International Journal of Current Research in Multidisciplinary (IJCRM) *ISSN: 2456-0979*
Vol. 9, No. 09 (October'24), pp. 01-06

Responsibilities of the Online Transaction processing system administrator – a comparative analysis of the Online Transaction Processing system with the personal data protection system, with particular emphasis on information security

Małgorzata Kochanowicz[1], Maryna Lassota[2]
[1](WSB Merito Universityin Poznan, ORCID: 0000-0003-3775-8854)
[2](WSB Merito University in Poznan, Warsaw School of Economics in Warsaw, ORCID: 0000-0003-3713-6000)

ABSTRACT: *The publication discusses the issue of the scope of responsibilities of the Online Transaction Processing system administrator (hereinafter referred to as: "OLTP"). The methodological basis used in the work was the qualitative method, the essence of which consisted in the comparison of two systems – the OLTP database system and the information security system in the form of personal data. It should be noted that the article concerns the law in force in Poland.*
As part of the qualitative method, a tool in the form of expert interviews was also used as a complement. The experts providing answers were people directly involved in the OLTP system - working as OLTP system administrators (and performing work in Poland). The inference method was also used in the work, which allowed to determine the boundaries of the scopes of responsibilities of OLTP system administrators.

Keywords: *Online Transaction Processing, personal data, IT system administrator, information security, security, know how*

INTRODUCTION

The issue of the responsibilities of OLTP system administrators is important due to the fact that more and more companies use new technologies, including the OLTP system, constantly processing countless data, including customer personal data. It is important that people responsible for the functioning of the OLTP system have selected duties and scopes of responsibilities, the proper implementation of which will lead to the correct processing of a lot of data from all over the world and improve their security. The article therefore has an universal aspect.

The issue of the scope of duties and responsibilities of the OLTP system administrator is important because their boundaries are not set by law. No legal act or any guidelines outline the area of the above issues. This paper aims to fill this gap and give proposals to organizations to address it. This solution can be used by any organization, supplementing it with its own know-how, so the article is characterized by an universal pragmatic value.In addition, the motive for writing the article is still the lack of exhaustive scientific publications in this area.

Due to the fact that the duties and responsibilities of the OLTP system administrator are not regulated anywhere by law, this paper focuses on the comparison of this system to the system of information in the form of personal data. The reason why the personal data system was used for comparison is that the OLTP system also processes personal data in the data when processing all various data. Secondly, the personal data protection system and the OLTP system process data – with the difference that personal data is information about a person (personal data protection system) and the OLTP system processes transaction data (which also contains personal data). Thirdly, both the personal data protection system and the OLTP system have similar challenges, threats and risks.

The subject of the study is the OLTP system.

The aim of the paper is to present the scope of duties and responsibilities of the OLTP system administrator.

The research question posed in the paper is: Can the knowledge about the scope of duties and responsibilities that may be imposed on the OLTP system administrator be derived – by analogy – from the personal data protection system?

It should be noted that,the article was written on the basis of the law in force in Poland, and the experts participating in the study are people working in Poland.

Today, OLTP systems are used in many sectors in different parts of the world. They are found in online banking, trade and accounting. Their existence is motivated by the development of business, in which humans are replaced by an IT system that processes very large amounts of data, at a pace that a human could not cope with. OLTP systems have many advantages, hence their elimination from the market of services seems impossible. Below is a list of the advantages of the OLTP system.

Table – advantages of an OLTP system with an explanation

	Advantages of an OLTP system	Explanation
1.	Ability to support multiple users at the same time.	The systems process huge amounts of data, handle a huge number of transactions at the same time.
2.	The atomicity of transactions.	A guarantee that all elements of the transaction will be correct and that the process will be executed.
3.	Automation.	A system that is largely independent of humans.
4.	Reduction of operating costs.	Eliminating the need to hire additional employees. Eliminate the need to buy expensive software.
5.	The speed of data processing.	Fast processing rate of a large number of transactions.
6.	Up-to-date data.	Maintain the actual state of the data. Instant data up-to-date.
7.	High availability.	Minimized risk of data loss.
8.	Multi-availability.	Ability to support multiple users at the same time.
9.	Vertical scalability.	Increasing the computing power of a single server.
10.	Horizontal scalability.	Adding more servers.
11.	Transaction security.	A system that is resilient to threats, including failures.

Source: [1]

OLTP systems are increasingly used in practice. The level of protection of data processed in these systems affects the security of users and participants in processes taking place in the digital environment around the world. An organization based in one country can process the data of residents from the most remote corners of the world, and financial operations can amount to very high amounts. So how do you ensure the security of transactions taking place using these systems?
There are numerous ways to secure transactions, some of them are generally known, and some of them are proprietary solutions of individual organizations, often constituting their valuable know-how. In this paper, we will look at the responsibilities of the OLTP system administrator as one of the guarantors of OLTP system security. Below are the results of the study, which focuses on the scope of responsibilities of the OLTP system administrator.

RESEARCH RESULTS

In May 2024, interviews were conducted with three experts in the field of the Online Transaction Processing system working directly on the system. Experts are OLTP system administrators.

The experts were asked the question:
"What tasks should be imposed on the data administrator of the OLTP system.
Please justify your answer."
Individual experts indicated that the tasks that should be imposed on the OLTP system data administrator are:
Expert number 1:
1) ensuring continuous monitoring of the OLTP system,
2) ensuring continuous optimization of the OLTP system,
3) cooperation of database administrators and developers to ensure compliance of the OLTP system with best practices.

Expert number 1 gave examples of specific actions of the administrator as examples:
1) database design,

2) indexing,
3) query optimization,
4) hardware configuration,
5) loadbalancing.

Expert number 2:
management of access permissions, including:
1) control of user access to data,
2) creating user profiles,
3) user profile management,
4) granting appropriate rights to users,
5) tracking user activity to ensure data security,
maintaining current data, including:
1) monitoring databases in order to maintain their integrity and correctness,
2) managing databases to maintain their integrity and correctness,
3) entering new data into the system, updating existing data and removing outdated or unnecessary data.

Expert number 3:
1) regularly monitor system performance to ensure that it meets user expectations,
2) ensuring that data is consistent and accurate, and that any errors are quickly identified and corrected,
3) regularly restore and back up data and have plans in place in case of disaster to ensure the continuity of the system's operation,
4) regularly updating the system and fixing the security vulnerability,
5) implementing and maintaining security policies, including authentication, authorization, encryption and protection against attacks.

OBLIGATIONS OF THE ADMINISTRATOR OF THE IT SYSTEM PROCESSING PERSONAL DATA – IN THE PERSONAL DATA PROTECTION SYSTEM – IN THE CONTEXT OF INFORMATION SECURITY

In this part of the work, the authors will share the conclusions from the analysis of the personal data system in terms of the duties and responsibilities of the administrator of the system in which personal data is processed. The authors will answer the question:
Is there an administrator of the IT system processing the data in the personal data system? If so, what tasks does it have assigned by law?

First of all, it should be pointed out that the personal data system is an information system strictly based on the law. Each personal data processing activity must comply with the law. The law provides for civil, criminal and administrative consequences for breaching the protection of personal data. The personal data system is regulated in the first place by European Union law, in particular by Regulation (EU) 2016/679 [2]. The conclusion from the analysis of the content of the above document is that the Regulation does not require the appointment of an administrator of the IT system in which personal data is processed. It should be noted, however, that the above act of law indicates the need to adapt new technologies in which personal data are processed to the requirements of the personal data protection law. The Regulation indicates that the legitimate interest of the controller (i.e. the organisation) is the processing of personal data to the extent that is absolutely necessary and proportionate to ensure network and information security (Regulation (EU) 2016/679, motif 49). Network and information security consists of, inter alia ensuring "the resilience of a network or information system at a given level of confidentiality to accidental events or illegal or hostile activities affecting the availability, authenticity, integrity and confidentiality of personal data stored or transmitted - and the security of related services offered or made available through these networks and systems by public authorities, computer threat response teams, computer security incident response teams, electronic communications network and service providers, and security technology and service providers" [2] (motif 49). Examples of these actions are "preventing unauthorised access to electronic communications networks and the distribution of malicious code, interrupting denial-of-service attacks", as well as preventing damage to computer and electronic communications systems"[2] (motif 49). The regulation in the above-quoted provision refers directly to the systems in which personal data is processed. OLTP systems are a kind of new technologies.

It is worth noting that the Regulation also addresses the issue of technical measures to which IT systems can be classified in the personal data protection system. Technical measures are provided for in Article 24 of Regulation (EU) 2016/679. It introduces a requirement that the organization should implement such security measures of IT systems that

they correspond to the risk that may materialize in a given personal data processing process. In addition, security measures should be selected in accordance with the state of technical knowledge and the cost of implementation. The nature, scope, context, purposes of the processing, as well as the risk to the rights and freedoms of natural persons of varying likelihood and severity must also be taken into account. Here are examples of security measures that can be used in an IT system and which are listed in the above Regulation:

1) pseudonymization,
2) encryption,
3) the ability to ensure confidentiality, integrity, availability,
4) ability to provide immunity,
5) the ability to quickly restore the availability of personal data,
6) the ability to quickly restore access to them in the event of a physical or technical incident,
7) testing, measuring and evaluating the effectiveness of IT systems processing personal data.

On the basis of the above, the following range of examples of tasks of the administrator of the IT system used to process personal data could be indicated:

1) selection of appropriate security measures in the IT system processing personal data,
2) introduction of such security measures in the IT system as: pseudonymization and encryption. The administrator should also constantly monitor whether the organization's employees comply with these requirements and apply safeguards for the processing of personal data,
3) monitoring the organization's ability to ensure the resilience of the IT system,
4) monitoring the appearance of physical or technical incidents in the organization. The controller should immediately respond to them and propose safeguards to protect the organisation against incorrect processing of personal data,
5) ensuring confidentiality, integrity, availability of data processed in the IT system,
6) monitoring threats and technical condition of the IT system,
7) creating backup copies of data processed in the IT system and their successive removal,
8) acquiring up-to-date knowledge about security and transferring it in the organization to employees operating the IT system,
9) knowledge of the regulations concerning the processing of personal data, the scope of threats, challenges for the IT system.

In addition to the above tasks, the administrator of the IT system processing personal data may perform the following tasks:

1) granting authorizations to process personal data in the IT system,
2) supervising the provision of data from the IT system,
3) negotiating contracts for the purchase of IT systems processing data,
4) conducting training in the field of data processing in IT systems.

In a large organization, written policies regarding IT systems should be introduced, in the creation of which the administrator of the IT system in which personal data is processed can be involved, for example:

1) instructions for passwordfiles,
2) ICT security policy,
3) procedure for using portable and private computers for business purposes,
4) incidentresponseprocedure,
5) procedure for using mobile devices that are used to process personal data,
6) backup procedure,
7) a register of events violating data security,
8) incidentdetectionprocedure,
9) the procedure for the emergence of crisis situations [3].

The personal data protection system introduced the principle of the so-called pravicy by design. In this case, the data protection system imposes an obligation to take into account the protection of personal data at the design stage. Therefore, if an entrepreneur intends to buy an IT system that processes personal data or, for example, creates such a system, then already at the end of the design stage, preparation for the process of purchase/development of the system is obliged to plan the processing of data in this system so that the processing process meets all legal requirements for the protection of personal data. Such a requirement is a manifestation of a proactive approach, in which the process of personal

data processing is secured already at the design stage, instead of focusing on preventive actions, i.e. those that are taken after the threat materializes.

In addition, the personal data protection law requires that technical measures, including IT systems, process only the personal data that is necessary to achieve the purpose of processing by default - this is the so-called *privacy in default* principle.

The above general legal orders and examples can be a hint on what tasks should be imposed on the OLTP system administrator. In addition, it is worth noting that the OLTP system should have the following features: infallibility, accuracy also known as reliability, record transaction stages, predetermined trade path, concurrency, anonymity of users, availability of the OLTP system, availability of data for users, throughput, accountability, data minimization, no delays, disaster recovery, automatic database scalability, compatibility with the needs of the organization, reliability, guarantee of database security, which are also important when assigning tasks to the OLTP system administrator – he is responsible for providing the system with these features at all times.

CONCLUSION

The duties and responsibilities of an OLTP system administrator are not regulated by law, and organizations must decide for themselves how to define them. The personal data protection system does not support the OLTP system in terms of the controller's duties. It should be noted that the personal data protection system, which is most important, does not oblige the organization to establish an administrator of the IT system processing personal data. In accordance with the above, organizations have no legal obligation to create such jobs or use paid services of other entrepreneurs. The appointment of an IT system administrator depends only on the decision of the top management of the organization. Secondly, it should be noted that the Regulation (EU) 2016/679does not impose requirements directly related to the IT system processing data. The regulation regulates the issue of new technologies and technical and organizational measures. "The intention of the authors of the regulation was to present organizations with a choice as to appropriate technical and organizational measures. Therefore, the task of the organization is to supplement the above regulation with internal law - rich in technical and organizational means. The effectiveness of the organization in the area of personal data protection will depend on how effectively the organization does it [1]".

The issue of data protection in the OLTP system is similar. There is no law that would indicate what technical and organizational measures, including the tasks of the OLTP system administrator, should be or should be introduced in the organization. The provisions of the law on the protection of personal data will not be a hint in this respect. Although the personal data protection regulations refer to the framework in which new technologies are to operate, including networks and systems processing personal data, as well as organizational and technical measures, they do not constitute guidelines and detailed guidelines.

The current conditions of functioning in the digital environment impose on governments the need to develop government programs for investing in the development of technology, including shaping data flow systems so that they meet the expectations of digital communities and standards in industries and, above all, are safe. For example, in Nigeria, an infrastructure has been introduced to improve electronic payments, including „real time gross settlement system; which settles transactions on one to one basis once processed to ensure that payments remain final and irrevocable", Internet banking: were customers instructions and desires are taken and resolved through the internet(e-banking), smart card banking; which performs banking transaction through the use of electronic cards such as debit cards etc" [4].Improving electronic payments requires the introduction of appropriate security measures, but also features that will encourage their use. "The ease of making transactions for consumers makes consumers very interested in technology-based payment systems [5]". In the department of development of new technologies, including systems, it is important that the law and the know-how of entrepreneurs cooperate.

REFERENCES

[1] *M. Kochanowicz, M. Lassota, Advantages of the OLTP System in the Context of Information Security, American International Journal of Business Management (AIJBM) 7(6), 2024, pp. 70-72 or pp. 207. https://www.aijbm.com/wp-content/uploads/2024/06/H767072.pdf*

[2] *Regulation (EU) 2016/679 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) of 27 April 2016, motif 49 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679, access: 24.08.2024*

[3] *M. Kochanowicz, Personal data protection policy is a tool for ensuring the security of the organization (Military University of Technology, 2024), pp. 105.*

[4] *Otuka, Lilian C. &Nwezeaku, Nathaniel C.Ph.D, Chris-Ejiogu Gloria U.Ph.D, Effect of transformation of payment system on commercial banks performance in Nigeria, International Journal of Current Research in Multidisciplinary (IJCRM) 8(2), 2023, pp. 30-39. https://ijcrm.com/publish_article/edition-78/e783039.pdf*

[5] *Imelda Mardayanti, Legal Protection for Consumers Using Technology-Based Payment Services in Indonesia, International Journal of Current Research in Multidisciplinary (IJCRM) 4(2), 2022, pp. 01-07. https://ijcrm.com/publish_article/edition-66/Legal%20Protection%20for%20Consumers%20Using%20Technology-Based%20Payment%20Services%20in%20Indonesia.pdf*