

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:

Contents

1	Purpose and scope of work	3
1.1	Description of the problem	3
2	Personal data protection	7
2.1	Personal data as a value	7
2.2	Genesis of personal data protection	8
2.3	Historical acts of international law	8
2.4	Status in Poland before GDPR comes into force	9
3	GDPR	11
3.1	Personal data according to GDPR	11
3.2	Principles of data processing and their scope	12
3.3	Information obligations and the rights of the data subjects	13
3.4	Consent to the processing of personal data	14
3.5	Security	15
3.6	Documentation of processed data	16
3.7	Rules of privacy by design and privacy by default	17
3.8	Data protection violations and impact assessments	17
3.9	Cross-border data processing	17
4	Analysis of commercial solutions in the scope of support of personal data processing	19
4.1	RSA Archer GRC	19
4.2	Microsoft GDPR	19
4.3	SAP	19
5	Prototype of the application that supports compatibility with GDPR	21
5.1	Application status before adapting to GDPR	21
5.2	Adapting the application to compliance with GDPR	22
5.2.1	Pseudonymisation of personal data	23
5.2.2	Managing access to the personal data	24
5.2.3	Logs	25
5.3	New module supporting compliance with GDPR	26
5.3.1	Register of processing activities	26
5.3.2	Dictionary	28
6	Conclusions	29
7	Summary	31

Bibliography	31
List of figures	34

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 [11]. 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 purposes 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 position 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 ourselves 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 business 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 highlighted 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 business 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 development 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 measures applying 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 GODO 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 [11].

Accountability rule also assumes demonstration by the administrator of compliance with the law. It could be realized, for example, by documentation of implemented legal instruments 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 occurring 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 [9]. 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 physical, 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 your real identity there.

One can meet the term 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 business. The more precise these data are, the more valuable are they. For example, same 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 [20].

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 millions petabytes or 30 millions of dollars every year [20]. Over the years 2011 and 2015 cost of storage 1 petabyte of data decreased from 1 million USD to 100 000 USD [20]. 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 [14]. 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 [14]. 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 [14].

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 Parliament from 1970, on the union level, and Swedish law from 1973 on the state level [13]. 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 institutions, French law on informatics, files and civil liberties 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 [13].

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 Assembly 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 [13]. 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.

Although these two documents regulated much wider aspects of human rights protection, they significantly influed the legal basis for the protection of personal data [13]. The most important UN resolutions from the point of view of personal data protection are resolutions 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 life excluding cases justified legally, socially or economically from the point of view of the state [13].

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 requirement 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. [13]. 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 [13].

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 [8]. 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 information, 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 [13]) and specific 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 [13]). 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 measures 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.

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 amendments were introduced, which implemented the current European directive 95/46/WE [13]. After these changes, three more amendments 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 GODO 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 movement 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 [12]. 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 progressive 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 movement between Member States. Ensure consistency and uniformity in application of these principles in Member States, and to make protection of natural persons independent from applied techniques to reduce the risk of circumvention as much as possible [12]. The new regulation gives special protection to children, motivating this with their less awareness of the risks associated with the processing of personal data. 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 [10] 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* [7] while the GDPR uses the concept of *specific data category* [3]. A novelty in the collection of these special categories of data is the precise 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 affiliation, party affiliation, information on judgments 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, succinctly 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 acquiring data may not exceed the amount necessary 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 slightly 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 unauthorized 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 necessary. 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 recommended by Article 29 Working Party GDPR [15]. 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 information 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 strengthens 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[11]:

- *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 [16]. 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 [16].

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 [16].

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 [16].

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 [16]. 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 unambiguous 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 [22].

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 [22]. 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 [22].

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 [22].

The voluntary 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 voluntary character, for example [22]:

- making contract performance conditional upon consent, even though processing of personal data is not necessary for that,
- refusal of consent is subject to legal consequences,
- 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 [17]:

- *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 (3.9) 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 [18]. 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

3.8 Data protection violations and impact assessments

3.9 Cross-border data processing

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 [19]. *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 occur 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 [19].

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

4.2 Microsoft GDPR

4.3 SAP

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 information system that can work with various business systems and applications available on the market. 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 you 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 adapt 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.

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. 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, for example to the administration of users accounts

Login ▾	First name ▾	Last name ▾	Last login ▾	Account's status ▾	Session's status ▾	Actions
testowy6	Jan	Testowy	2018-04-27 11:09	Active	Active	
testowy5	Jan	Testowy	2018-04-27 11:07	Active	Active	

Figure 5.1 Exemplary view of administrating users accounts

(Fig. 5.1). 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.

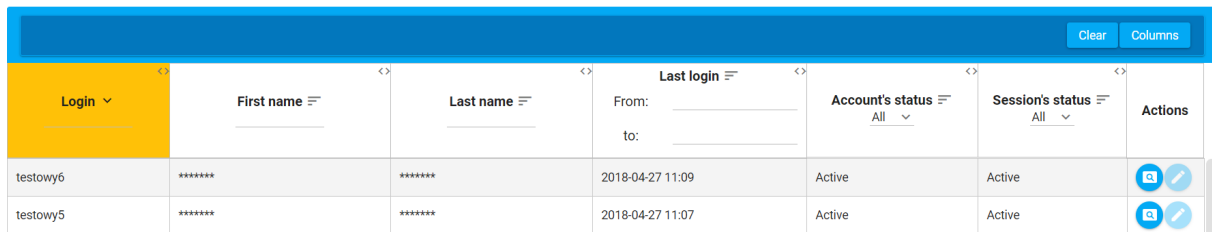
Therefore, an effective form of protection of personal data should be implemented against unauthorized access, it is explicitly stated in the Article 25 GDPR [4]. In addition, Article 32 provides that a person who has access to the processing of personal data may process it only at the request of the personal data administrator [6]. 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. Article 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 (Fig. 5.2). 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 (user-controller, applicant-approval etc.).

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 [21]. In this case, pseudonymisation is realized by substitute the data with the string of asterisks ("*").

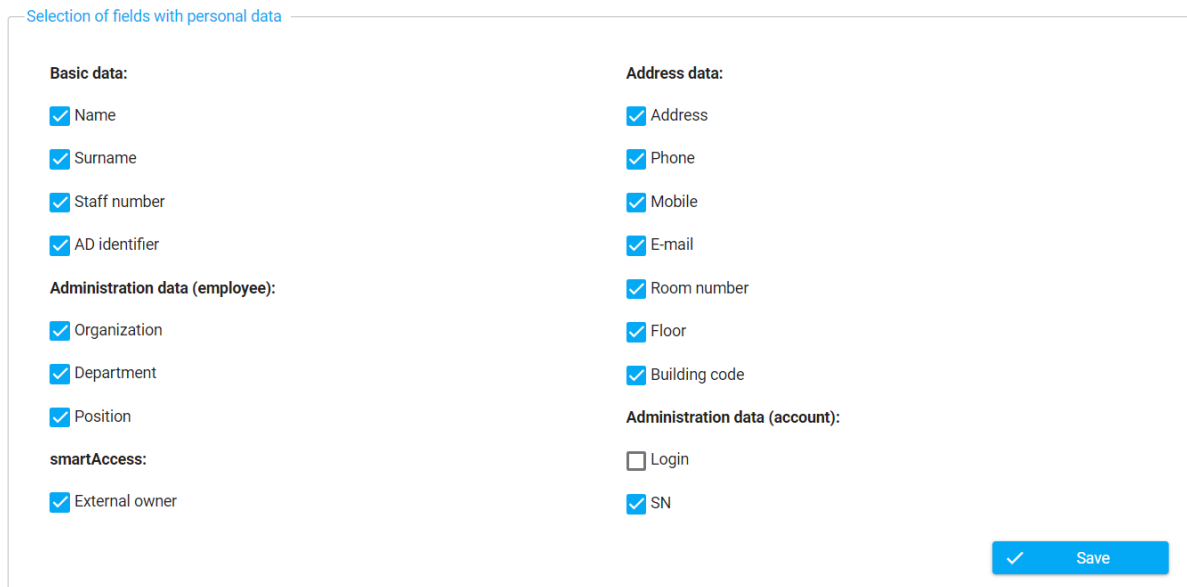
The modular structure of the application also requires the introduction of a pseudonymisation configuration that allows flexible definition of the data to be protected (Fig. 5.3). This is important because each of the modules processes personal data to varying degrees, which is related to the scope of 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 in the system, entitling him to access the configuration panel.



The image shows a web application interface for managing user accounts. At the top, there is a blue header bar with 'Clear' and 'Columns' buttons. Below the header is a table with columns: 'Login', 'First name', 'Last name', 'Last login', 'Account's status', 'Session's status', and 'Actions'. The 'Login' column has a dropdown menu. The 'First name' and 'Last name' columns have search filters. The 'Last login' column has 'From:' and 'to:' filters. The 'Account's status' and 'Session's status' columns have dropdown menus set to 'All'. The 'Actions' column contains icons for edit and delete. The table contains two rows of data: 'testowy6' and 'testowy5', both with pseudonymized names (*****), last login dates, and 'Active' status.

Login	First name	Last name	Last login	Account's status	Session's status	Actions
testowy6	*****	*****	2018-04-27 11:09	Active	Active	[Edit] [Delete]
testowy5	*****	*****	2018-04-27 11:07	Active	Active	[Edit] [Delete]

Figure 5.2 Exemplary view of administrating users accounts with pseudonimization included



The image shows a configuration window titled 'Selection of fields with personal data'. It contains several sections with checkboxes for selecting fields to be pseudonymized. The sections are: 'Basic data' (Name, Surname, Staff number, AD identifier), 'Administration data (employee)' (Organization, Department, Position), 'smartAccess' (External owner), 'Address data' (Address, Phone, Mobile, E-mail, Room number, Floor, Building code), and 'Administration data (account)' (Login, SN). A 'Save' button is at the bottom right.

Basic data:

☒ Name

☒ Surname

☒ Staff number

☒ AD identifier

Administration data (employee):

☒ Organization

☒ Department

☒ Position

smartAccess:

☒ External owner

Address data:

☒ Address

☒ Phone

☒ Mobile

☒ E-mail

☒ Room number

☒ Floor

☒ Building code

Administration data (account):

☐ Login

☒ SN

Figure 5.3 View of pseudonimization configuration

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 principle (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. 5.4). 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. 5.5).

Personal data access managing

Add access to personal data

Select user from list

Login * Name * Surname *

Access from: * to: *

+ Add

Employees with access to personal data

Login	Name	Surname	Access from	to	Access status	Consent	Actions
testowy5	Jan	Testowy	Jun 20, 2018	Jun 23, 2018	Active	Active	

Figure 5.4 Registry panel of entitled to personal data processing

History of access to personal data				
Access from	To	Status	Change date	Change by
Jun 20, 2018	Jun 23, 2018	Active	Jun 20, 2018	Pawel Rymer

Figure 5.5 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:

- 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 admin panel (new functionality).

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 principle, 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).

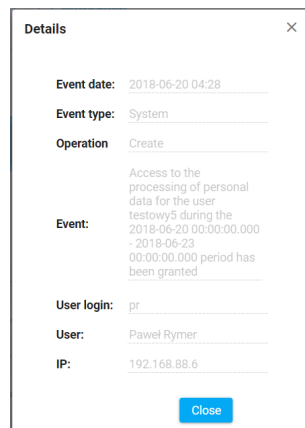


Figure 5.6 Example of recorded log after granting permission to the processing of personal data

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 collects the data about:

- Basic information:

- Number, name and description of registry,
 - person adding the registry,
 - time of adding,
 - person modifying 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 acquiring 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 countries 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 assessment,
 - related business processes,
 - information 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 adding a new processing activity. There are fields in it that are used in the form of adding a new processing activity. Its collection of fields is permanent and contains:

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 acquiring data,
9. methods of transmitting data,
10. categories of processed data,
11. categories of data audience,
12. categories of persons which data concern,
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.

As one can easily see, some of the dictionary fields coincide with the data required to fill in the form adding a new processing activity. The essence of its application was to improve the filling in of this form. Because of the amount of data that need to enter 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.

Chapter 6

Conclusions

Chapter 7

Summary

Bibliography

- [1] Act of 29 august 1997 on the protection of personal data (Dz.U. nr 133, item 883).
- [2] Art. 4 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. 9 *ibidem*.
- [4] Art. 25 *ibidem*.
- [5] Art. 30 *ibidem*.
- [6] Art. 32 *ibidem*.
- [7] Article 27 of the Act of August 29, 1997 on the protection of personal data (Journal of Laws No. 133, item 883).
- [8] 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. 483 Journal of Laws No. 78, item 483 with changes to the law on the protection of personal data).
- [9] Article 6 of the Act of August 29, 1997 on the protection of personal data (Journal of Laws No. 133, item 883).
- [10] 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).
- [11] General Inspector of Personal Data Protection: Law reform - current work. <https://www.gioudo.gov.pl/pl/1520281/10255>. Access: 2018-22-03.
- [12] 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).
- [13] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, and J. Łuczak. *Personal Data Protection Law*. 2016.
- [14] 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.

- [15] 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.
- [16] 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-c.html>, Apr 2018.
- [17] LexDigital. Ochrona danych osobowych - nowe zasady rodo. <https://lexdigital.pl/ochrona-danych-osobowych-nowe-zasady-rodo>, Jun 2018.
- [18] 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.
- [19] A. Partyka. GRC - terra incognita? *Magazyn informatyki śledczej i bezpieczeństwa IT*, 35, Sep 2017.
- [20] B. Schneier. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. 2017.
- [21] R. Stępniewski. Pseudonimizacja według rodo - o czym należy wiedzieć? <https://www.politykabezpieczenstwa.pl/pl/a/pseudonimizacja-wedlug-rodo-o-czym-nalezy-wiedziec>, Aug 2017.
- [22] M. Surdyn. Zgoda na przetwarzanie danych osobowych według rodo. <https://blog-daneosobowe.pl/zgoda-przetwarzanie-danych-osobowych-gruncie-rodo/>, May 2018.

List of Figures

5.1	Exemplary view of administrating users accounts	23
5.2	Exemplary view of administrating users accounts with pseudonimization included	24
5.3	View of pseudonimization configuration	24
5.4	Registry panel of entitled to personal data processing	25
5.5	The history of the user's accesses to processing of personal data	25
5.6	Example of recorded log after granting permission to the processing of personal data	26