned new challenges in the field of personal data protection that resulted in rapid technological development and prograssive globalization, to harmonize the protection of the fundamental rights and liberties of individuals with regard to the processing of their personal data and to ensure their free movment between Member States. Ensure consistency and uniformmity in application of these principles in Member States, and to make protection of natural persons independent from applied technics to reduce the risk of circumventions as much as possible [14]. The new regulation gives special protection to children, motivating this with their less awareness of the risks associated with the processing of personal data. What should be emphasized here is that GDPR only concerns the protection of natural persons, and all entities that process personal data of those natural persons are subject to this regulation. The most important provisions and changes introduced by the new regulation will be discussed below.

3.1   Personal data according to GDPR

In the scope of the definition of personal data, the GDPR does not introduce any significant changes and is based on those elements on which Directive 95/46/WE of the European Parliament [12] or Polish law of the protection of personal data [1]. However, it introduces important concept of *pseudonimisation* of data, which consist in the reversal of identity secreting, e.g by encrypting them with a specific key. Importantly, the use of this mechanism is highlighted directly as an example of the application of technical means for data processing by the administrator.

Significant differences in the new regulation occur on the basis of certain categories of data, the processing of which is generally prohibited, and allowed only under certain conditions. The current Polish law defines them as *sensitive data* [9] while the GDPR uses

the concept of *specific data category* [3]. A novelty in the collection of these special categories of data is the precisie definition of the concepts of genetic data and biometric data. In addition, some categories of data, which previously were included in this collection, according to Polish law, are not covered by new regulations as special category of data. This applies to religious beliefs, religious affilation, party affilation, information on judgements issued in court or administrative proceedings, or addictions. Instead, information about ideological beliefs were included.

3.2 Principles of data processing and their scope

The general rules for the processing of personal data are clearly set out in the new European regulation. Article 5 is comprehensive set of general rules for the processing of personal data. This collection consist of principles:

- *compliance with the law, reliability, clarity* - consist of three elements. First of all the purpose of data processing must have the legal basis set out in Regulation. For such a basis, new provisions accept the consent of the person to whom data concern, the necessity resulting from the purpose of the contract performance, the administrator's performance of legal obligations or a task carried out in the public interest (*"compliance with the law"*). Individuals whose data is processed should be aware of this. The purpose of the processing should be formulated clearly, succiently and in such simple language that the child could easily understand them. This information should also contain administrator data, data processing period and rights of their owners (*"reliability and clarity"*),

- *limited purpose of data processing* - means that data can only be processed, for a clearly defined and legitimate purpose. It is worth noting that this point provides for further processing for archival purposes in the public interest, scientific, historical or statistical research as consistent with the law and original purpose. If the legal basis for the processing was consent, the change of the purpose of the processing requires a new consent at this point,

- *data minimization* - GDPR places special emphasis on this principle. According to this rule, the scope of aquiring data may not exceed the amount necessery for the purpose of processing. The data processing period should also be as short as possible. The practical implementation of this rule means, therefore, that the purpose of the processing should first be analyzed in order to determine wheather personal data is necessary for this purpose at all,

- *correctness of data* - this principle assumes, that the data being processed must be current and correct. It should be noted here that this is significantly connected to the right of persons whose data is processed, to require the correction and completion of data about themselves. It imposes on the administrator the obligation to ensure the implementation of appropriate technical and organizational measures that will allow for a smooth correction of data in case of irregularities,

- *limited data storage* - refers to the principle of data minimization, but slighty extend it. It requires that prior to the start of the processing, determine the time of their storage, after which this data has be removed, and also periodical reviews of data should be implemented,

- *integrity and confidentiality of data* - this point imposes on the data administrator the obligation to protect data in terms of inviolability from unathorized access. It also obliges to quickly restore data to the correct state after any incident. It does not specify exactly what technical measures are to be used, but when it comes to confidentiality, it suggests, for example, using *pseudonymisation* or data encryption. GDPR defines *pseudonymisation* as the processing of personal data in a way that makes it impossible to assign them to the data subject without additional information [2],

- *accountability* - the last of these rules is the point of contact between all the above. At this point, the data administrator is required to demonstrate compliance with all of these principles. The practical implementation therefore requires him to analyze all measures taken to demonstrate compliance with the general rules of personal data processing personal data contained in the GDPR.

Most of the above principles had their equivalents, direct or indirect, in the regulations established before the GDPR became applicable. What is new in this case are the principles of minimization and data storage rules, which emphasize the importance of data protection in new regulations. However, by applying strict administrative fines, its rank grows even more.

3.3 Information obligations and the rights of the data subjects

The new regulation assumes to realize information obligation towards persons, which data concern. This approach is similar to the previous provisions e.g. Directive 95/46/EC or Polish Act on personal data protection. However, the GDPR introduces obligations which so far were not necessery. This applies, among other, to the information about duration of the processing data, possibility of being subject to automated decisions and its consequences or contact details to the Data Protection Officer, if he is appointed. Therefore, having regard to the information clauses existing before date of GDPR coming into force, they need to be reviewed and updated to ensure that they meet requirements of the principle of data transparency. This approach is recomended by Article 29 Working Party GDPR [17]. New in this area is also requirement for information to be conveyed in a concise, clear and understandable language. It is also connected with the principle of accountability. The data administrator will have to show that the specific way of transmitting information was the most appropriate in a given case. Therefore, it can be concluded, that proper implementation of the inforamtion obligation compliant with GDPR will be visible at the first glance.

As regards the rights of natural persons in accordance to processing of their personal data, the assumptions of the GDPR are twofold. It not only preserves and strenghtens the current set of rights, but also extends it with new privileges. The set of privileges granted under the new regulation consist of the rights to[13]:

- *being informed about processing operations*,

- *access*,

- *rectify/supplement data,*

- *to be forgotten,*

- *limiting the processing,*

- *data transfer,*

- *opposition,*

- *not to be subject to automatic decisions.*

Most of the above were available to user earlier, but it is worth paying attention to novelty in this scope.

The *right to be forgotten* existed on the basis of provisions preceding the GDPR. However, these provisions were not adapted to the capabilities of current data processing technologies. According to this law, any data subject, may require the data controller to delete it without undue delay if certain circumstances exist. The new regulation provides for several circumstances that must occur in order to make the exercise of this law justified. On this basis one will be able to apply for deletion of data if e.g the purpose of processing does not require this anymore, there are no overriding reason for processing or when the processing of data was unlawful [19]. The premise for refusal to delete data by the administrator may be, however, if it is necessary to exercise the right to freedom of expression and information [19].

The *right to limiting the processing* assumes that the data subject may request the controller to stop processing and limit himself only to their storage. It can be used when the data subject questions the correctness of data processing or it is illegal [19].

The *right to data transfer* is a completely new privilege, allowing the individual to request their data from the controller and deliver them in an accessible format. One can also request the controller to transfer this data, if it is possible, directly to the other administrator. This provision, however, is not clarified, and additionally, contains some discrepancies in terms of technology used by the administrators. This right can be used only if the legal basis for processing is the individual's consent or contract [19].

The *right to opposition and not to be subject to automatic decisions* gives the opportunity to oppose a decision based solely on automatic processing, e.g. *profiling*, and whose effects affect the data subject to a large extent [19]. At this point, it is worth explaining what *profiling* is according to the GDPR definition. New provisions define this as any form of automatic data processing, consisting in collecting information about a data subject based on its behavior and determining its consumer preferences [2].

3.4   Consent to the processing of personal data

The consent of the data subject is one of the basic premises for the legal processing of its personal data. The new law precisely defines what consent to data processing is and also in what form it should be granted. For the right consent, voluntary and unambigious demonstration of the will is considered, and awareness of the purpose of the processing as well as basic information about the administrator. Such consent should be expressed in the form of a statement or explicitly confirming action [25].

The new provisions also regulate how consents should be obtained in relation to the purposes of processing. They indicate that it is acceptable to collect one consent for many processing purposes. This is a significant relaxation of requirements in relation to previous obligations [25]. The new assumptions also place special emphasis on the conditions under

which consent has been expressed. This is all the more important, because in the event of inadequate consent, it will not be valid by law, so that data processing on its basis will also be illegal [25].

Another important thing that GDPR introduces is the requirement that the withdrawal of prior consent needs to be as simple as submitting it. This is to protect users from using mechanisms that make it difficult to resign of services that use personal data processing. Therefore, the procedure of withdrawal of consent involves the use of the same means of communication by which consent has been given [25].

The volouriary nature of consent is subject to particular pressure according to the new rules. The GDPR directly mentions cases where the consent does not have a volouriary character, for example [25]:

- making contract performance conditional upon consent, even though processing of personal data is not necessary for that,

- refusal of consent is subject to legal consquences,

- compulsion to consent to many processing purposes at the same time, despite the appropriateness of dividing consent on each of those purposes.

As regards children, the GDPR allows the data processing of persons over 16 years of age. It also stipulates that Member States may reduce this age, but not more than up to the age of 13. The consent given by the legal guardian of the child is necessary below the age limit. At this point, the new regulations require the administrator to implement reasonable measures to verify whether it is the authorized person who consented.

3.5   Security

Each data controller must individually implement appropriate organizational and technical measures to ensure that the amount of data processed, the scope of their processing or their storage period do not violate the new provisions of the GDPR. This also applies to the availability of this data, and above all to the guarantee that these data will not be made available to unauthorized persons without the consent of their owner. In terms of IT infrastructure and the tools used in it, the main authority for the protection of personal data in Poland, on the basis of the new regulation, distinguishes the following safeguards [20]:

- *authentication* - giving special permissions to people who process personal data by data controller,

- *firewall protection* - according to the new regulation, the IT system processing personal data should be protected against threats from the network by means of implementing physical or logical security measures,

- *encryption of personal data* - transmission of files with personal data should be encrypted. The files themselves should be password protected and sent to the recipient in a different way,

- *data backups* - according to the GDPR it is recommended to create backups and store them in a different place than the right data. However, according to the principle of limited storage, after the specified processing period has elapsed or its purpose has been achieved, all data should be deleted,

- *pseudonymisation* - recommended as an effective measure limiting the ability to link data with a natural person. It consists in replacing one of the attributes with the other, which implies the possibility of indirect identification of that person.

- *anonymisation* - it consists in transforming the data in a way that makes it impossible to identify person on their basis. This process is assumed to be irreversible.

In addition to the technical safeguards suggested, it should also be noted that it is people and not machines that pose the greatest threat to data processing. Therefore, the data controller should also adequately ensure the implementation of organizational measures in relation to the personnel responsible for the processing of personal data. This is, among others, about raising the level of knowledge and awareness of employees, keeping records of persons responsible for data processing, organization of work space and ensuring the secrecy of data processing among staff.

3.6   Documentation of processed data

The new regulation puts a lot of emphasis on documenting the processing of personal data. This is particularly important from the point of view of the accountability principle (3.2) to which data controllers must adhere. In particular, this applies to information such as:

- Type of data held,

- way of obtain them,

- legal basis for their processing,

- way of fulfilling the information obligation,

- to whom and when this data is shared,

- way of reporting security breach incidents,

- method of appointing a data protection officer,

- supervisory authority for cross-border data processing.

The GDPR regulations require explicitly that in certain conditions the data controller keeps a register of processing activities [5]. Examples of such circumstances are the employment of more than 250 people by the entity, or specific processing conditions, such as a high risk of violating the rights and freedoms of the data subject or the processing of a specific data category. The very concept of processing activities is not defined in the regulation, whereas GIODO indicates that this can be interpreted as a set of operations on data that are interrelated. They can be carried out by one or several people, which can be defined collectively in connection with the purpose of undertaking these activities [21]. The new regulation also indicates that such a register is required to enable the supervisory authority to properly monitor the processing.

3.7 Rules of privacy by design and privacy by default

Both concepts being the subject of this point are not new but very important in the context of the new regulation. It assumes that each of them should be treated not as an addition to services, but rather as one of the basic elements [18]. *Privacy by design* refers to the very beginning of the project and assumes that privacy protection must be implemented in new solutions at the design stage. It also assumes, that by default, only minimum personal data that is need for purpose should be processed. This is to ensure that organizations in their new products, services, or applications at the design stage determine the minimum amount of personal data necessary to achieve the goal. Thanks to the implementation of such transparency, from the business point of view, the service provider ensures greater confidence of its clients if it can offer them privacy protection as a basic service. On the other hand, the clients themselves can consciously control the impact of the service on their privacy. *Privacy by default* is directly related to the principle of data minimization (3.2). According to this principle, each new system user is to be provided with default settings to protect their privacy at the highest possible level. In this case, only the necessary amount of personal data of the user is allowed. This rule follows directly from the *privacy by design* principle. The application of both these principles is a legally conditioned obligation arising directly from art. 25 of GDPR [4].

3.8 Violation of data protection

As defined in GDPR, a breach of personal data protection means a security incident resulting in incidental or illegal destruction, loss, modification, disclosure or access to processed personal data.

Among the new obligations imposed on data controllers by GDPR is the need to report incidents of data protection breaches to a designated supervisory authority. According to these requirements, such notification must take place no later than 72 hours after the detection of this violation [6]. If there is a high risk of violating the rights and freedoms of the data subject in connection with a breach of protection, he should also be notified immediately [7]. In both cases, the new provisions precisely define in what form such a notification should be submitted.

The new regulation also says that data controllers should use adequately effective means of detecting such violations in order to be able to respond as quickly as possible to incidents to persons whose protection of personal data has been compromised. A quick response to such events is extremely important, because it can prevent many serious, from the point of view of the data subject, consequences. For example, let a data leak, which can be used, for example, to steal one identity in order to take out a loan. In this case, rapid detection of the incident, and informing the supervisory body, as well as data owners, can prevent high material losses.

3.9 Penalties for violation the provisions

The GDPR provides for substantial penalties for violations of the law, which depend, of course, on the degree of violation. These can be both financial and non-financial sanctions. Among non-financial penalties, there are warnings, rebukes, prescripts (e.g. to notify a person about data violation or fulfillment of its requests) by limiting processing until a complete ban. Regarding financial penalties, the regulation assumes that their amount is

intended to discourage particularly serious infringements. For less serious infringements, a penalty of up to 10,000,000 EUR or 2% of the total worldwide turnover from the previous year is expected, whichever is greater. This applies to the following violations:

- Rules of privacy by design and privacy by default (Art.25),

- processing on authorization of data controller or processing entity (Art.29),

- registering processing activities (Art.30),

- cooperation with supervisory authority (Art.31),

- processing security (Art.32).

For more serious infringements, a penalty of up to 20,000,000 EUR or 4% of the total worldwide turnover from the previous year is expected, whichever is greater. This applies to the following violations:

- General rules of processing data (Art.5),

- consenting conditions for data processing (Art.7),

- executing by data subject right to access (Art.15),

- executing the right to rectifing or deleting the data (Art.16).

Chapter 4

Analysis of commercial solutions in the scope of support of personal data processing

The entry into force of the Regulation not only forces companies to adapt to the new requirements, but also created a space for new business solutions that, by supporting compliance with GDPR, may be a new source of profit. One of the areas of business where the new regulations constitute a particularly important subject of interest is the GRC area. This area has no formal definition, while the acronym comes from the words *Governance*, *Risk* and *Compliance*. The lack of a formal definition results in the freedom to interpret this concept depending on the organization, but all boil down to the integration of these three elements, as well as the interaction between people, technologies and processes supporting them [22]. *Governance* defines the way of managing the organization and managing the risks, including their planning, use and counteracting them, *Risk* stands for identifying risks possible to occure based on the analysis of resources and processes in the organization, *Compliance* means fulfilling internal and external requirements, including provisions of legal acts, such as GDPR and industry guidelines [22].

The subject of the next chapter will be the presentation of changes implemented in business application operating in this area, which is why it is justified to present the analysis of solutions available in this field. This will allow one to formulate functional requirements and help to choose those which will not only adapt the application to the new regulations, but also make them a useful tool supporting the data controller in new duties.

4.1   RSA Archer GRC

RSA Archer GRC is an extensive, multi-functional business support system in areas such as policy, compliance or vulnerable risks management (GRC). This is software from the American company RSA dealing with computer and network security. An interesting fact about this company is the fact that its founders are the creators of the RSA public key encryption algorithm - Ron Rivest, Adi Shamir and Leonard Adleman.

RSA Archer GRC is a universal platform that can be expanded with various modules supporting individual areas of the company's operations. The system can be used freely to cooperate with other business products. It facilitates cooperation between business users from various fields such as IT, financial and legal industries. Provides user access

control, process automation or streamlining workflow. It allows to build own applications within the system, tailored to the individual needs of the organization.

In terms of GDPR compliance, it may be used as support in four main aspects which are:

- risk management - allows to catalog organizational hierarchies and business processes that process personal data. This allows to document in the registry the risks associated with critical business connections. It also allows reducing compliance gaps and introducing an effective risk mitigation strategies,

- compliance management - assistance in the area of compliance assessment, detection of possible compliance gaps and their tracking as well as implementation of proper corrective actions,

- supervision over data - thanks to the extensive control of users access to detailed data in the system, it is ensured that these users can only see the information intended for them,

- violation and information leaks management - it allows to catalog incidents of personal data breach and assess their scale of impact on security. Thanks to this, it allows to react appropriately on those incidents.

In the scope of supporting requirements according to GDPR, this system provide two solutions:

- RSA Archer Data Governance - module supporting the organization in identifying, managing and implementing appropriate controls regarding the personal data processing activities. It gives the opportunity to review the data retention schedules and provides the functionality of maintaining the expanded registry of processing activities. Supports the management of notices and consents for the processing of personal data.

- RSA Archer Privacy Program Management - module supporting the organization in grouping of processing activities in order to evaluate the impact of data protection and monitor communication with data protection authorities in relation to regulatory and data violations. It also allows you to assess the impact of these effects on privacy. Conducting such assessments is required in accordance with the provisions of Articles 35 and 36 of the GDPR.

4.2   SAP

SAP is an abbreviation of German *Systemanalyse und Programmentwicklung* what can be explained as Systems Applications and Products in Data Processing. It is a German IT company that is the world leader in the ERP (*Enterprise Resource Planning*) software market. As the first in the world, it has created a commercial ERP solution in the form of software, which is successfully implemented all over the world. Tools of this type are used to collect, analyze and use the acquired data to make optimized decisions. The SAP software is now so extensive that it covers every aspect of the company's operation. These tools effectively control many processes taking place in the enterprise.

SAP does not offer solutions dedicated exclusively to GDPR, but some of its products have built-in functionalities to support compliance with the new regulation. Examples of such solutions are:

- SAP GRC Access Control - the functionality of this software allows to effectively restrict and control access to data, including personal data or a specific data category. In addition, it allows to manage business roles by defining their attributes and acceptance paths for data that requires special control. In addition, it provides comprehensive protection of access to data through risk analysis or a comprehensive review and verification of this access for user accounts.

- SAP GRC Process Control - enables constant monitoring of the status of control, gives access to monitoring of extraordinary events in the scope of a special data category, allows to control the maps of GDPR requirements for organizations, checks effectivnes of reaction on risk.

- SAP GRC Risk Management - makes it possible to conduct an impact assessment on the protection of personal data, gives the possibility of full control over risk management in the field of data protection, makes available infringement reports storing data on materialized risk,

- SAP Information Lifecycle Management (ILM) - consists of two tools, the appropriate ILM and IRM (Information Retrieval Framework). The first is used to manage the retention of all data, including personal data. It provides easy deletion of personal data, for which legal basis for processing is no longer valid and allows to build rules of retention and destruction of this data. Ensures protection of access to archived data

4.3 Microsoft

Microsoft is an IT company founded in 1975 by Bill Gates and Paul Allen. One of the largest enterprises in the industry in the global market. Known mainly as a manufacturer of the Windows and MS-DOS operating system and Office suite. In addition to its flagship products, the company also deals with the creation of computer games, Xbox consoles, Visual Studio programming tools, media services such as the MSNBC news channel, provides a place in the cloud in the form of OneDrive service, as well as a computing platform by Azure, and a number of other solutions. In terms of business support, Microsoft offers a group of Microsoft Dynamics 365 products. They are used for customer relations management (CRM), enterprise resource management (ERP), material resource planning (MRP) and supply chain management (SCM). In terms of compatibility with GDPR, Microsoft offers a set of tools supporting the protection of personal data in its products:

- Data Loss Prevention for Office 365 - for identifing sensitive categories of data,

- Rights Management Services and Azure Information Protection - a tool used to protect documents and electronic correspondence. It allows for their encryption, labeling and classification,

- Advanced Threat Protection - protection in the field of isolation and scanning of electronic mailboxes in order to detect and protect against suspicious attachments,

- Microsoft Cloud App Security - management of access to applications and data in the cloud,

- Azure Backup - a supporting tool in data retention,

- Compliance Manager - monitors the state of implementation of Microsoft solutions in the area of data protection and compliance with legal requirements.

4.4   Analysis summary

The basic feature of all the above solutions is to ensure compliance of personal data processing with the new requirements resulting from GDPR. This is mainly done by analyzing the managed data set in terms of identifying personal data and detecting particulary sensitive data, as well as introducing data access management. Direct data protection is also a key aspect for each of the above examples. It is also extremely important to properly manage data retention and the ability of the system to select and delete, as soon as possible, selected personal data or those whose legal processing has already passed.

Both the RSA product and the SAP toolkit, whose task is to directly support the company, offer solutions dedicated to supporting data administrators in legal duties. In this respect, there are many different possibilities of different solutions, the selection of which depends on the individual needs of the company. The SAP toolbox as one of the most comprehensive tools for comprehensive support of the company offers a whole range of different solutions in this area, but they are built into larger modules, which can generate a redundant cost for the case of particular solution. RSA Archer GRC serves as a specialized tool for supporting organizations in the field of GRC and offers two specialist solutions in the field of supporting the administrator, such as modules for managing personal data processing activities. Microsoft does not offer any IT solutions dedicated to supporting data controllers, but it guarantees compatibility of its products with GDPR.

The smartGRC application being the subject of modification in the next chapter is used to support the company in the field of GRC, but it is not as extensive a tool as RSA Archer GRC, and even more so SAP products. Therefore, for her needs, the most justified choice is the implementation of support functionality in the registration of processing activities, which is the basis in both of the previously mentioned tools.

Chapter 5

Prototype of the application that supports compatibility with GDPR

The subject of this chapter is the application prototype, created on the basis of an existing business support tool called smartGRC. This application is a modular IT system that can work with various business systems and applications available on the market. From the mechanics side, it is a web application that works on the server and is available to users through the intranet of the organization in which it is implemented. Its main task is to control the use of IT systems used inside the company, in order to limit the attempts of abuses by users as much as possible. This process involves the processing of employees personal data, and hence, compliance with new regulations.

The construction of the prototype consisted of two stages. The first was to adapt the application to the new requirements regarding the processing of personal data by the application itself. It means analyzing the existing functionalities to determine the scope of personal data being processed, potential risks for their owners, their type, sensitivity, reasonableness of their processing and the level of their accessibility. Thanks to this, it is possible to specify which specific points of the regulation this processing applies to, and what mechanisms should be used to make this processing safe and legal.

The second stage was the implementation of features supporting compliance with GDPR. This means expanding the existing system with such functionalities so that it can be successfully used as a support in fulfilling the new legal obligations imposed on the data controller.

5.1 Application status before adapting to GDPR

The usefulness of the smartGRC application is based on its modular construction. Thanks to this, one can adapt this tool to different company's needs. The application includes the following modules:

- smartWorkFlow - a tool for managing user permissions in different systems and business applications, e.g. SAP,

- smartAccess - a tool that allows users in special situations to access an account with a wide range of rights in the SAP system. It also allows one to control the risk resulting from granting these rights through detailed logging of events from the use of this account,

- smartSoD - a tool allowing to analyze the distribution of duties, simulations and periodical reviews of entitlements,

- smartReport - a tool that allows one to generate personalized and customized reports on data in the system,

- smartArchitect - a tool that allows one to create and manage a roles catalog,

- smartReview - a tool that allows one to cyclically analyze the permissions held by users

Some of the above-mentioned tools support the compatibility with GDPR indirectly from the idea itself and not only from the need to adpat to new conditions. Managing privileged access, reporting risks arising from the segregation of duties, identifying people with too wide access to various systems, including the processing of personal data, all these concepts overlap in some part with the assumptions of the new regulation. This indicates how close the two areas are to each other, the protection of personal data and the support of the business on the field of GRC. However, the smartGRC system at the construction stage was not adapted to the requirements and direct support of compliance with GDPR, because it was created in 2008, 8 years before the adoption of new regulations. For this reason, the application had to be analyzed in terms of compliance with the new regulations in order to be able to continue to be a fully usable business support tool.

5.2   Adapting the application to compliance with GDPR

The first step of the analysis was to verify what data related directly to individuals are processed in the application. On this basis, a data set has been defined that contains:

- Basic data:

    – First name, last name, staff number, Active Directory identifier.

- Administration data (related to employee):

    – Organization unit, department, position, building code.

- Administration data (related to user account):

    – Login, Secure Network Communications login.

- Data related to usage of smartAccess account:

    – External employee.

- Address data:

    – Address, phone number, mobile number, e-mail, room number, floor number.

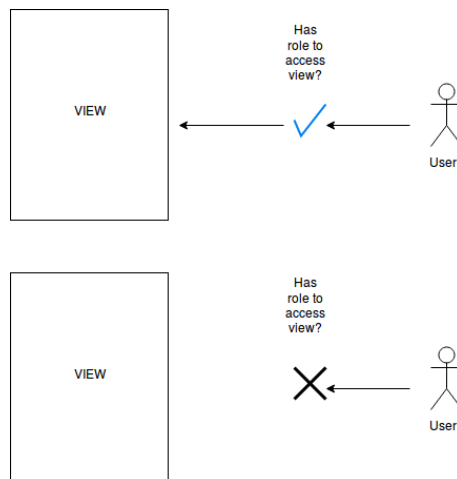Figure 5.1 Example of window for employee selection from list

Figure 5.2 Access authorization scheme using roles

After determining the set of all personal data appearing in the application, it was analyzed in relation to the places where any of this data is processed. From among about 180 views of the application, 36 were designated in which personal data are processed uncorrectly. Almost half of the cases was the possibility of unauthorized access associated with the windows of user or employee selection from the list, on which there are such data as login, name, surname, position, department, data of the superior (Fig. 5.1).

Based on this information, it became clear that the application has places where, despite the use of access control in the form of roles assigned to users by the administrator, data processing is not completely safe against the new regulations. These roles entitle users to whom they are assigned to access specific views (Fig. 5.2), or example to the administration of users accounts (Fig. 5.3). From this level, the authorized only by system role person can check the login history of a given user, he has also the option of administratively logging it out, however, he should not have access to data such as the name or surname of a given user without the administrator's authorization. In other words, for this purpose of processing personal data, in accordance with the principle of data minimization (3.2), it may not be necessary to know the name or surname of a person assigned to a given account.

Login ⌄	First name ☰	Last name ☰	Last login ☰ From: to:	Account's status ☰ All ⌄	Session's status ☰ All ⌄	Actions
testowy6	Jan	Testowy	2018-04-27 11:09	Active	Active	🔍 ✏️
testowy5	Jan	Testowy	2018-04-27 11:07	Active	Active	🔍 ✏️

Figure 5.3 Exemplary view of administrating users accounts

Therefore, an effective form of protection of personal data should be implemented against unauthorized access, it is explicitly stated in the art. 25 GDPR [4]. In addition, art. 32 provides that a person who has access to the processing of personal data may process it only at the request of the personal data administrator [8]. Therefore, beside the implementation of appropriate measures to secure personal data, it is also necessary to introduce functionality which will help to manage the access to the processing of personal data. At this point, it may also be useful to know who has granted such access and when. This is particularly important from the point of view of the accountability rule (3.2).

5.2.1   Pseudonymisation of personal data

The first step to bring the existing system to compliance is to put in place an effective data protection mechanism. Art 25 of the Regulation indicates the pseudonymisation of data as an effective form of such protection. Defining a set of personal data processed in the application indicates which data should be pseudonymised by default. Analysis of the places where this data is processed allows to conclude that the most sensitive places for personal data are several views in main application modules. This is the administration module responsible for managing employees and accounts in the system, the smartWorkflow module, due to the management of user permissions in the SAP system and smartAccess, due to the extensive event logging system of usage of the emergency account. In the mentioned modules, apart from the administration module, there is a high interaction between users at various levels of authority (e.g. user-controller, applicant-approval etc.).

The modular structure of the application also requires the introduction of a pseudonymisation configuration that allows flexible definition of the data to be protected (Fig. 5.4). This is important because each of the modules processes personal data to varying degrees, which is related to the scope of data needed for processing for a specific purpose (3.2). Access to this configuration is provided for the administrator by giving him an appropriate role (Fig. 5.2) in the system, entitling him to access the configuration panel.

Figure 5.4 View of pseudonimization configuration

According to the default privacy rule, in the default configuration all fields will be checked, which means that unauthorized users will not have access to any of these data in the application. This configuration is global for the entire application, which means that one setting is then used for each user in each application location. In the future, however, it is expected that this functionality will be expanded to include the option of selecting users to assign this configuration.

As regards the pseudonymisation process itself, the Regulation does not mention the best pseudonymisation methods. However, the Working Party, which is an independent European advisory authority in the field of personal data protection, indicates the most common methods of pseudonymisation [24].

In this case, pseudonymisation is realized by substitute the data with the string of asterisks ("*") (Fig. 5.5). This is done at the application logic level so that the user is not able, for example, to view the actual data in the browser's development tool. All data on which the application operates, including personal data, is stored in the database. When needed, the application logic loads them into the variables in model object (e.g. employee model). From this level, proper or pseudonymised data may be obtained depending on the user's rights and the configuration of the pseudonymisation. Below is an example of getting the name from the model:
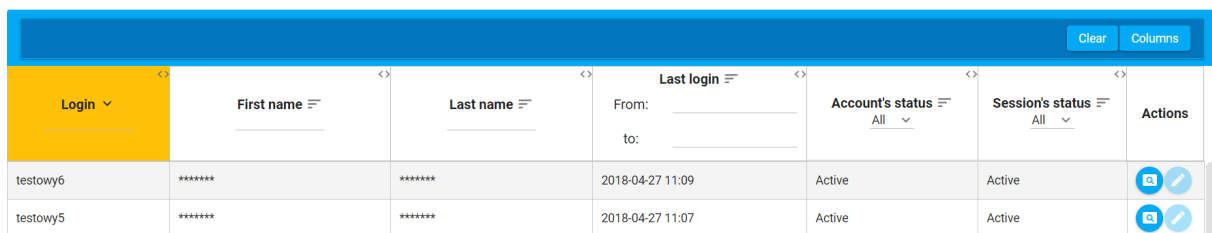
```
func getNameSecured()

        if permission to access the data
                return nameVariable
        else
                return "*******"
endfunc
```

These functions are used only in places where data is taken from the model directly to the given view. In addition to these special functions, the model also has ordinary functions that take the value directly from the variable regardless of the permissions or

configuration:

```
func getName()
        return nameVariable
endfunc
```

The duality of such data extraction is related to securing the case of using the same functions at the moment of retrieving the value to the view and saving it in the database. In this case, it could happen that the given pseudonymised data will be saved in the database in the place of the correct value.

Login ˅	First name ≡	Last name ≡	Last login ≡ From: to:	Account's status ≡ All ˅	Session's status ≡ All ˅	Actions
testowy6	*******	*******	2018-04-27 11:09	Active	Active	
testowy5	*******	*******	2018-04-27 11:07	Active	Active	

Figure 5.5 Exemplary view of administrating users accounts with pseudonimization included

5.2.2   Managing access to the personal data

In the next step, one need to ensure that the application is compatible in the terms of the access to the processing of personal data. The configuration of pseudonymisation from the previous step provides the data controller with global control over the degree of confidentiality of personal data. In order for him also to have proper control over the distribution of permissions to the processing of personal data, it was necessary to implement the appropriate interface in the application, which will allow to determine to whom and for what period of time the rights will be granted. It was also important from the point of view of compliance with the accountability rule (3.2) in order to be able to prove that the processing of personal data occurred only under the authority of the administrator.

This interface was implemented by creating a register with access only for the administrator or authorized person on the basis of assigning the appropriate role in the system. From its level, the administrator can grant permissions to selected users for a selected period of time, as well as delete the granted permissions (Fig. 5.6). In addition, in the panel of a given user account, the history of granted access to personal data processing has been added in the form of a list containing all data about granted permission (Fig. 5.7).

Personal data access managing

Figure 5.6 Registry panel of entitled to personal data processing

Figure 5.7 The history of the user's accesses to processing of personal data

To increase the level of security, full access to personal data and their processing may take place if the user has (Fig. 5.8):

- the appropriate role in the system that allows access to a specific view (earlier functionality),

- access granted by the administrator via the panel of access to the processing of personal data (new functionality),

- assignment to a specific consent in the system, which is the legal basis for the processing of personal data. In the absence of this consent, an error message appears in the administrator's panel for granting personal data processing permissions (new functionality).
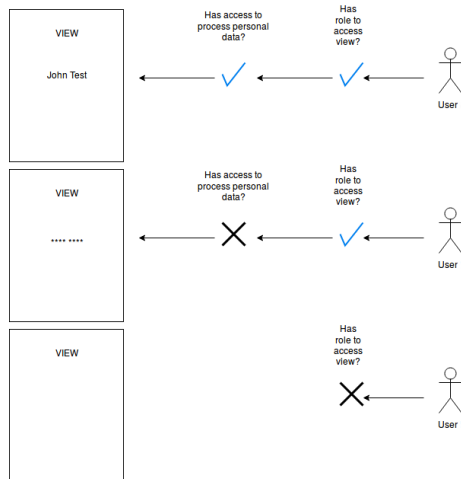
Figure 5.8 New access authorization scheme using roles and permission for data processing

After adding the user to the list of persons authorized to process personal data. information about this access is stored in the user's session and refreshed each time the user sends a request to the server (e.g. he will want to go to the next view). Refreshing this information is so important that data should be protected as soon as possible after the expiration of the access to processing.

5.2.3   Logs

The final stage of application adaptation was the expansion of system logs. This functionality involved capability for recording of information on any changes introduced in both the configuration of pseudonymisation, as well as the granting and deleting by the administrator of access to the processing of personal data. Logs of these events are equally important from the point of view of the accountability rule, as keeping the register of privileges granted. However, in this case, information about who and when made the change is saved, as well as the range of values that have changed (in the case of pseudonymization configuration).

Figure 5.9 Example of recorded log after granting permission to the processing of personal data

5.3 New module supporting compliance with GDPR

New obligations imposed on personal data administrators create a space for new solutions in this area. One of such new duties is the registration of processing activities [5]. It is imposed on every enterprise or entity that employs more than 250 people, or where the purpose for which it processes personal data may carry the risk of violating the rights of such persons. Such a register must also be kept if the processing is not occasional, it involves the processing of a specific category of personal data or personal data regarding court judgments.

This register is required for two reasons. The first is direct compliance with article 30 of GDPR. The second is to allow the supervisory authority to verify the processing carried out. For enterprises using business support of the GRC area, this is particularly important. Apart from the fact that it is possible to employ over 250 people, personal data may be processed there in many different systems, and each such system must have properly cataloged personal data.

In the case of the smartGRC application, this is an important fact because significant part of its functionality is based on cooperation with other business applications that process personal data in various systems. The development of the smartGRC system with a register of processing activities is therefore fully justified by the considerations of both the application area itself and its competitiveness on the market. This tool is the basis for the successive development of a new application module that is smartGDPR.

5.3.1 Register of processing activities

The analysis of available market solutions from the previous chapter showed that the degree of complexity of this tool may be different depending on the needs of the application in which it was implemented. Although the register of processing activities according to assumptions has the form of a simple form for collecting specific information divided into sections, it must be sufficiently detailed and at the same time legible and easy to use in order to be able to effectively fulfill its task. For the needs of the smartGRC application, the functionality of the processing activity register needs to be fulfilled with the information like:

- Basic information:

    - Number, name and description of registry,
    - person adding the registry,
    - time of adding,
    - person modifing the registry,
    - time of modification,
    - status.

- Stakeholders:

    - Data controller,
    - processing entity,
    - data protection officer.

- Scope of processing data:

  - Purpose of processing,

  - description of processing operation,

  - role in the processing,

  - legal basis,

  - methods of aquiring data,

  - methods of transferring data to processors,

  - information about third-party companies,

  - information about transmitting data to third countries or international organizations (including names of coutries and organizations)

  - processed categories of data,

  - categories of data audience related to processing,

  - specification of categories of people whose data concern,

  - retention period,

  - way of proceeding after the retention period,

  - information about the high risk of violation of the rights and freedoms of natural persons,

  - information on the required performance of data protection impact assesment,

  - related business processes,

  - inforamtion on applications / systems.

- Security identification:

  - policies,

  - control procedures,

  - technical security,

  - organizational security.

For the register to be complete, each of the information must be provided. The completed processing activities form after approval is saved in the database.

5.3.2 Dictionary

The dictionary serves as a repository of values used in the form for adding a new processing activity. There is constant set of fields in it to which, required values are assign. Each of this fields is easy to editing. But only authorized person, which is designate to completion the register of processing activities by administrator, is able to access it. Below the set of editable fields, that are used in the register:

1. Business unit,

2. third parties,

3. company,

4. department,

5. purpose of processing,

6. role in the processing,

7. legal basis,

8. methods of aquiring data,

9. methods of transmitting data,

10. categories of processed data,

11. categories of data audience,

12. categories of persons which data concer,

13. way of proceeding after retention period,

14. applications / systems,

15. processing entity - third parties,

16. representative,

17. policies,

18. control procedures,

19. technical securities,

20. organizational securities.

The essence of application of this dictionary was to improve the completion of processing activities registry. Because of the amount of data that needs to be entered into the form, writing everything by hand would be too cumbersome. This process has been improved thanks to the use of a dictionary that can be completed both from the interface of the dictionary itself and when filling out the form. One can assign specific values to each field, depending on the needs of the organization that uses this tool.

5.3.3 Further development prospects

In the future, a significant expansion of this module is expected. The analysis of similar, commercial solutions has shown that in order to be more competitive on the market, one must also take care of the development of reporting tools that analyze the risks associated with the processing of personal data or record incidents of personal data breach. Therefore, the smartGDPR module provides for the following functionalities:

1. Construction of a repository based on the processing activity register and processing category register,

2. categorizing the risk of personal data processing,

3. extensive reporting,

4. periodic risk verification based on surveys,

5. register of incidents related to the management of personal data.

Chapter 6

Conclusions

According to the privacy by design principle, the protection of personal data of application users should be taken into account at the system design stage. In the case of systems processing personal data built before the entry into force of the new regulation, it is for obvious reasons impossible. Therefore, in order for such a system to continue to play its role, it should be adjusted accordingly to the new requirements. At this stage, it is important to precisely determine how data processing has taken place in this system so far. It is also important to determine to what extent personal data are processed, what are the categories of data, what risk for data subjects carries this processing, and above all, whether the application is processing an acceptable range of data resulting from the purpose of processing. One should also verify who has access to this data. It is only the set of all these parameters that allows to specify the appropriate requirements to be implemented so that the application can process data with compliance to GDPR. In particular, that the GDPR directly indicates the mechanisms that allow compliance with certain requirements. In the case of smartGRC application, the problem was the scope of data necessary for processing, as well as broad access to them without verifying the validity of this access. In addition, the application did not meet the requirements of the privacy by default principle, and the data could be processed without the administrator's authorization. Only the implementation of a pseudonymisation mechanism controlled by the administrator in combination with the possibility of granting by him the right to process data, as well as the extension of logging mechanisms and the history of access to personal data processing made it possible to meet these requirements.

Administrator support in fulfilling the duties contributes to the greater usability of the application, so from a business point of view it is a favorable direction of application development. The analysis of the regulation itself in this respect brings immediately several solutions, confirmed by the analysis of other commercial products. One of them is a register of processing activities, which must be kept by each administrator in certain circumstances. Considering that the smartGRC application is used to cooperate with other business applications that process personal data, implementing the mentioned registry is fully justified. However, there will certainly be other possibilities of solutions that are worth implementing in this type of applications, which will result from familiarity with administrators with new responsibilities.

Chapter 7

Summary

The rapid development of technology gives us more and more opportunities in the processing of information. Many of the everyday devices have embedded computers in them so that they can serve us better. The Internet gives us great access to data, communication and information transfer. All these devices that facilitate our lives, thanks to the Internet access, provide us with even more convenient services. The amount and scope of data collected for the needs of these services makes the seemingly insignificant everyday activities that we perform using these useful devices generate a lot of confidential information about us. By analyzing everyday behaviors, one can determine which products or services you are more likely to spend money on. Analyzing our social behavior can determine what our views are, with whom and where we like to spend time, or what our habits are. This data in unauthorized possession creates a serious threat for both the individual and society as a whole. This is particularly problematic when it comes to business entities, especially those whose business model is mainly based on the provision of services related to the processing of personal data.

The law in this area has been regulated in some way already some time ago to protect the privacy of people. However, we live in a time when the speed of technological development is much greater than the ability to adapt provisions and regulations to it. In the absence of appropriate legal restrictions, the scale of uncontrolled acquisition and processing of personal data has increased to unprecedented proportions. This has triggered the need to introduce appropriate regulations that will not only ensure greater security for individuals, but will limit the possibilities of redundant acquisition and processing of personal data, and will be general and universal enough to keep up with the rapid technological changes.

This work addresses the issue of supporting the processing of personal data based on an IT system in a company in the face of the new GDPR regulation. This legal act aims to adapt legal requirements to the current state of technological, social and political development. It introduces a number of mechanisms that are to safeguard the privacy of data subjects, reduce the pointless collection of personal data by various entities, and improve the cross-border flow of data.

The result of this work is the prototype of the application created on the basis of the existing IT system that processes personal data, which has been adapted not only to meet the new legal requirements, but also supports the entity that processes personal data in new legal obligations. In order to achieve this goal, it was necessary first of all to analyze the changes that took place in the law after the new regulations came into force. On the basis of this analysis, it was possible to determine in which aspects the previous system does not comply with the new regulation. It also allowed to define the requirements nec-

essary to implement in the prototype so that it could continue to fulfill its function. The analysis of the new provisions has also helped to determine what are the new obligations imposed on the data controller, and the analysis of existing, commercial market solutions in this area, indicated the best practices in supporting the administrator in these duties. The result is a new module being the basis for further development. Functionality in the new module supports the administrator in fulfilling the obligation to document the processing of personal data.

In the future, this module may be extended with other functionalities. For example a register of categories of operations related to processing, i.e. types of services that the processor performs on behalf of particular administrators, or a system for verifying the legitimacy of processing personal data.

Chapter 8

Abstract in Polish

Cel i zakres pracy

Niniejsza praca porusza problematykę przetwarzania danych osobowych w przedsiębiorstwie wobec nowego rozporządzenia RODO (*Rozporządzenie Ogólne o Ochronie Danych Osobowych*). Dotyczy ono przetwarzania a także ochrony danych osób fizycznych a podlegać mu będą wszystkie organizacje, firmy, oraz przedsiębiorstwa, które na swoje potrzeby przetwarzają dane osobowe.

W pracy tej zostają omówione podstawowe zagadnienia dotyczace danych osobowych, od definicji, przez genezę ich prawnej ochrony, status przepisów w Polsce przed wejściem w życie rozporządzenia RODO aż po omowienie najważniejszych zmian jakie wnoszą nowe przepisy. Następnie przeanalizowane zostaną dostępne na rynku komercyjne rozwiązania, które pozwolą określić jakie funkcjonalności mogą zapewnić zgodność z RODO a także jakie są oferowane narzędzia do wspierania administratorów danych. Część projektowa tej pracy obejmuje dostosowanie istniejącego systemu informatycznego przetwarzającego dane osobowe do zgodności z RODO, a także wprowadzenie w nim nowych funkcjonalności które pozwolą na wsparcie administratórów danych w ich nowych prawnych obowiązkach.

Wejście w życie nowego rozporządzenia wnosi wiele zmian w zakresie przetwarzania danych osobowych, które wymagają od podmiotów przetwarzających takie dane spełnienie określonych wymagań. Powodem wprowadzenia nowych przepisów, jest gwałtowny rozwój technologiczny, społeczny oraz polityczny na świecie. Coraz większa moc obliczeniowa komputerów pozwala przechowywać i przetwarzać coraz więcej danych z coraz większą prędkością. Komputeryzacja urządzeń codziennego użytku, oraz ich zdolność do wymiany danych przez internet, skutkuje zbieraniem coraz większej ilości danych o ich użytkownikach. Stwarza to zagrożenie dla prywatności jednostki, ponieważ traci ona kontrolę nad ochroną dostępu do swoich personalnych danych. Wiele przedsiębiorstw opiera swój model biznesowy na przetwarzaniu takich danych osobowych. Nowe rozporządzenia ma na celu zapobiegać sytuacjom nadużyć w zakresie przetwarzania danych osobowych, chronić prywatność podmiotów danych w możliwie największym stopniu, a wobec politycznego rozwioju Unii Europejskiej także usprawniać transgraniczny przepływ tych danych.

Ochrona danych osobowych

Dane osobowe stanowią bardzo wysoką wartość w dzisiejszym świecie. Wiele różnych przedsiębiorstw przetwarza dane osobowe w celu osiągania profitów. Przykładem niech będą firmy marketingowe, które na podstawie zachowań ludzi są w stanie dopasować

reklamy do tego, aby były jak najatrakcyjniejsze dla potencjalnych nabywców różnych produktów bądź usług. Kosz takich danych jest zależny od rodzaju dostarczanych informacji. Im bardziej precyzyjne dane, tym koszt jest większy. Dane osobowe mogą służyć także do celów politycznych, aby na podstawie poglądów politycznych zachęcić do głosowania na daną opcję polityczną. Dlatego też, aby uniknąć niekontrolowanego wykorzystania tych danych z negatywnymi skutkami dla ich właścicieli tak ważna jest ochrona danych osobowych.

Ochrona danych osobowych ma swoje źródła w rozważaniach filozoficznych. Pierwsze poważne artykuły odnoszące się do prawa do prywatności pojawiły się u schyłku XIX w. Przepisy prawne odnoszące się bezpośrednio do ochrony danych osobowych są stosunkowo nowe i pojawiły się w drugiej połowie XX wieku na terenach państw europejskich. W historycznych aktach prawa międzynarodowego XX wieku, ochrona danych osobowych była raczej "dodatkiem" do przepisów o ochronie prywatności. Akty takie zaczęły pojawiać się w Europie w połowie XX wieku.

W prawie Polskim przed wejściem RODO, ochronę danych osobowych ragulowały głównie Konstytucja Rzeczypospolitej Polski oraz Ustawa o Ochronie Danych Osobowych, obie z 1997 roku. W związku z przystąpienie Polski do Unii Europejskiej, należało dostosować to prawo do obowiązującej w Europie Dyrektywy 95/46/WE za pomocą szeregu poprawek.

RODO

Rozporządzenie RODO zostało uchwalone jako Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Powstała jako odpowiedź na rosnące przemiany w zakresie technologii, przemian społecznych i politycznych na terenie Unii Europejskiej. Przepisów tych muszą przestrzegać wszystkie podmioty przetwarzające dane osobowe.

W zakresie definicji danych osobowych, RODO doprecyzowuje ją względem wcześniejszych definicji a także wprowadza i precyzuje nowe pojęcia takie jak dane biometryczne, dane genetyczne czy pseudonimizacja danych.

Opiera ogólne zasady przetwarzania danych osobowych na regułach takich jak zgodność z prawem, rzetelność, klarowność, ograniczony cel przetwarzania danych, minimalizacji danych, poprawność danych, ograniczone przechowywanie danych, integralności i poufności danych a także rozliczalność.

Wprowadza nowe obowiązki informacyjne dla administratorów danych, które przewidują jasny, zwięzły i prosty sposób informowania podmiotów danych o tym w jakim celu i w jaki sposób ich dane będą przetwarzane. Daje właścicielom danych osobowych prawa do bycia poinformowanych o czynności przetwarzania, do dostępu do danych, do sprostowania/uzupełnienia danych, do bycia zapomnianym, do ograniczena przetwarzania, do transferu danych, do sprzeciwu a także do niepodlegania automatycznym decyzjom.

Określa podstawy prawne na jakich przetwarzanie może się odbywać. Jedną za takich podstaw jest zgoda podmiotu danych, która powinna być wyrażona dobrowolnie a także w odpowiedniej formie, potwierdzającej świadomość osoby wyrażającej zgodę na przetwarzanie danych.

Nakłada na administratorów danych obowiązek wprowadzenia odpowiednich środków organizacyjnych i technicznych w celu ochrony danych przed zniszczeniem, nieuprawnionym

dostępem czy modyfikacją. Wymienia środki ochrony takie jak autoryzacja, ochrona firewall, szyfrowanie danych osobowych, tworzenie kopii zapasowych, pseudonimizację czy anonimizację.

Nakłada na administratora danych bezpośredni obowiązek dokumentowania przetwarzania danych osobowych w formie rejestru czynności przetwarzania, określając precyzyjnie, jakie informacje w takim rejestrze musza się znaleźć. Ma to umożliwić organowi nadzorczemu wgląd w proces przetwarzania danych u danego podmiotu.

Wprowadza zasady prywatności w fazie projektowania a także domyślnej prywatności, które mają skutkować skuteczną ochronę danych osobowych już w fazie planowania projektu zakładającego przetwarzającego dane osobowe.

Nakłada na administratorów danych obowiązek informowania organu nadzorczego o incydencie naruszenia ochrony danych osobowych w czasie do 72 godzin od momentu wykrycia incydentu. Nakazuje także wprowadzenie odpowiednich środków umożliwiających jak najszybsze wykrycie takiego incydentu. W momencie powstania ryzyka naruszenia praw i wolności podmiotów danych nakazuje także bezzwłoczne ich powiadomienie.

Za bardzo poważne naruszenia przepisów nowe rozporządzenie przewiduje kary rzędu 20 000 000 EUR albo 4% całkowitego światowego obrotu za roku poprzedni w zależności co większe. Za mniej poważne naruszenia przepisów, przewidywana jest kara 10 000 000 EUR lub 2% całkowitego światowego obrotu za rok poprzedni, w zależności co większe.

Analiza komercyjnych rozwiązań w zakresie wspierania przetwarzania danych osobowych

Wejście w życie nowego rozporządzenia o ochronie danych osobowych stworzyło przestrzeń dla nowych rozwiązań biznesowych. Jednym z takich obszarów jest GRC (ang. *Governance, Risk and Compliance*). W tym rozdziale zostaną omówione rozwiązania firm RSA oraz SAP z tego zakresu, oraz rozwiązania firmy Microsoft wdrażające zgodność z RODO.

Produkt RSA Archer GRC od firmy RSA, jest wielofunkcyjnym, modularnym wsparciem przedsiębiorstwa na polu GRC. Umożliwia on zarządzanie politykami organizacji, ryzykiem związanym z procesami oraz zasobami przedsiębiorstwa, a także wspomaga zgodność. W zakresie dostosowania do wymagań RODO, oprócz wymienionych cech, umożliwia także sprawny nadzór na danymi oraz zarzadzanie naruszeniami ochrony danych osobowych oraz incydentami wycieku informacji. W zakresie wspierania zgodności organizacji z RODO oferuje możliwość zarządzania i wdrażania odpowiednich kontroli związanych z czynnościami przetwarzania danych osobowych. Wspomaga to wywiązywanie się administratora danych z obowiązku prowadzenia rejestru czynności przetwarzania.

Firma SAP dostarcza kompleksowych rozwiązań we wspomaganiu każdego aspektu działalności firmy. Oferuje jedno z najbardziej rozbudowanych i zaawansowanych narzędzi tego typu dostępnych na rynku. W zakresie wsparcia zgodności z RODO nie udostępnia żadnych dedykowanych narzędzi, ale całe moduły funkcyjne, głównie z zakresu GRC, które mają wbudowane funkcjonalności wspierające spełnianie poszczególnych wymagań RODO. Moduły te posiadają takie funkcje jak zarządzenie dostępem do danych, monitoring nadzwyczajnych zdarzeń w zakresie wrażliwych danych, prowadzenie oceny wpływu na ochronę danych osobowych, raportowanie zmaterializowanego ryzyka, czy zarządzanie retencją danych.

Firma Microsoft nie udostępnia rozwiązań IT dedykowanych dla administratorów danych do wspierania zgodności z RODO, natomiast jej produkty są dostosowane do wymogów wynikających z nowego rozporządzenia w zakresie identyfikacji danych os-

obowych i wrażliwych, zarządzaniu dostępem do aplikacji oraz danych, a także wspieraniu zarządzania retencją danych.

Prototyp aplikacji wspierającej zgodność z RODO

Jest to rozdział poświęcony projektowej część niniejszej pracy. Przedstawia on aplikację smartGRC, która na potrzeby tej pracy została dostosowana do wymogów RODO oraz rozbudowana o narzędzia wspierające zgodność z nowym rozporządzeniem. Aplikacja jest modularnym systemem, podobnym pod względem funkcjonalności do narzędzia RSA Archer GRC. Jej działanie polega na zarządzaniu dostępem użytkowników do różnych systemów, wsparciu w analizie ryzyk, rozbudowanemu raportowaniu, prowadzeniu przeglądów okresowych z danych zawartych w systemach. Daje dostęp do konta awaryjnego w systemie SAP. Wszystkie te funkcjonalności wiążą się z przetwarzaniem danych osobowych pracowników.

W celu dostosowania aplikacji do nowych wymogów przeprowadzono inwentaryzację aplikacji pod kątem typu przetwarzanych danych a także miejsc w których te dane są przetwarzane. Analiza ta pozwoliła ustalić, że aplikacja nie zapewnia wystarczającej ochrony pod względem nieautoryzowanego dostępu do danych osobowych, a także może naruszać zasady minimalizacji danych. W związku z tym należało dobrać odpowiednie mechanizmy i funkcjonalności, dzięki którym aplikacja będzie zgodna z wymogami bezpieczeństwa. W celu ochrony danych przed nieautoryzowanym dostępem, wprowadzono możliwość określania co jest daną osobową w aplikacji, spośród wszystkich typów danych zebranych w czasie analizy. Wybór ten odbywa się z poziomu wygodnego panelu administratora. Po określeniu co jest daną osobową, żaden nieuprawniony użytkownik w aplikacji nie ma do niej dostępu, poprzez zastosowanie mechanizmu pseudonimizacji tej danej. Dodatkowo stworzony został panel administratora, pozwalający nadawać uprawnienia do przetwarzania tych danych. Nadanie takiego uprawnienia wykonuje się poprzez dodanie wybranego użytkownika spośród wszystkich kont w systemie, na określony okres, do listy osób uprawnionych do przetwarzania danych osobowych. Dopiero po tej czynności, użytkownik może swobodnie przetwarzać dane osobowe w sytemie. Każde przypisanie, wiąże się z wpisem do historii nadania dostępów w aplikacji, co jest łatwo dostępne z widoku konta danego użytkownika systemu. Wszystkie te operacje, czyli konfigurowanie danych osobowych w systemie oraz nadawanie użytkownikom dostępu do przetwarzania danych jest odpowiednio logowane w dzienniku systemowym, co wspiera zgodność z zasadą rozliczalności.

Kolejnym krokiem była rozbudowa aplikacji o narzędzia wsparcia administratora danych osobowych w wypełnianiu nowych obowiązków prawnych. Polegała ona na zaimplementowaniu rejestru czynności przetwarzania. Poszczególną czynność przetwarzania dodaje się do rejestru po uprzednim wypełnieniu formularza wymaganymi danymi. Odpowiednio wypełniony formularz trafia do bazy danych. Każdy taki formularz rejestruje dane na temat osoby wypełniającej/modyfikującej. Wsparciem tego rejestru jest słownik, który zawiera pola wymagane przy wypełnianiu formularza. Do każdego z tych pól uprawniona osoba może dodawać wedle potrzeb organizacji określone wartości, które potem będą mogły być użyte w formularzu. Ma to usprawnić proces dodawania wpisów do rejestru.

Wnioski

Zasada prywatności w fazie projektowania przewiduje ochronę danych osobowych już w momencie planowania nowego projektu który zakłada przetwarzanie danych osobowych. Systemy będące w użyciu przed wejście w życie nowego rozporządzenia z oczywistych względów mogą być niezgodne z tą zasadą. Ponadto mogą naruszać podstawowe zasady przetwarzania danych przewidziane w RODO. Dlatego też, aby takie narzędzia mogły dalej pełnić swoją rolę muszą zostać odpowiednio dostosowane. Przystosowanie takiej aplikacji do zgodności z nowymi przepisami wymaga przeprowadzenia analizy pod kątem ustalenia punktów niezgodności, określeniu nowych wymagań, dobraniu mechanizmów oraz funkcjonalności które przystosują tę aplikację do spełniania wymogów nowego rozporządzenia. Rozbudowa narzędzi klasy GRC o rozwiązania wspierające administratora w spełnianiu obowiązków względem RODO jest zasadna ze wzgledu konkurencyjności takiego narzędzia na rynku a także pokrewieństwa naturalnego obszaru jej działania z obszarem na które wpływa RODO.

Bibliography

[1] Act of 29 august 1997 on the protection of personal data (Dz.U. nrJournal of Laws No. 133, item 883).

[2] Art.04 of the regulation of the european parliament and of the council (eu) of 27 april 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of directive 95/46/ec (general regulation on data protection)[...] (Official Journal of the EU, L 119/1).

[3] Art.09 ibidem.

[4] Art.25 ibidem.

[5] Art.30 ibidem.

[6] Art.32 ibidem.

[7] Art.32 ibidem.

[8] Art.32 ibidem.

[9] Article 27 of the act of august 29, 1997 on the protection of personal data (Journal of Laws No. 133, item 883).

[10] Article 51 of the constitution of the republic of poland of april 2, 1997 of the act of august 29, 1997 on the protection of personal data (Dz.U. nr 78, poz.483Journal of Laws No. 78, item 483 with changes to the law on the protection of personal data).

[11] Article 6 of the act of august 29, 1997 on the protection of personal data (Journal of Laws No. 133, item 883).

[12] 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 (Official Journal of the EU, L 281/31).

[13] Genereal Inspector of Personal Data Protection: Law reform - current work. https://www.giodo.gov.pl/pl/1520281/10255. Access: 2018-22-03.

[14] Preamble to the regulation of the european parliament and of the council (eu) of 27 april 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of directive 95/46/ec (general regulation on data protection)[...] (Official Journal of the EU, L 119/1).

[15] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, and J. Łuczak. *Personal Data Protection Law.* 2016.

[16] J. Borecka. The genesis of the legal protection of personal data and the concept of personal data. *SCIENTIFIC SUBSIDIES of the Institute of Administration of the Academy Jan Długosz in Częstochowa*, 2006.

[17] L. Czujko. Rodo - nowe obowiązki informacyjne wobec podmiotu danych | deloitte. `https://www2.deloitte.com/pl/pl/pages/financial-services/articles/newsletter/finanse-i-bankowosc-grudzien-2017/RODO.html`, Dec 2017.

[18] K. Julisch. Gdpr-privacy by design and by default | deloitte switzerland. `https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html`, Jan 2018.

[19] J. Labuz. Rodo: Więcej praw dla osób fizycznych i więcej obowiązków po stronie przetwarzających dane osobowe | deloitte. `https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/newsletter-rodo0/wiecej-praw-dla-osob-fizycznych-i-wiecej-obowiazkow-po-stronie-przetwarzajacych-d html`, Apr 2018.

[20] LexDigital. Ochrona danych osobowych - nowe zasady rodo. `https://lexdigital.pl/ochrona-danych-osobowych-nowe-zasady-rodo`, Jun 2018.

[21] M. Młotkiewicz and A. Kaczmarek. Tips and explanations regarding the obligation under art. 30 para. 1 and 2 GDPR. `https://giodo.gov.pl/pl/1520281/10449`. Access: 2018-20-06.

[22] A. Partyka. GRC - terra incognita? *Magazyn informatyki śledczej i bezpieczeństwa IT*, 35, Sep 2017.

[23] B. Schneier. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* 2017.

[24] R. Stępniewski. Pseudonimizacja według rodo - o czym należy wiedzieć? `https://www.politykabezpieczenstwa.pl/pl/a/pseudonimizacja-wedlug-rodo-o-czym-nalezy-wiedziec`, Aug 2017.

[25] M. Surdyn. Zgoda na przetwarzanie danych osobowych według rodo. `https://blog-daneosobowe.pl/zgoda-przetwarzanie-danych-osobowych-gruncie-rodo/`, May 2018.

List of Figures