European Research Studies Journal
Volume XXV, Issue 1, 2022

pp. 382-394

The General Data Protection Regulation 3 Years After Implementation: A Comparison between Local Government Administration in Poland and the Republic of Lithuania

Submitted 17/11/21, 1st revision 01/12/21, 2nd revision 20/12/21, accepted 05/02/22

Dominika Lisiak-Felicka[1], Maciej Szmit[2], Jolanta Vaičiūnienė[3]

Abstract:

Purpose: *The aim of the article is to compare the current state of personal data protection almost 3 years after the General Data Protection Regulation (GDPR) in groups of local government administration offices in Poland and the Republic of Lithuania.*
Design/Methodology/Approach: *The diagnostic survey method with the Computer Assisted Web Interview was used. The survey was conducted in local government administration offices in Poland and the Republic of Lithuania almost 3 years after the GDPR implementation.*
Findings: *As the results of the research, the opinions about the office compliance with the GDPR requirements, personal data breaches, requests from data subjects, external audits and inspections, the GDPR impact on the office, the maturity of processing data and problems in ensuring compliance with the GDPR data processing from local government offices in Poland and Republic of Lithuania were obtained.*
Practical Implications: *The results constitute a knowledge base on the personal data protection situation in surveyed countries and can be a form of the basis for further, more in-depth analysis and research.*
Originality/Value: *The article presents our original research. So far, to the best of our knowledge, no comprehensive research has been conducted into this field and compared the current situation in the surveyed countries.*

Keywords: *General Data Protection Regulation (GDPR), data protection, public administration, information security management.*

JEL classification**:** *M15, H83, K24.*

Paper Type: *Research article.*

[1]*Corresponding author, Department of Computer Science in Economics, Faculty of Economics and Sociology, University of Lodz, Lodz, Poland, ORCID ID: 0000-0001-8451-4268, dominika.lisiak@uni.lodz.pl;*
[2]*Department of Computer Science, Faculty of Management, University of Lodz, Lodz, Poland, ORCID ID: 0000-0002-6115-9213, maciej.szmit@uni.lodz.pl;*
[3]*Faculty of Social Sciences, Arts and Humanities, Kaunas University of Technology, Kaunas, Lithuania, ORCID ID: 0000-0001-5378-4847, jolanta.vaiciuniene@ktu.lt;*

1. Introduction

It has been more than 3 years since the implementation of the GDPR requirements to all entities processing personal data in EU countries. Before entering the regulation, the research in local government administration offices in Poland and the Republic of Lithuania has been conducted. Then the opinion about the GDPR compliance after 1,5 years of the implementation date and the present research presents results about opinion after three years of experience.

2. Theoretical Background

2.1 Personal Data Protection in Local Government Administration

The Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, 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 – GDPR) has entered into force on 25th of May 2018. The regulation had changed the approach to the processing of personal data but also caused a lot of problems in organizations that have to prepare for new requirements, especially in local administration offices. This is confirmed by the results of previous authors' studies, many offices had been not prepared and had not implemented all changes on time. The previous researches also indicated that the management of personal data security had been still at a relatively low level of process maturity in most offices (Lisiak-Felicka *et al.,* 2019; Lisiak-Felicka *et al.*, 2020; Lisiak-Felicka and Szmit, 2021).

The local government administration offices have not been avoided before cybercrime. Many of the attacks have been performed on offices. In 2021, the Marshal's Office of Lesser Poland Voivodeship has become a victim of a cyberattack (PAP, 2021). Cybercriminals paralyzed, among others, functioning of electronic mail and contact with the office was possible only by phone. In October 2021 cybercriminals took over the servers of the Otwock office using the ransomware. The citizens could not handle official matters (iOtwock, 2021). There were also big cyberattacks on the Lithuanian administration at the end of the 2020. The content management systems were targeted in an attack to gain access to 22 websites administered by the Lithuanian public sector, mainly regional governments. The attackers then posted three types of fake news (LRT.lt, 2020).

The issue of GDPR compliance in public administration is not the subject of extensive research. Typically, researchers focus on different types of organizations, enterprises and economic sectors (Larrucea *et al.*, 2020; Tankard, 2016, Tikkinen-Piri, 2018). Other publications concentrate on the implementation of changes resulting from the GDPR in a specific case (Martins *et al.,* 2021, Starčevič *et al.,* 2018). Only rare articles are devoted to cases in local administration (Homburg, 2020; Ali, 2020).

2.2 Local Government Administration in Poland and the Republic of Lithuania

Poland has three levels of local government subdivision. The territory is divided into 16 voivodeships (województwa in Polish), which are further divided into 379 districts (powiaty in Polish), which in turn are divided into 2479 municipalities (gminy in Polish). Major cities have the status of both, the municipality and the district. According to Polish Constitution (art. 169 sec. 1) units of local self-government shall perform their duties through constitutive and executive organs. Organizational units that help the local government heads in their tasks are: municipal offices, districts offices and marshal's offices (Journal of Laws, 1998).

In Lithuania, the basic unit of the administrative division is the local government (lit. savivaldybė) - there are 60 local governments. Each local government has a local government council whose members are elected in universal and direct elections for a four-year term. The council is a legislative and decision-making body, adopts the budget and establishes the smallest territorial units. Starosts (lit. seniūnija) are the smallest units and do not play a significant role in national politics. As a result of the administrative reform of 2010, the existing counties were liquidated (10 in total, lit. apskritis), which, however, still retained their statistical and geographical function (Official Statistics Portal, 2021, Ministerstwo Spraw Zagranicznych, 2021).

3. Research Methodology

The presented research has an exploratory and descriptive character and focuses on problems concerning GDPR requirements and operations of the local government administration related to implemented changes in personal data processing. The research covered the existing state of personal data protection in local administration offices in Poland and the Republic of Lithuania after 3 years of GDPR implementation. Specific research questions were as follows (Lisiak-Felicka and Szmit, 2021b):

- Question 1 – Opinion about the office compliance with the GDPR requirements compared to what it was on the day of their implementation and the level of compliance of the office's data processing with the GDPR requirements.
- Question 2 – Have there been any cases of personal data protection breaches over the last year and what were the types of personal data breaches?
- Question 3 – Have the surveyed offices received requests from data subjects over the last year? How many such requests have been received?
- Question 4 – Has an external audit and inspection of the GDPR implementation been conducted at the office?
- Question 5 – Opinion about the GDPR implementation impact.
- Question 6 – Opinion about the maturity of processing data with the GDPR requirements.

- Question 7 – What kind of problems do officials see in ensuring that the office processes data under the requirements of the GDPR?

A diagnostic survey method using the Computer Assisted Web Interview has been performed. The survey invitation was sent by e-mail to all local government administration offices in Poland and the Republic of Lithuania. The survey questionnaire was anonymous and contained 16 questions in the Polish version and 14 questions in the Lithuanian version.

This change is concerned with differences in specific administration divisions in surveyed countries. It was conducted in the first quarter of 2021. From 2,807 offices in Poland, 384 responses were received, and from 60 offices in the Republic of Lithuania, 20 responses were obtained (Figure 1a with note and Figure 1b).

Table 1 presents the numbers of employees in surveyed offices. The largest group in Poland were small offices with several employees not exceeding 50. In turn, the largest group in the Republic of Lithuania were medium office with a number between 100 and 500 employees.

4. Results and Discussion

The officials were asked about the opinion of the compliance of GDPR almost three years after the implementation changes resulting from the regulation. The vast majority from Poland and the Republic of Lithuania assessed that after this period offices are more compliant with the GDPR than earlier (Figure 2). The next question was concerned with the specification of the level of compliance. Both in Poland and the Republic of Lithuania opinions about this level are very optimistic (Figure 3).

Respondents were asked about the number of data security breaches. In the great majority of offices in Poland, there were no such cases. Only 61 offices declared that such cases had occurred (three offices did not specify the number of breaches). In the Republic of Lithuania, 5 offices declared that there were security breaches. The numbers of such cases were presented in Figure 4 and Table 2.

Respondents were also asked about the number of requests data from data subjects. Such applications were received in the case of 47 offices from Poland and 9 offices from the Republic of Lithuania.

Table 3 presents detailed data from offices. It could be seen that that great majority of offices received a small number of applications. The number of applications is not large enough to interfere with the day-to-day work of officials.

Figure 1. *The geographical location of offices participating in the survey from a) Poland, b) Lithuania*

a)

Voivodeship	Sample
Masovian	50
Greater Poland	37
Silesian	32
Lesser Poland	31
Subcarpathian	29
Kuyavian-Pomeranian	27
Łódź	24
Lower Silesian	22
Pomeranian	22
Lublin	19
Warmian-Masurian	19
Podlaskie	17
Opole	16
West Pomeranian	15
Świętokrzyskie	13
Lubusz	9
Total	**382**

Note: *Due to the anonymous survey, the marshal offices were not asked about the location because of the possibility of identification (there is only one marshal office in each voivodeship). Two marshal offices participated in the survey.*

b)

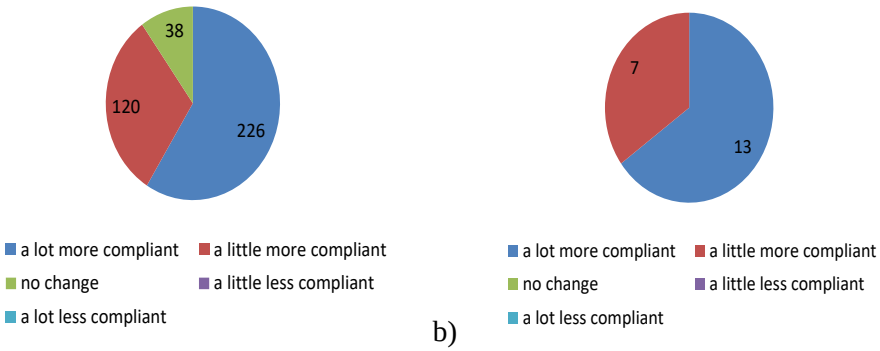
County	Number
Kauno	5
Panevėžio	3
Šiaulių	3
Vilniaus	3
Alytaus	2
Marijampolės	2
Klaipėdos	1
Telšių	1
Tauragės	0
Utenos	0
Total	**20**

Source: *Own research.*

Table 1. *The numbers of employees in surveyed offices.*

Numbers of employees	Numbers of offices – Poland	%	Numbers of offices – Lithuania	%
up to 50 people	223	58.1%	0	0.0%
51 to 100 people	94	24.5%	3	15.0%
101 to 500 people	54	14.1%	15	75.0%
501 to 1,000 people	6	1.5%	2	10.0%
1,001 to 2,000 people	4	1.0%	0	0%
2,001 to 3,000 people	0	0.0%	0	0%
over 3,000 people	3	0.8%	0	0%

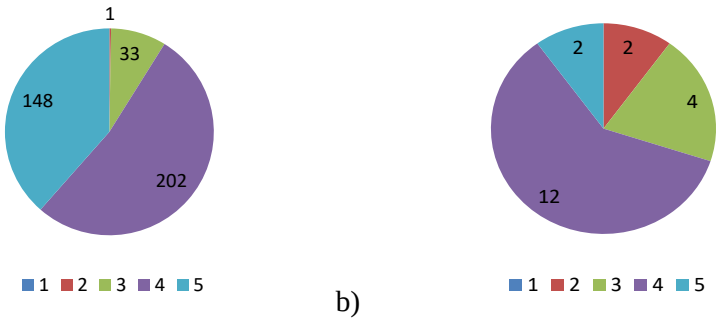
Figure 2. *Compliance with GDPR almost 3 years after the implementation: a) Poland, b) Lithuania*



a) b)

Source: *Own research.*

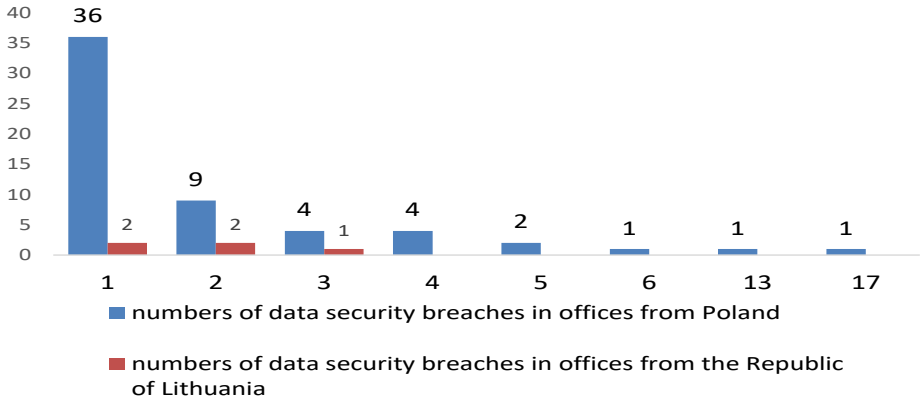
Figure 3. *The level of compliance with GDPR: a) Poland, b) Lithuania*



a) b)

Source: *Own research.*

Figure 4. *The numbers of data security breaches in offices from Poland and the Republic of Lithuania*



Source: *Own research.*

Table 2. *The numbers of data security breaches – comparison between offices from Poland (58 answers) and the Republic of Lithuania (5 answers)*

Type of personal data protection breaches according to the classification of the Personal Data Protection Office	Number of indications (Poland)	Number of indications (Lithuania)
Personal data sent to the wrong recipient	15	2
Unintentional publication	14	2
Paper documentation (containing personal data) lost, stolen or left in an unsecured location	11	0
Incorrect personal data anonymization in the document	9	2
Disclosure of the data of the wrong person	9	0
Verbal disclosure of personal data	8	0
Paper correspondence lost by the postal operator or opened before returning it to the sender	5	0
Software interfering with confidentiality, integrity and data availability	5	0
Unauthorized access to information by breaking security	5	1
Unauthorized access to information	4	2
Lost or stolen media/device	2	0
Obtaining confidential information by a seemingly trusted person in official electronic communication, such as e-mail or internet messenger (phishing)	1	0
Incorrect removal/destruction of personal data from the media/electronic device before its sale by the controller	1	0

Source: *Own research.*

Table 3. *The numbers of requests data from data subjects – comparison between offices from Poland (47 answers) and the Republic of Lithuania (9 answers)*

Number of requests	Number of indications (Poland)	Number of indications (Lithuania)
1-50	42	9
51-100	3	0
101-500	2	0

Source: *Own research.*

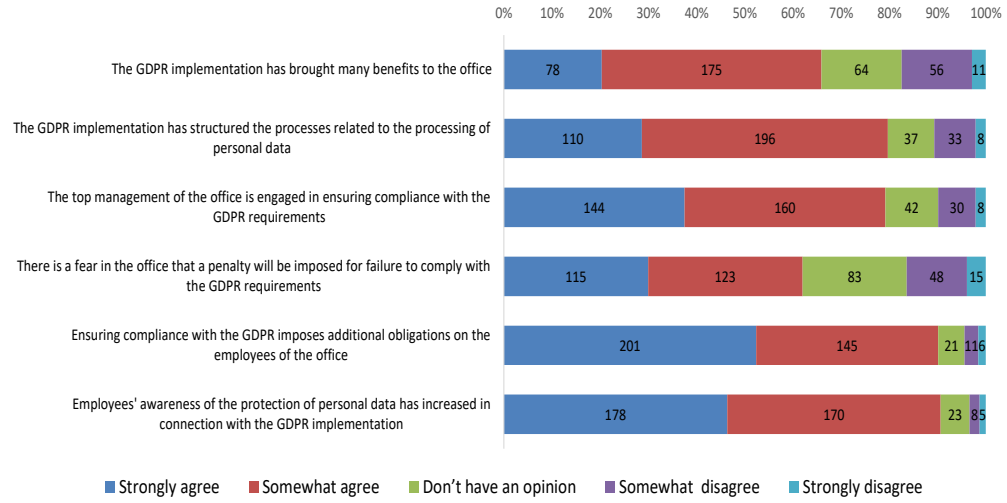
Another question focused on the impact of the GDPR implementation. Respondents were asked about six statements:

- The GDPR implementation has brought many benefits to the office.
- The GDPR implementation has structured the processes related to the processing of personal data.
- The top management of the office is engaged in ensuring compliance with the GDPR requirements.
- There is a fear in the office that a penalty will be imposed for failure to comply with the GDPR requirements.
- Ensuring compliance with the GDPR imposes additional obligations on the employees of the office.
- Employees' awareness of the protection of personal data has increased in connection with the GDPR implementation.

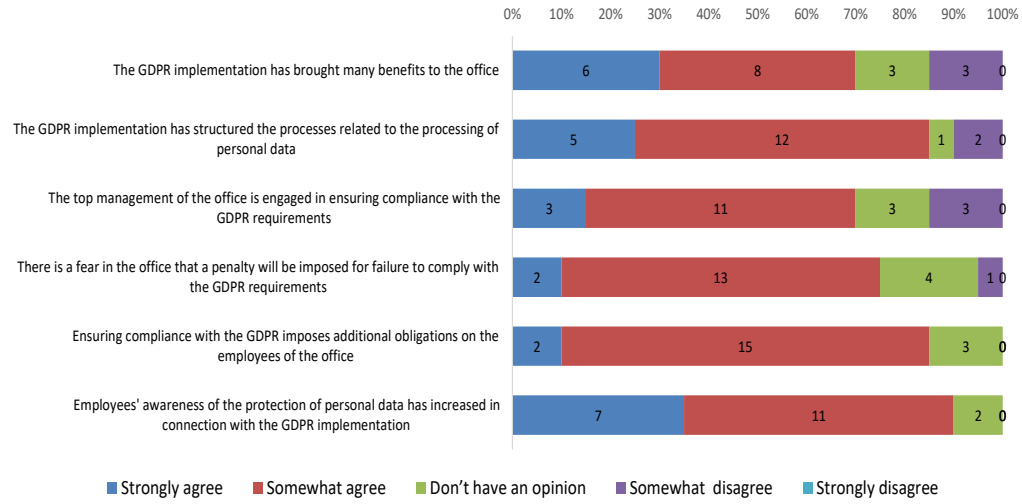
The answers were given on the scale from strongly agree to strongly disagree (Figure 5).

Figure 3. *Opinion about the impact of the GDPR implementation: a) Poland, b) Lithuania*

a)



b)



Source: *Own research.*

The great majority of respondents both in Poland and the Republic of Lithuania indicated that the GDPR implementation had an impact on all situations commented in these statements. Relatively many "disagree" responses or "no opinion" were given to the statements: "There is a fear in the office that a penalty will be imposed for failure to comply with the GDPR requirements", "The GDPR implementation

has brought many benefits to the office" and "The top management of the office is engaged in ensuring compliance with the GDPR requirements". The same statements were indicated in Poland and the Republic of Lithuania.

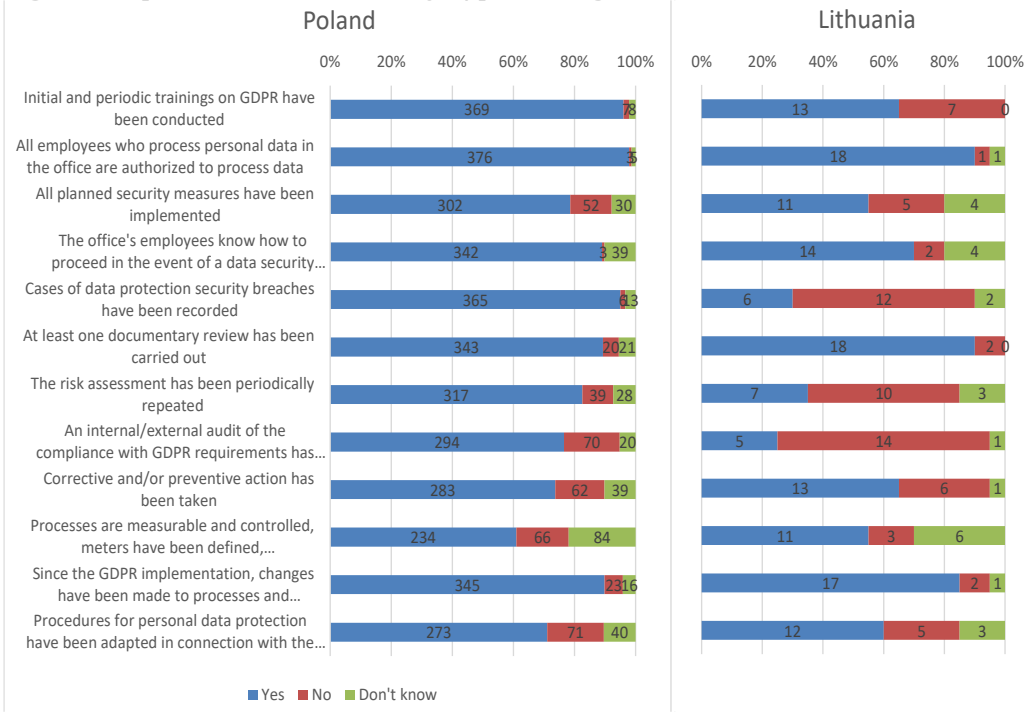
The next question concerned external audits and external inspections of the GDPR implementation conducted at the office. In Poland, in 119 offices there has been provided external audits of the GDPR implementation and in 58 offices there has been provided external inspections of the GDPR implementation. In the Republic of Lithuania, only one office have been provided external audit and none of them has been provided external inspection.

In the following question opinions about some statements connected with the maturity of processing data with the GDPR were included. The respondents answer these questions using "yes", "no" or "don't know". The detailed results are present in Figure 6.

- Initial and periodic pieces of training on GDPR have been conducted.
- All employees who process personal data in the office are authorized to process data.
- All planned security measures have been implemented.
- The office's employees know how to proceed in the event of a data security breach incident.
- Cases of data protection security breaches have been recorded.
- At least one documentary review has been carried out.
- The risk assessment has been periodically repeated.
- An internal/external audit of the compliance with GDPR requirements has been carried out.
- Corrective and/or preventive action has been taken.
- Processes are measurable and controlled, meters have been defined, measurements and monitoring have been carried out.
- Since the GDPR implementation, changes have been made to processes and procedures.
- Procedures for personal data protection have been adapted in connection with the introduction of remote working in an epidemic situation.

As it could be seen, the highest difficulties in Polish offices were: internal/external audits, measurability and control of processes, conducting measurements and monitoring, security measures implementation, procedures for protecting data in the epidemic situation. On the other hand, in Lithuanian offices problems were with internal/external audits, recording the data security breach and repeating the risk assessment.

Figure 4. *Opinion about the maturity of processing data with the GDPR*



Source: *Own research.*

The last question was concerned with problems in ensuring the proper processing of personal data, by the requirements of the GDPR. Both in Poland and the Republic of Lithuania officials have found legal, financial, bureaucratic, organizational, and human problems. The answers from Poland were presented in detail in our previous publication. In this article only problems indicated from Lithuania respondents were exposed:

- "the requirements of the regulation for many employees are still seen as redundant,
- lack of consciousness,
- requirements for employee involvement in the GDPR compliance,
- lack of human and financial resources,
- these are not challenges, but extra work,
- the biggest challenge was to be affected the human factor
- employees' perspectives on personal data requirements,
- there is a widespread perception among both staff and management that data protection is only a concern for the Data Protection Officer. For this reason, data protection issues are not even on the agenda.

- the Data Protection Officer was appointed only because it is required by the GDPR. In other words, the prevailing view is that "until you check as long as it is and "as is."
- it is sometimes difficult to convince Council members of certain deadlines for publishing and storing data,
- pandemic
- so far there is still a lot of uncertainty / grey area in GDPR;
- national legislation often contradicts the GDPR because it was adopted before it entered into force;
- management does not pay enough attention to the protection of personal data, it is necessary to prove every time;
- difficult to consult with the supervisory authority - difficult to contact, long deadlines for answers, and answers are template, bureaucratic, without any specificity.
- there is a lack of specific training for DPOs, general training is often offered, a lot of information is already known, so the supply is very limited,
- it is difficult to identify data users and managers,
- various innovations that need to be explored and absorbed,
- with changes in processes and procedures, development and updating of various procedures,
- the functions of the DPO are as additional functions for employees, so not enough time and attention is given to this area,
- reckless decisions on the processing of personal data,
- lack of time to adequately ensure the protection of personal data,
- improper application of GDPR requirements,
- familiarization of employees with the implementation of the GDPR,
- lack of knowledge of employees about personal data protection and processes."

5. Conclusion

The articles present a comparison of compliance almost 3 years after GDPR implementation in local government administration in Poland and the Republic of Lithuania. Opinions about the compliance of GDPR requirements are similar in both countries. The majority of offices indicated, that almost three years of the implementation the offices are a lot of or more compliant with the resulting required in GDPR. Only 10% of Polish offices indicated, that there is no change comparing the day of implementation and 3 years later. This means that offices (mostly) need more time to properly implement all requirements. It is also confirmed that the vast majority indicated that the level of compliance is on a good and very good level.

On the other hand, it could be seen that despite the high rating, offices still face the problem of proper management of information security incidents. As previous research has shown and the current one, relatively few offices register such incidents

and there are very few of them. Dominant in Poland were: personal data sent to the wrong recipient, unintentional publication, paper documentation (containing personal data) lost, stolen or left in an unsecured location, incorrect personal data anonymization in the document, disclosure of the data of the wrong person. In turn, in Lithuania: personal data sent to the wrong recipient, unintentional publication, incorrect personal data anonymization in the document and unauthorized access to information. Due to the low number of reported incidents, these results cannot be generalized.

The results also show that there are few requests data from data subjects in both countries. As the results of the research, the opinion about the impact of GDPR implementation in surveyed countries and opinion about the maturity of processing data with the GDPR were examined. The problems indicated by Lithuanians' offices were similar to the issues specified in Polish.

References:

Ali, O., Shrestha, A., Chatfield, A., Murray, P. 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1). doi:10.1016/j.giq.2019.101419.

Dz.U. (Journal of Laws) of 1998, item 96, pos. 603. (1998), 'Act of 24 July 1998 on the introduction of a basic three-tiered territorial division of the country (Ustawa z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa Dz.U. 1998 nr 96 poz. 603)]. http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19980960603.

Homburg, V., Kokje, J. 2020. Information policy security compliance in Dutch local government: Results from a vignette survey. Paper presented at the Proceedings of the 15th International Conference on Cyber Warfare and Security. ICCWS 2020, 211-218. doi:10.34190/ICCWS.20.025.

https://pdfs.semanticscholar.org/d75a/1a38e0a560f7ac9dde52c33a387c0c6fe21a.pdf.

https://www.lrt.lt/en/news-in-english/19/1300455/lithuania-came-under-biggest-cyber-attack-in-years-says-defence-minister.

iOtwock.info. 2021. Cyberatak na Urząd Miasta Otwocka - jak można go było uniknąć? https://iotwock.info/artykul/cyberatak-na-urzad-miasta/1250396.

Larrucea, X., Moffie, M., Asaf, S., Santamaria, I. 2020. Towards a GDPR compliant way to secure european cross border healthcare industry 4.0. Computer Standards and Interfaces, 69. doi:10.1016/j.csi.2019.103408.

Lisiak-Felicka, D., Szmit, M. 2021b. The GDPR Compliance in Local Government Administration in Poland almost 3 Years after Implementation. Innovation Management and information Technology impact on Global Economy in the Era of Pandemic, 2767-9640, s. 9842-9853.

Lisiak-Felicka, D., Szmit, M. 2021a. GDPR implementation in public administration in Poland 1.5 year after: An empirical analysis. Journal of Economics & Management, 43, 1-21.

Lisiak-Felicka, D., Szmit, M., Szmit, A. 2019. The assessment of GDPR readiness for local government administration in Poland. In: Wilimowska, Z., Borzemski, L., Świątek, J. (Eds.), Information systems architecture and technology, Advances in Intelligent Systems and Computing, 854, 417-426.

Lisiak-Felicka, D., Szmit, M., Szmit, A., Vaičiūnienė, J. 2020. GDPR implementation in local government administration in Poland and Republic of Lithuania. In: Wilimowska, Z., Borzemski, L., Świątek, J. (Eds.), Information systems architecture and technology, Advances in Intelligent Systems and Computing, 1052, 49-60.

LRT.lt. 2020. Lithuania came under biggest cyber attack in years, says defence minister.

Martins, F., Amaral, L., Ribeiro, P. 2020. Implementation of GDPR: Learning with a local administration case study. doi:10.1007/978-3-030-51005-3_19.

Ministerstwo Spraw Zagranicznych. 2021. Informator ekonomiczny. https://www.gov.pl/web/litwa/litwa.

Official Statistics Portal. 2021. Administrative territorial division. https://osp.stat.gov.lt/regionine-statistika-pagal-statistikos-sritis.

PAP. 2021. Małopolski Urząd Marszałkowski zaatakowany przez hakerów. https://samorzad.pap.pl/kategoria/aktualnosci/malopolski-urzad-marszalkowski-zaatakowany-przez-hakerow.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Starčevič, K., Crnkovič, B., Glavaš, J. 2018. Implementation of the General Data Protection Regulation in companies in the Republic of Croatia. Ekonomski Vjesnik / Econviews, 31(1), 163-176.

Tankard, C. 2016. What the GDPR means for businesses. Network Security, 2016(6), 5-8. doi:10.1016/S1353-4858(16)30056-3.

Tikkinen-Piri, C., Rohunen, A., Markkula, J. 2018. EU general data protection regulation: Changes and implications for personal data collecting companies. Computer Law and Security Review, 34(1), 134-153. doi:10.1016/j.clsr.2017.05.015.