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, what is RODO, what it stands for and scope of changes in regulations. The available solutions will be analyzed and there will be also described proposed prototype of RODO supporting module for existing 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 [4]. These rules assumes increasing self-reliance, but also responsibility of data administrators.

New regulation determines way of approaching to data processing called *risk based approach*. It assumes that first thing that we do 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 [4].

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 regulations, personal data are *any information regarding natural person, allowing to detemine the identity of this person* [3]. The new RODO regulation is defining personal data more detailed, as *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* [1]. 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 [7].

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 [7]. Over the years 2011 and 2015 cost of storage 1 petabyte of data decreased from 1 million USD to 100 000 USD [7]. 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 [6]. 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 [6]. 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 [6].

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 [5]. They initiated regulation of legal provisions in Western Europe in 20th century. The next Acts that appeared were the first federal law of RFN 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 [5].

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 [5]. 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 may be subject to arbitrary or unlawful interference*

with his private life, family life, home or correspondence" [5]. 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 [5]. 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 [5].

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. [5]. 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 [5].

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 [2]. 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 [5]) 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 [5]). 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 [5]. 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 study 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.

Chapter 3

RODO

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] Art.4 rozporządzenia parlamentu europejskiego i rady (ue) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenia o ochronie danych)[...] (Dz.Urz. UE, L 119/1).

[2] Art.51 konstytucji rzeczypospolitej polskiej z dnia 2 kwietnia 1997 r. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 78, poz.483 ze zm. przepisy dotyczące prawa do ochrony danych osobowych).

[3] Art.6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz.882 i 883).

[4] GIODO: Reforma przepisów - aktualne prace. https://www.giodo.gov.pl/pl/1520281/10255. Dostęp: 2018-22-03.

[5] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, and J. Łuczak. *Prawo ochrony danych osobowych*. 2016.

[6] J. Borecka. Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych. *ZESZYTY NAUKOWE Instytutu Administracji Akademii im. Jana Długosza w Częstochowie*, 2006.

[7] B. Schneier. *Dane i Goliat: Ukryta bitwa o Twoje dane i kontrolę nad światem*. 2017.