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/RODO). Upcoming changes in regulations oblige any entity that processes 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 RODO, such IT system should also support meeting new standard of personal data protection.

In this work will be described the value which personal data represents, origins of personal data protection, legal state in Poland before RODO and the risks associated with the processing of personal data on a large scale. In the following, the issue of the RODO 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 RODO requirements will be presented and analyzed. The example of the existing GRC system will show how it has been adapted to the new requirements resulting from the new regulation, and there will be also described proposed prototype of RODO supporting module for this GRC system.

1.1 Description of the problem

On the 25th of May 2018, RODO will take effect. 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 [8]. 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.

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. When RODO will take effect, 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 GIODO, guidelines from European Data Protection Board or data protection officer. Besides, the ISO norms could be used as a source of practical knowledge [8].

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 RODO comes into force regulations, personal data are information allowing unambiguous determination of the identity of natural person [6]. The new RODO 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 your 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, 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 [13].

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 [13]. Over the years 2011 and 2015 cost of storage 1 petabyte of data decreased from 1 million USD to 100 000 USD [13]. 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 [11]. 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 [11]. 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 [11].

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 [10]. 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 [10].

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 [10]. 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 [10]. 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 life excluding cases justified legally, socially or economically from the point of view of the state [10].

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. [10]. Prior to the effective date of the RODO, this Convention is only by a legally binding internation Act concerning protection of personal data, ratified by all countries belonging to the European Union [10].

2.4 Status in Poland before RODO 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 [5]. At this point, it is worth noting that the Constitution only partially regulates the protection of personal data, an 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 [10]) 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 [10]). 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.

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 [10]. 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.

2.5 Threats associated with the processing of personal 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 us. 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 our data. After the Cambridge Analytica scandal, a public hearing of Facebook CEO Mark Zuckerberg was held before the US Congress. In the course of the 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.

Chapter 3

RODO

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 [9]. 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 circumventionas as much as possible [9]. 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 RODO

In the scope of the definition of personal data, the RODO does not introduce any significant changes and is based on those elements on which Directive 95/46/WE of the European Parliament [7] 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* [4] while the RODO 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 int 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 performence, the administrator's performence 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* - RODO 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,

- *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 RODO.

Most of the above principles had their equivalents, direct or indirect, in the regulations established before the RODO 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 New information obligations

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 RODO introduces obligations which so far were not necessery. This applies, among other, to the information about duration of the processing data, possible profiling 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 RODO 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 RODO [12]. 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 RODO will be visible at the first glance.

3.4 The rights of the data subjects

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, but also 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[8]:

- *being informed of about processing operations*
- *access*
- *rectify/supplement data*
- *to be forgotten*
- *limiting the processing*

- *data transfer*
- *opposition*
- *not to be profiled*

3.5 Consent to the processing of personal data

3.6 Security

3.7 Documentation of processed data

3.8 Rules of privacy by design and privacy by default

3.9 Impact assesments for data protection

3.10 Personal data of children

3.11 Automatic data processing based on profiling

3.12 Data protection violations

3.13 Personal data inspector

3.14 Cross-border data processing

3.15 Entrusting data

3.16 Rasing awareness of the general regulation

Chapter 4

Analiza komercyjnych rozwiazan z zakresu przetwarzania danych osobowych

4.1 RSA Archer

4.2 Microsoft GDPR

4.3 SAP

Chapter 5

Prototyp modulu smartGDPR wspierajacy zgodnosc z RODO

5.1 Rejestr danych przetwarzania

5.2 ...

Chapter 6

Wnioski

Chapter 7

Podsumowanie

Bibliography

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

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

[5] 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).

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

[7] 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).

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

[9] 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).

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

[11] 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.

[12] L. Czujko and Adwokat. Rodo - nowe obowiązki informacyjne wobec podmiotu danych | deloitte, Dec 2017.

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