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 [1]. 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 [1].

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

2.2 Genesis of personal data protection

2.3 Historical acts of international law

2.4 Status in Poland before RODO comes into force

Chapter 3

RODO

3.1 Zakres przetwarzanych informacji

3.2 Nowe obowiazki informacyjne

3.3 Uprawnienia osob, ktorych dane dotycza

3.4 Zgoda na przetwarzanie danych osobowych

3.5 Zabezpieczenia

3.6 Dokumentacja przetwarzania danych

3.7 Privacy by design i privacy by default

3.8 Ocena skutkow dla ochrony danych

3.9 Dane osobowe dzieci

3.10 Automatyczne przetwarzanie danych oparte na profilowaniu

3.11 Naruszenia ochrony danych

3.12 Inspektor danych osobowych

3.13 Transgraniczne przetwarzanie danych

3.14 Powierzenie danych

3.15 Podnoszenie wiedzy na temat ogolnego rozporzadzenia

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] GIODO: Regulation reform - current works. https://www.giodo.gov.pl/pl/1520281/10255. Access: 2018-22-03.