



Dominika Lisiak-Felicka

 <https://orcid.org/0000-0001-8451-4268>

Department of Computer Science
in Economics
Faculty of Economics and Sociology
University of Lodz, Lodz, Poland
dominika.lisiak@uni.lodz.pl

Maciej Szmit

 <https://orcid.org/0000-0002-6115-9213>

Department of Computer Science
Faculty of Management
University of Lodz, Lodz, Poland
maciej.szmit@uni.lodz.pl

GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis

Accepted by Editor Ewa Ziemia | Received: November 3, 2020 | Revised: December 29, 2020;
January 18, 2021; January 30, 2021 | Accepted: February 2, 2021 | Published: February 15, 2021.

© 2021 Author(s). This article is licensed under the Creative Commons Attribution-NonCommercial 4.0 license
(<https://creativecommons.org/licenses/by-nc/4.0/>)

Abstract

Aim/purpose – The paper contains descriptive exploratory research on the implementation of General Data Protection Requirements (GDPR) in a group of Polish public administration offices. The purpose of this research is to investigate the current state of personal data protection in the entities surveyed.

Design/methodology/approach – The diagnostic survey method using the Computer Assisted Web Interview was employed. The survey was conducted in local government administration offices a year and a half after the GDPR implementation.

Findings – All marshal offices and the majority of districts (about 80%) confirmed that they comply with all the GDPR requirements. The situation was slightly worse in municipal offices – about 23% of them declared that they do not comply with all the GDPR requirements. In officials' opinion this situation may be improved by conducting training for employees, employee engagement, and appropriate support of the office management. Another aspect that draws attention is a very small budget dedicated to the GDPR implementation and maintenance in most of the offices surveyed.

Research implications/limitations – The limitation of the findings is the relatively low responsiveness of the questionnaire survey.

Originality/value/contribution – The research concerns a relatively new subject. The state of personal data protection in public administration in Poland after 18 months of the GDPR implementation was analyzed. So far, there is no comprehensive research that has been conducted into this field in local government administration.

Keywords: General Data Protection Regulation (GDPR), public administration, personal data, GDPR implementation, data protection breaches.

JEL Classification: M15, H83, K24.

1. Introduction

The Regulation (EU) 2016/679 of the European Parliament (2016) 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) came into force on May 25, 2018. Since this date, many organizations have worked to ensure compliance (Breitbarth, 2019).

The results of previous own research indicated that the public administration offices faced many problems with introducing changes caused by the GDPR implementation.

In 2018, we researched the level of preparation of local government administration offices in Poland to the implementation of changes resulting from GDPR. The results of the study were published in a scientific article (Lisiak-Felicka, Szmit, & Szmit, 2019). Based on that research it was concluded that a large group of respondents had not even defined the implementation strategy for the GDPR. The biggest problems in the GDPR implementation were indicated by the offices surveyed: lack of Polish Personal Data Protection Act (appropriate law was introduced on May 10, 2018, shortly before the entry into force of the GDPR Regulation (Ustawa o ochronie danych osobowych [Act on Personal Data Protection], 2018), unclear rules, absence of specific legal acts (e.g., regulations of appropriate ministers), implementation of regulations and specific guidelines.

Poland was not the only country that had had issues with the GDPR implementation. Many concerns were also experienced by other countries, such as Lithuania, where we have conducted a similar study (Lisiak-Felicka, Szmit, Szmit, & Vaičiūnienė, 2020). Readiness to implement changes resulting from GDPR both in Poland and Lithuania was low and the manners of its introduction were not mature enough.

A relatively large number of publications on the GDPR functioning devote much attention to its legal and practical aspects. There is a research gap in the field of empirical research on the current situation. This type of research should be conducted periodically (Jatkiewicz, 2015, p. 68). Only knowledge, even procured on a piecemeal basis, of the implementation and compliance practices can provide the information necessary to assess their effectiveness as a whole and,

consequently, support the process of introducing possible changes, under the evidence-based legislation approach.

The paper contains descriptive exploratory research on the implementation of General Data Protection Requirements in a group of Polish public administration offices. The purpose of this research was to investigate the current state of personal data protection in the entities surveyed.

This paper follows our earlier research (Lisiak-Felicka et al., 2020) and is divided into five main sections. Section 1 introduces the research topic. Section 2 presents an overview of the literature. Section 3 explains the research methodology and Section 4 presents the results of the questionnaire survey. Section 5 is the discussion and conclusion.

2. Literature review

Despite its very short duration, GDPR has been the subject of several scientific studies (largely devoted to legal and technical aspects). In the Scopus database on December 19, 2020, there were 901 articles with the abbreviation ‘GDPR’ as a keyword and 580 in the title, in the Web of Science (core collection) there were 33 texts with ‘GDPR’ in the title and 109 in the topic. The Polish database BazEkon returned 258 texts for the keyword ‘Personal data protection’ (a pre-defined phrase in the BazEkon database) and 29 with ‘GDPR’ in the title. The Science Direct database (Elsevier’s database of electronic journals) returned 1,997 articles with ‘GDPR’ in the title.

After the literature review, it could be concluded that many scientists identified critical success factors, barriers and enablers of the GDPR implementation. Furthermore, the benefits of complying with GDPR have been indicated (e.g., Almeida Teixeira, Mira da Silva, & Pereira, 2018; Krystlik, 2017; Laybats, & Davies, 2018). The regulation changed the approach to the system of personal data protection, introduced many important changes and unified the rules on personal data protection (Ferreira, 2020; Tamburri, 2020; Zerlang, 2017).

There are also critical voices about the regulation disadvantages: organizational consequences, such as bureaucracy, over-regulation, implementation costs, potential level of penalties, need to employ lawyers, training, annoying and time-consuming opt-in mechanisms, and data breach notifications (Fazzini, 2019), as well as technical problems, including blockchain technology (Tatara, Gokceb, & Nussbaum, 2020) or difficulties for computer forensic specialists in evidence collecting (Forbes Technology Council, 2018).

The first penalty for non-compliance with GDPR in public administration in Poland was charged in 2019.

At the turn of January and February 2019, an inspection of compliance of personal data processing with the regulations on personal data protection was carried out, especially with the General Data Protection Regulation and the Act of May 10, 2018 on Personal Data Protection.

During the inspection at the Aleksandrów Kujawski Municipal Office, irregularities were found:

- lack of internal procedures for reviewing resources published in the Public Information Bulletin,
- making personal data available to external entities, without entering into an entrustment agreement with them,
- lack of risk analysis and the implementation of appropriate technical and organizational measures in connection with the storage of recordings from the sessions of the Municipal Council on YouTube servers, lack of backup copies of these recordings,
- no indication of the personal data processing activities of all recipients of the data in the proper register, and
- no indication of a time limit for the deletion of data in such a way as to ensure that the data are processed under the principle of limited storage.

In connection with the infringement of the provisions of Article 5(1)(a), (e) and (f), Article 5(2), Article 28, Article 30(1)(d) and (f) and Article 32 of the General Data Protection Regulation, on October 18, 2019, the President of the Office for Personal Data Protection imposed a fine of PLN 40,000 on the Mayor of Aleksandrów Kujawski (UODO, 2019b). This was the first time that a fine had been imposed in a public entity.

So far (until October 2020), the President of the Personal Data Protection Office has issued 37 decisions in the public sector, two of which concerned local authorities, ordering the rectification of irregularities (UODO, 2019ac) and a few decisions refusing to initiate the procedure.

The Personal Data Protection Office decisions do not cover all possible personal data security breaches because a breach may also be linked to fraud or crime and thus becomes a matter of interest not for the regulator but the criminal justice. For instance, in the recent days, the Polish press has published information about the official from the District Office in Sanok, who is suspected of passing on the car owners' data to persons carrying out insurance activity.

Comparing the situation at EU level, not only in the public sector but also in the private sector, it can be observed that the numbers of penalties and fines for breaches of the GDPR rules are very different. Spain has experienced most of the cases with 139, followed by Romania with 39. The other countries had between 1 and 30 such cases. The webpage GDPR Enforcement Tracker contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the General Data Protection Regulation (GDPR Enforcement Tracker, 2020).

Although this is a crucial aspect, not all national authorities publish statistics on the number of incidents, thus it is difficult to say anything about the GDPR effectiveness in this area. In those circumstances, it is necessary to rely on estimates and secondary sources.

The report by DLA Piper's cybersecurity and data protection team shows that European data protection regulators have imposed EUR114 million in fines under the GDPR regulation and notifications about personal data breaches have exceed 160,000 in Europe since the GDPR introduction (DLA Piper, 2020).

Report prepared by the Association of Personal Data Protection Companies covered 277 organizations, supported by 8 different companies associated in this organization, contains information about the number of recorded security incidents. In total, in the period from May 25, 2018 to May 25, 2019, 127 incidents were officially recorded in the organizations mentioned above. As much as 80% of all incidents were recorded in the private sector (ZFODO, 2020).

The statements above, results of earlier research and information about the first penalty in public administration were an impulse for further study. Therefore, the research on 18 months after the GDPR implementation was conducted.

3. Research methodology

This exploratory descriptive research focuses on investigating and describing the current state of personal data protection in local government administration offices in Poland after the implementation of changes resulting from GDPR.

The research questions fielded on the GDPR implementation and cost of this process, elements that had a significant impact on the GDPR implementation, changes in the approach to personal data management.

Specific research questions were as follows:

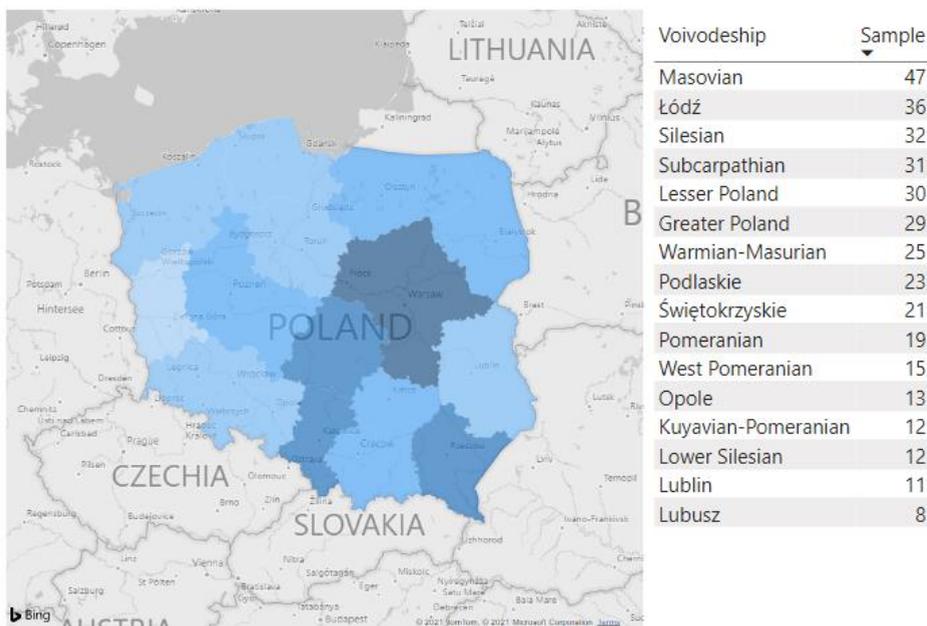
- Q1 – Do the surveyed offices meet all the GDPR requirements and have all changes been made by May 25, 2018?

- Q2 – What was the indicative cost of implementing GDPR in the surveyed offices?
- Q3 – Which factors are the most important for the GDPR implementation?
- Q4 – How has GDPR changed the approach to personal data management?
- Q5 – Have the surveyed offices received requests from data subjects? How many such requests have been received?
- Q6 – Have there been any cases of personal data protection breaches since the GDPR implementation and what were the types of the personal data breaches?
- Q7 – Have the GDPR entry into force and the related activities had an impact on the overall management of information security (not only personal data) in offices?

A diagnostic survey method using the Computer Assisted Web Interview has been used. The survey invitation was sent by e-mail to all local government administration offices. It was explained that the obtained data would be used in an aggregated form only for the preparation of statistical summaries and analyses in scientific publications. The survey questionnaire contained 15 questions and was anonymous. It was conducted at the turn of December 2019 and January 2020. From 2,807 offices, 368 responses were received.

The subjects of the research were offices of local government administration in Poland. The administrative division of Poland is based on three organizational levels (Ustawa o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa [Act on the introduction of a basic three-tiered territorial division of the country], 1998). The territory of Poland is divided into provinces, these are further divided into districts, and these, in turn, are divided into municipalities. Major cities have the status of both municipality and district. The organizational units whose aim is to assist municipality officers, districts heads and marshals in the tasks defined by the law of the state are as follows: municipality offices, districts offices and marshal offices (Ustawa o samorządzie gminnym [Act on municipal government], 1990; Ustawa o samorządzie powiatowym [Act on district local government], 1998; Ustawa o samorządzie województwa [Act on the voivodeship self-government], 1998).

Comparing the location structures of all offices and the locations of the offices participating in the study, it can be stated that they are approximated (Figure 1). The quite similarity of structures in terms of the type of office is also visible (Table 1).

Figure 1. The geographical location of offices participating in the survey

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

Source: Authors' own research.

Table 1. The geographical location of offices participating in the survey regarding the sample from the previous survey and population (except for the marshal offices)

Province	Sample	Previous research	Population (Poland)
Lower Silesian	12	22	195
Kuyavian-Pomeranian	12	19	163
Lublin	11	29	233
Lubusz	8	13	94
Łódź	36	43	198
Lesser Poland	30	49	201
Masovian	47	46	351
Opole	13	11	82
Subcarpathian	31	29	181
Podlaskie	23	30	132
Pomeranian	19	24	139
Silesian	32	40	184
Świętokrzyskie	21	17	115
Warmian-Masurian	25	25	135
Greater Poland	29	43	257
West Pomeranian	15	16	131

Source: Authors' own research.

For the obtained data the Renkonen Similarity Index was calculated, according to the formula:

$$S_r = \sum_1^i \min(p_{1,i}, p_{2,i})$$

where p is the percentage of the relevant fraction in the relevant sample.

The Renkonen Similarity Index between the current sample and the previous research one is 89.3%, between the current sample and the population – 85.5% and between the previous research sample and the population – 88.9%.

Renkonen Similarity Indexes by type of offices were also counted (Table 2).

Table 2. Structures in terms of the type of office – sample vs. previous research vs. population

Type of office	Sample		Previous research		Population	
	%		%		%	
Marshal office	1.1%	4	1.3%	6	0.6%	16
District office	13.6%	50	14.3%	66	11.2%	314
Municipality office	85.3%	314	84.4%	390	88.2%	2477
Total	100.0%	368	100.0%	462	100.0%	2807

Source: Authors' own research.

The Renkonen Similarity Index between the current sample and the sample from the previous research is 99.1%, between the current sample and the population – 97.1% and between the previous research sample and the population – 96.2%.

The majority of the sample examined in the current research were offices with no more than 100 employees. Table 3 presents the number of employees in the offices.

Table 3. Structures in terms of numbers of employees – current research vs. previous research

Numbers of employees	Numbers of offices – current research	%	Numbers of offices – previous research	%
up to 50 people	192	52.17%	279	60.39%
51 to 100 people	98	26.63%	104	22.51%
101 to 500 people	66	17.93%	59	12.77%
501 to 1,000 people	4	1.09%	7	1.52%
1,001 to 2,000 people	6	1.63%	7	1.52%
2,001 to 3,000 people	1	0.27%	4	0.87%
over 3,000 people	1	0.27%	2	0.43%

Source: Authors' own research.

The Renkonen Similarity Index between both datasets is 90.6%.

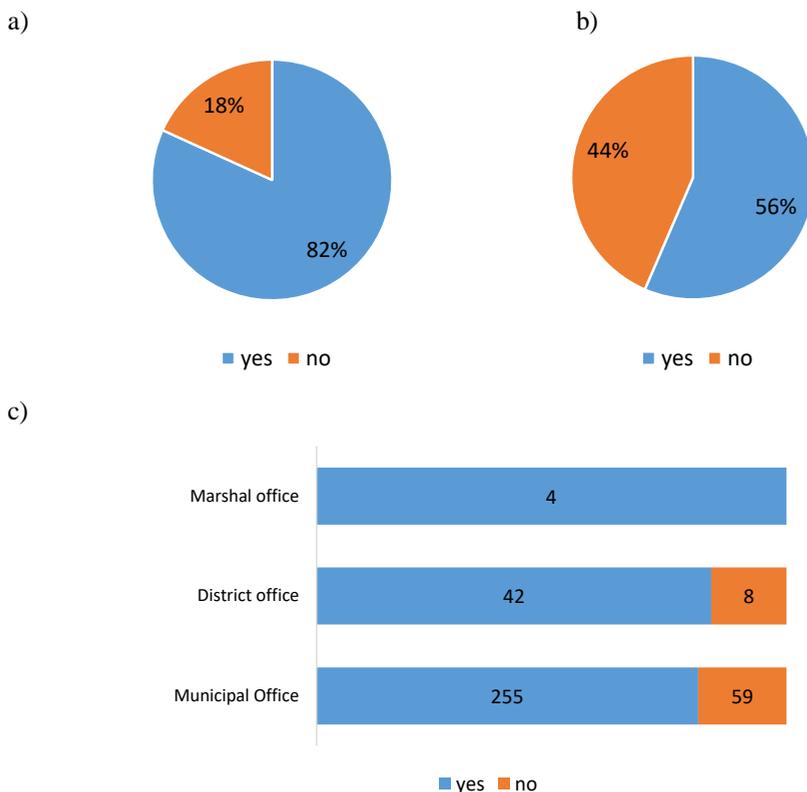
4. Research findings

The results of the study are presented in the subsections concerning the research questions.

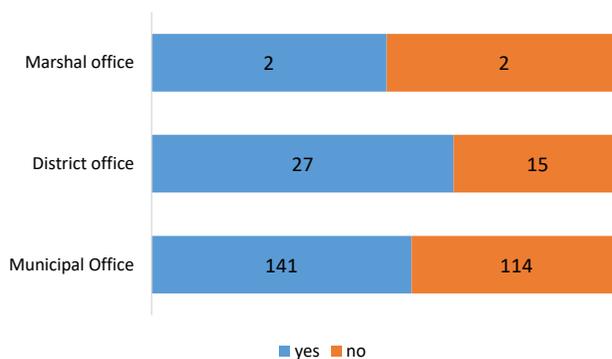
4.1. The GDPR implementation

Among 368 received responses to the question: “Does the office, in your opinion, comply all the GDPR requirements?” the 301 (82%) were affirmative, and 67 (18%) were negative (Figure 2a). Only 170 (56%) declared that all requirements have been implemented before May 25, 2018. Others 131 (44%) offices have not implemented all changes within the required deadline (Figure 2b). The answers to this question by type of office are shown in Figures 2c and 2d.

Figure 2. Answers to questions: a) Does the office, in your opinion, comply with all the GDPR requirements? and b) Have all the changes been implemented before May 25, 2018? And the same answers by type of office c) and d)



d)



Source: Authors' own research.

All marshal offices and the majority of districts declared that they complied with all the GDPR requirements, but only half of the marshal offices and slightly more than half district offices and municipal offices have done it in the required time.

In previous research (between March and April 2018) respondents were asked to assess the degree of office readiness for implementing changes resulting from GDPR (on a scale of 1 to 5, where 1 – no readiness, 5 – all the GDPR requirements have been already implemented). Among 462 offices, 83 declared score 4 or 5, 332 – score 3 or 2, and 47 declared no readiness (score 1).

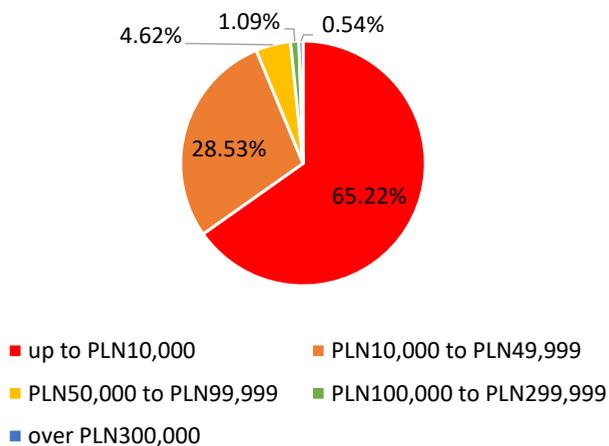
Two months before the GDPR deadline, the vast majority had not been prepared to implement the changes. More, the current study has shown that not all the changes were implemented within the required deadline.

4.2. The cost of the GDPR implementation

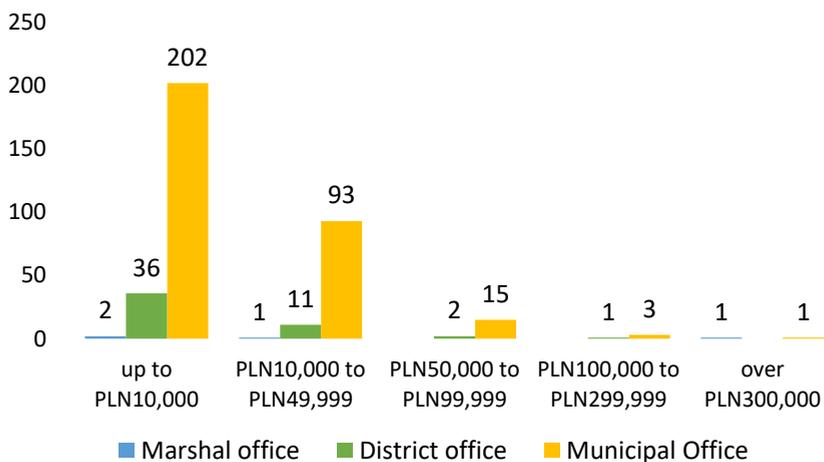
The next question concerned the costs incurred by the surveyed offices for the implementation of changes resulting from the GDPR (Figure 3a and 3b). Over 65% of offices allocated less than PLN10,000 for this purpose.

Figure 3. The cost of the GDPR implementation in offices: a) general data and b) by type of office

a)



b)



Source: Authors' own research.

4.3. The most important factors for the GDPR implementation

The officials were asked to indicate which of the elements they considered most important in the GDPR implementation. Most of the indications received answers: conduct training for employees, employee engagement, and appropriate support of the office management (Figure 4).

Figure 4. Elements that had a significant impact on the GDPR implementation



Source: Author's own research.

As an additional element, one of the offices indicated cooperation with experts in the field of personal data protection.

4.4. The GDPR impact on personal data management

In another question, "What do you think GDPR has changed in the approach to personal data management," the officials indicated that the GDPR implementation has raised employees' awareness of the protection of personal data, structured the process of personal data processing and influenced the development of appropriate documentation.

The remaining answers received indications according to the graph (Figure 5).

Figure 5. Answers to the question: “What do you think GDPR has changed in the approach to personal data management”



Source: Authors' own research.

Moreover, two officials pointed to two aspects of the GDPR implementation:

- discouraged employees from the idea of personal data protection due to increased responsibilities,
- raised citizens' awareness of their rights under data protection legislation.

4.5. Requests from data subjects

Next question was: “Since the GDPR implementation, has the office received any requests from data subjects arising from the data:

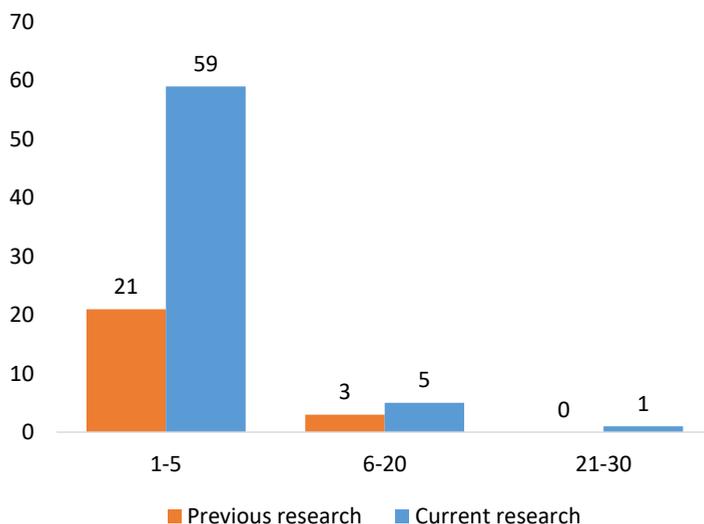
- the right of access to their data and to receive a copy of them,
- the right to rectify their data,
- the right to delete personal data when the data processing is not carried out to fulfil an obligation arising from a legal provision or to exercise public authority,
- the right to restrict data processing?”

Such applications were received in the case of 49 offices. And for the question concerning the number of such applications from the ranges <1-50>, <51-100>, <101-500>, <501-1000>, and over 1000, all respondents indicated the first range. Three applications were received in marshal offices, 11 in district offices, and 35 in municipal offices.

4.6. Personal data protection breaches

Officials have also been asked to indicate whether there have been breaches of personal data protection since the GDPR implementation in the office. Among 368 offices, 67 (18%) indicated that there have been such breaches (marshal office – 3, district office – 11, and municipal office – 53). Two offices declared breaches but did not indicate their number. The results were compared with the previous study (Figure 6). Only 24 (5%) surveyed offices declared that there has been a case of personal data security breach during the last year before the GDPR implementation (21 of them had one to 5 breaches and 3 offices – from 6 to 20 cases).

Figure 6. Numbers of personal data protection breaches indicated by officials, previous research – 24 offices, current research – 65 offices



Source: Authors' own research.

It can be seen that with a smaller sample size (462 for the previous and 368 for the current research), there has been an increase in the number of offices where personal data breaches occurred (24 for the previous and 67 for the current research). There are more infringements in general and more situations where more than one infringement has occurred. There are more cases in all ranges, so there is a clear increasing trend in the number of such cases. Furthermore, the structure has changed – there is a higher percentage of offices where few infringements have been detected. Only one office declared a higher number than 20 breaches.

The officials indicated the types of personal data breaches (Table 4).

Table 4. Types of personal data protection breaches indicated by officials according to the classification of the Personal Data Protection Office (current research)

Type of personal data protection breaches according to the classification of the Personal Data Protection Office	Number of indications
Personal data sent to the wrong recipient	19
Incorrect personal data anonymization in the document	16
Unauthorized access to information	15
Unintentional publication	10
Paper documentation (containing personal data) lost, stolen or left in an unsecured location	8
Paper correspondence lost by the postal operator or opened before returning it to the sender	7
Disclosure of the data of the wrong person	6
Lost or stolen media/device	5
Software interfering with confidentiality, integrity and data availability	5
Unauthorized access to information by breaking security	2
Verbal disclosure of personal data	1
Obtaining confidential information by a seemingly trusted person in official electronic communication, such as e-mail or internet messenger (phishing)	0
Incorrect removal/destruction of personal data from the media/electronic device before its sale by the controller	0

Source: Authors' own research.

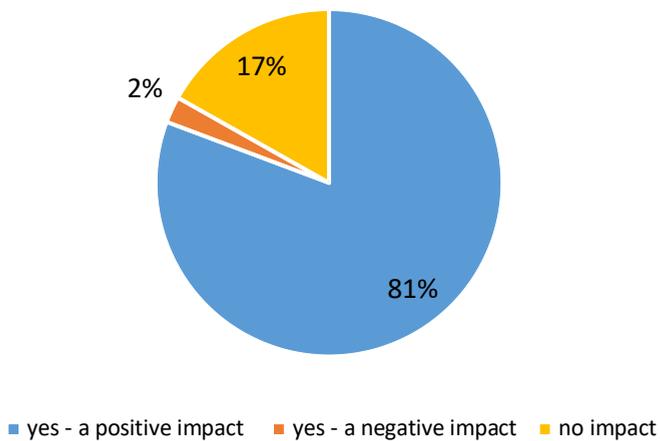
Other 13 officials declared breaches of personal data security outside the questionnaire directory: publishing data on the Public Information Bulletin website, greater scope for data processing, a lost letter by the Polish Post Office, temporary loss of availability – interruption of power supply due to transformer station failure, an unintended publication of data, limitation of data availability, a software error that caused data loss, failure of the telecommunications network, leaving documentation unsecured at the office, unauthorized activities of the processor, lack of power supply, breach of key management procedure, false e-mails, not hiding e-mail address while sending, loss of availability of copies of data on the server by hackers attacks.

4.7. The GDPR impact on overall information security management

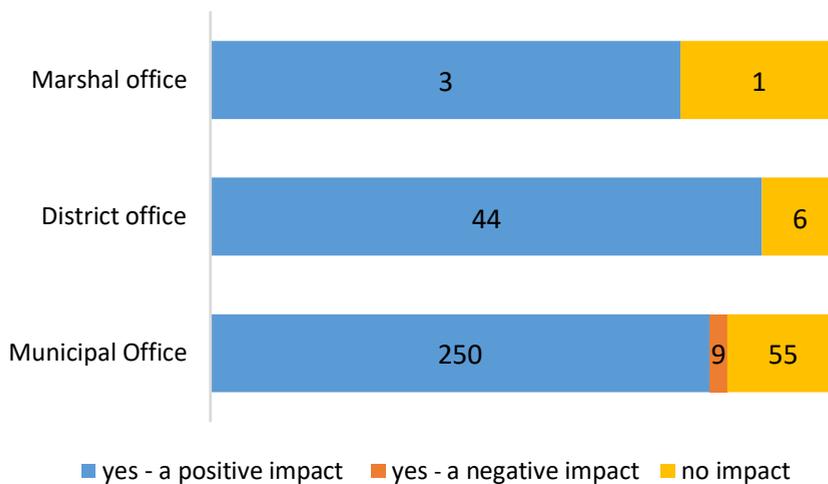
The last substantive question was as follows: “In your opinion, did the GDPR entry into force and related activities have an impact on the overall management of information security (not only personal data) in the office?” The answers are shown in Figure 7.

Figure 7. The impact of the GDPR on the overall management of information security (not only personal data) in the offices: a) general data and b) by type of office

a)



b)



Source: Authors' own research.

The vast majority of the respondents declared that the GDPR implementation had a positive impact on the overall management of information security.

5. Discussion

Data privacy law has undergone a massive change. This was a significant challenge to make the required changes and ensure compliance with GDPR, especially for public entities that have experienced many problems with this process. The results of the study revealed that not all offices have implemented the changes resulting from GDPR in time (Q1). This could be a result of many problems that had been reported during previous research. Another aspect is a limited budget. Over 65% of offices allocated less than PLN10,000 for this purpose, but this is not enough to ensure compliance with GDPR (Q2). This amount is less than the average monthly salary of a senior IT security specialist in a large corporation (Sedlak & Sedlak, 2020). At all levels of the offices (marshal, district, and municipal), this response was indicated most often.

Nevertheless, officials did not identify 'sufficient financial resources' as a key element in implementing the changes resulting from GDPR. In officials' opinion 'conducting training for employees', 'employee engagement' and 'appropriate support of the office management' have a significant impact on this process (Q3).

GDPR has changed the approach to personal data management, especially it raised employees' awareness of the protection of personal data (Q4).

Only 13% of the offices received requests from data subjects during the period under research (Q5). The majority of respondents (81%) claimed that the GDPR entry into force and related activities have a positive impact on the overall information security management. This means that by adopting organizations to the changes resulting from GDPR, the level of information security is also being improved in general (Q7).

Comparing the results of the survey with the previous data, it can be seen that previously, officials declared that their offices were not prepared to implement GDPR and only 21% had an implementation strategy. The current survey confirmed that not all changes were implemented in time.

Although both studies were conducted on different samples and at different intervals, there is a clear strong upward trend in the number of offices reporting personal data protection breaches, especially taking into consideration that the number of offices participating in the current survey is lower than in the previous one. This may be explained either by a real increase in dangerous situations or by higher sensitivity and tendency to report incidents because of fears of financial penalties under the general data protection regulation.

The most popular infringements were: personal data sent to the wrong recipient, incorrect personal data anonymization in the document and unauthorized access to information (Q6). The ‘other’ element has taken a rather high position. This means that respondents have problems with the allocation of the type of infringement or that the infringement catalogue prepared by Personal Data Protection Office is not sufficient. The administration officials could have problems with notification of a personal data breach. The lack of complete reports of infringements by regulators in some EU countries makes it difficult to make comparisons and to draw broader conclusions in this regard.

6. Conclusions

The research concerns a relatively new subject. The state of personal data protection in public administration in Poland after 18 months of the GDPR implementation was analyzed. The research findings were compared with the data obtained from our previous research. As far as we know, there is no comprehensive research that has been conducted into this field in the local government administration in Poland.

The research results provide comparative material for other analyses conducted in the next the GDPR period. They also establish a knowledge base for officials who are responsible for information security management. In order to improve the GDPR implementation, public administration offices should place emphasis on GDPR training for employees, engage employees in the GDPR adoption, support employees activities by top management, and raise citizens’ awareness of their rights under data protection legislation.

It is also important to stress the limitations of the survey, in which we examine the opinions of respondents and the fact that the questionnaire survey was conducted only in Poland, thus the potential recipients of the research results will be Polish citizens. This does not exclude recipients from other countries who would like to obtain information to conduct comparative analyses. Another limitation is the relatively low responsiveness of the questionnaire survey.

The above implies the need for further research in this area. It would be appropriate to conduct a similar survey in the next time interval. It would also be interesting to extend the research to other European Union countries.

References

- Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, 21(4), 402-418. <https://doi.org/10.1108/DPRG-01-2019-0007>
- Breitbarth, P. (2019). The impact of GDPR one year on. *Network Security*, 7, 11-13. [https://doi.org/10.1016/S1353-4858\(19\)30084-4](https://doi.org/10.1016/S1353-4858(19)30084-4)
- DLA Piper. (2020). *GDPR Data Breach Survey 2020*. Retrieved from <https://www.dlapiper.com/en/global/insights/publications/2020/01/gdpr-data-breach-survey-2020/>
- European Parliament. (2016). 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). Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Fazzini, K. (2019). *Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators*. Retrieved from <https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html>
- Ferreira, A. (2020). GDPR: What's in a year (and a half). In J. Filipe, M. Smialek, A. Brodsky, & S. Hammoudi (Eds.), *Enterprise information systems, Proceedings of the 22nd International Conference, ICEIS 2019* (Vol. 2; pp. 209-216), Science and Technology Publications, Berlin: Springer. <https://www.doi.org/10.5220/0009386002090216>
- Forbes Technology Councils. (2018). *15 Unexpected Consequences of GDPR*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#7affb2c994ad>
- GDPR Enforcement Tracker. (2020). *Fines database*. Retrieved October 10, 2020 from <https://www.enforcementtracker.com/>
- Jatkiewicz, P. (2015). Zarządzanie bezpieczeństwem w jednostkach samorządowych [Security management in local government units]. In T. Szatkowski (Ed.), *Bezpieczeństwo danych w sektorze publicznym* [Data security in the public sector]. Warsaw: PTI. Retrieved from <https://ir.pti.org.pl/wp-content/uploads/2017/02/Biblioteczka-Izby-Rzeczoznawc%C3%B3w-PTI-Tom-4.pdf>
- Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security*, 6, 5-8. [https://doi.org/10.1016/S1361-3723\(17\)30050-7](https://doi.org/10.1016/S1361-3723(17)30050-7)
- Laybats, C., & Davies, J. (2018). GDPR: Implementing the regulations. *Business Information Review*, 35(2), 81-83. <https://doi.org/10.1177%2F0266382118777808>
- Lisiak-Felicka, D., Szmit, M., & Szmit, A. (2019). The assessment of GDPR readiness for local government administration in Poland. In Z. Wilimowska, L. Borzemski, & J. Świątek (Eds.), *Information systems architecture and technology* (Advances in Intelligent Systems and Computing, Vol. 854; pp. 417-426). Berlin: Springer. https://doi.org/10.1007/978-3-319-99993-7_37

- Lisiak-Felicka, D., Szmit, M., Szmit, A., & Vaičiūnienė, J. (2020). GDPR implementation in local government administration in Poland and Republic of Lithuania. In Z. Wilimowska, L. Borzemski, & J. Świątek (Eds.), *Information systems architecture and technology* (Advances in Intelligent Systems and Computing, Vol. 1052; pp. 49-60). Berlin: Springer. https://doi.org/10.1007/978-3-030-30443-0_5
- Sedlak & Sedlak. (2020). *Ile zarabia specjalista ds. bezpieczeństwa informatycznego? Raport wynagrodzeń* [How much does an IT security specialist earn? Salary report]. Retrieved October 10, 2020 from <https://wynagrodzenia.pl/moja-placa/ile-zarabia-specjalista-ds-bezpieczenstwa-informatycznego>
- Tamburri, D. (2020, July). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 91, Article 105454. <https://doi.org/10.1016/j.is.2019.101469>
- Tatara, U., Gokceb, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, 38, Article 105454. <https://doi.org/10.1016/j.clsr.2020.105454>
- UODO. (2019a). *Decyzja Prezesa Urzędu Ochrony Danych Osobowych ZSPU. 421.2.2018* [Decision ZSPU.421.2.2018 of President of the Personal Data Protection Office]. Retrieved from <https://uodo.gov.pl/decyzje/ZSPU.421.2.2018>
- UODO. (2019b). *Decyzja Prezesa Urzędu Ochrony Danych Osobowych ZSPU. 421.3.2019* [Decision ZSPU.421.3.2019 of President of the Personal Data Protection Office]. Retrieved from <https://uodo.gov.pl/decyzje/ZSPU.421.3.2019>
- UODO. (2019c). *Decyzja Prezesa Urzędu Ochrony Danych Osobowych ZSPU. 421.8.2018* [Decision ZSPU.421.8.2018 of President of the Personal Data Protection Office]. Retrieved from <https://uodo.gov.pl/decyzje/ZSPU.421.8.2018>
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) [Act of 10 May 2018 on Personal Data Protection (Journal of Laws of 2018, item 1000)]. Retrieved from <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>
- Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990 nr 16 poz. 95) [Act of 8 March 1990 on municipal government (Journal of Laws of 1990, No. 16, item 95)]. Retrieved from <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900160095>
- Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. 1998 nr 91 poz. 578) [Act of 5 June 1998 on district local government (Journal of Laws of 1998, No. 91, item 578)]. Retrieved from <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910578>
- Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz.U. 1998 nr 91 poz. 576) [Act of 5 June 1998 on the voivodeship self-government (Journal of Laws of 1998, No. 91, item 576)]. Retrieved from <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910576>

-
- Ustawa z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz.U. 1998 nr 96 poz. 603) [Act of 24 July 1998 on the introduction of a basic three-tiered territorial division of the country (Journal of Laws of 1998, No. 96, item 603)]. Retrieved from <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19980960603>
- Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, 6, 8-11. [https://doi.org/10.1016/S1353-4858\(17\)30060-0](https://doi.org/10.1016/S1353-4858(17)30060-0)
- ZFODO. (2020). *Incydenty ochrony danych osobowych. Raport Związku Firm Ochrony Danych Osobowych* [Personal data protection incidents. Report of the Association of Personal Data Protection Companies]. Retrieved from https://www.zfodo.org.pl/wp-content/uploads/2020/02/raport_zfodo_naruszenia-16.02.20.pdf