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 [3]. 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 [3].

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* [2]. 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 50 and 80 groszy 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 zlotych. 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 [6].

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 [6]. Over the years 2011 and 2015 cost of storage 1 petabyte of data decreased from 1 million dollars to 100 000 dollars [6]. 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 [5]. 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 [5]. 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 [5].

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 [4]. It 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 [4].

2.3 Historical acts of international law

2.4 Status in Poland before RODO comes into force

2.5 Threats associated with the processing of personal data

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

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

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

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

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