






The Assessment of GDPR Readiness for Local Government Administration in Poland

Dominika Lisiak-Felicka¹ , Maciej Szmit² ,
and Anna Szmit³ 

¹ Department of Computer Science in Economics,
University of Lodz, Lodz, Poland
dominika.lisiak@uni.lodz.pl

² Department of Computer Science, University of Lodz, Lodz, Poland
maciej.szmit@uni.lodz.pl

³ Department of Management, Lodz University of Technology, Lodz, Poland
anna.szmit@p.lodz.pl

Abstract. The article presents the most important changes introduced by the 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). The processing of personal data takes place in various spheres of economic and social activity, including public administration. The article presents results of the Computer Aided Web Interview (CAWI) survey that has been conducted among local government administration offices in Poland between March and April 2018. The aim of the research was to determine the degree of preparation of local government administration to implement changes resulting from the GDPR, and to identify sources and forms of support and problems in the implementation of these changes. On the basis of the conducted survey, an assessment the General Data Protection Regulation readiness for local government administration was performed and presented.

Keywords: General data protection regulation (GDPR) · Data protection
Local government administration

1 Introduction

The 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) will take effect on the 25th of May, 2018 [9]. Entities will have to make considerable efforts to get their data protection system into compliance with the GDPR [16, 17].

It lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and protects fundamental rights and freedoms of natural persons and in particular their right

to the protection of personal data [9]. GDPR defines the conditions that the entities that process personal data will have to implement. The most important of them are (see e.g. [2–6, 8, 11]):

- extended rights of the data subject,
- Data Protection Officer position,
- information obligation and consent to data processing,
- notification of a personal data breach obligation,
- administrative fines,
- records of processing activities,
- processor and responsibility,
- data protection by design and by default [7, 10],
- data protection impact assessment,
- limitations on profiling.

As a part of the research, it was planned to check if the local government administration offices in Poland are prepared to implement changes resulting from the GDPR. Data protection in these units are directly concerned with personal data protection of citizens. Offices are processing data on the basis of legal regulations and everyone of citizens transfers his/her personal data to the office.

The administrative division of Poland is based on three organizational levels [12]. The territory of Poland is divided into voivodeships (provinces, “województwo” in Polish); these are further divided into districts (“powiat” in Polish), and these in turn are divided into municipalities (“gmina” in Polish). Major cities have the status of both gmina and powiat [13–15]. There are currently: 16 voivodeships, 380 districts (including 66 cities with districts status), and 2,478 municipalities in Poland.

The organizational units whose aim is to provide assistance to 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.

2 Method

The aim of the research was to determine the degree of preparation of local government administration to implement changes resulting from the GDPR, and to identify sources and forms of support and problems in the implementation of these changes. The survey has been conducted using Computer Aided Web Interview (CAWI) method between March and April 2018.

The survey invitation was sent by email 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 questionnaire was anonymous.

The questionnaire had been available on the web for a few weeks and 462 offices decided to participate in the survey: 6 offices at the voivodeship level (marshal offices), 66 at the districts level (district offices) and 390 at the municipalities level (municipal offices). Figure 1 presents their location structure. Table 1 presents the numbers of employees in the offices.

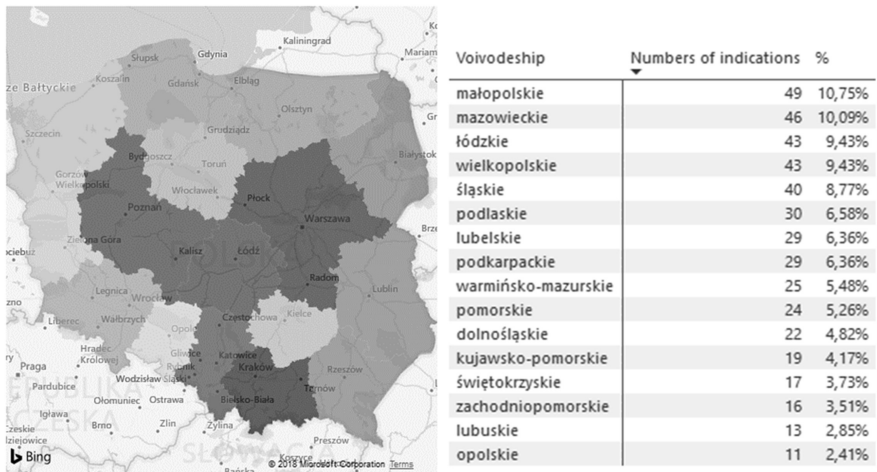


Fig. 1. The geographical location of offices participating in the survey. Due to the anonymous survey, the marshal offices were not asked about the location because of the possibility of identification (in each voivodeship there is one marshal office). Source: own survey.

Table 1. Numbers of employees in the offices. Source: own survey.

Numbers of employees	Numbers of offices	%
up to 50 people	279	60,39%
51 to 100 people	104	22,51%
101 to 500 people	59	12,77%
501 to 1,000 people	7	1,52%
1,001 to 2,000 people	7	1,52%
2,001 to 3,000 people	4	0,87%

The structure of municipal offices responded to the survey were similar to the structure in Poland (chi-squared test p value = 0,044) – see Fig. 2.

Also the percent of different types of municipalities were similar in the sample and in the whole country – see Fig. 3.

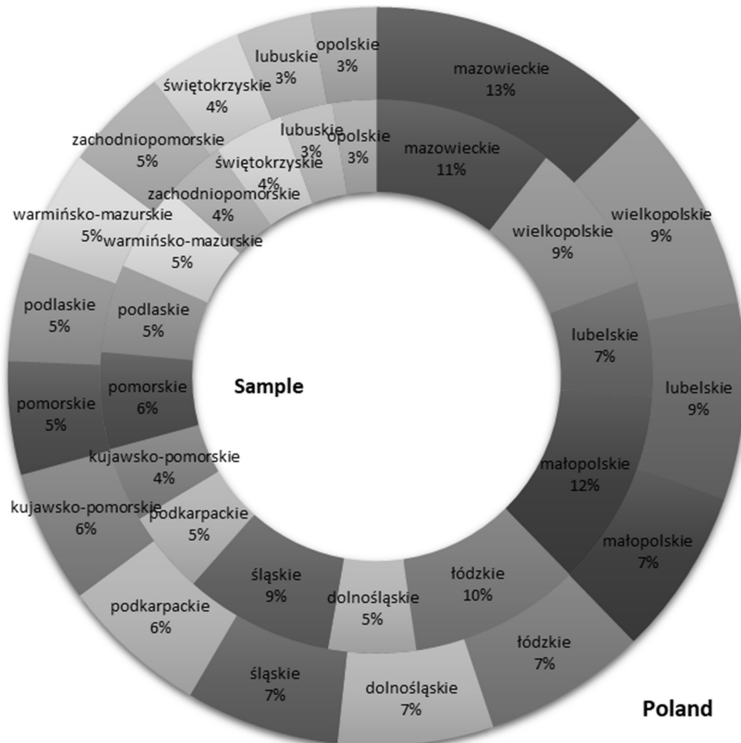


Fig. 2. The percentage structure of municipal offices in the sample and in Poland. Source: own survey.

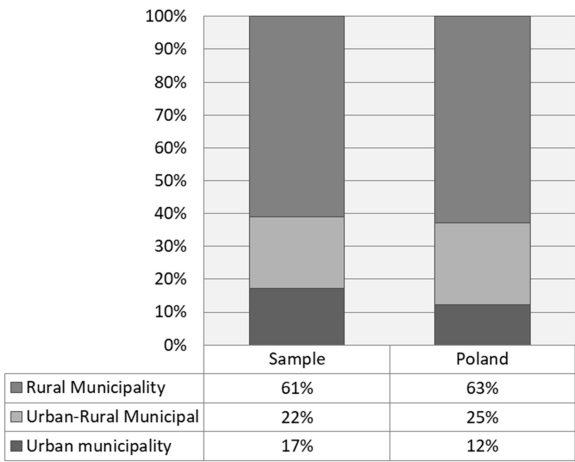


Fig. 3. The percentage structure of types of municipal offices in the sample and in Poland. Source: own survey.

3 Results

Among 462 offices, only 96 (21%) formally defined implementation strategy for the GDPR (objectives, deadlines, responsible persons, procedures), but only 12 of them provided a link or attached a file that includes strategy specification. Other respondents did not want to include attachment or they declared that the strategy is in preparation.

Only 32 offices (7%) defined the indicators of readiness/maturity of the GDPR implementation, such as following (described by offices):

- % of trained employees, % of updated documentation, % of contracts/annexed contracts for entrusting data processing that complying with the requirements of the GDPR;
- completing tasks specified in the schedule on time;
- measures corresponding to the requirements of specific GDPR articles;
- checklists;
- monitoring of changes in regulations, participation in training;
- training, documentation preparation, security policy, records of processing activities, risk analysis,
- method of conducting the audit, DPO appointment;
- preparation of appropriate documentation, introduction of changes in the security level of IT systems and access control, development of training improving employees' competences;
- developing procedures in the required time;
- performance measures, in the context of the organization's objectives, time intervals, integrity and confidentiality, storage constraints, correctness, data minimization, purpose limitation, legal compliance, reliability and transparency;
- deadlines for projects, persons responsible for implementation, annotations on performance;
- threats, list of incidents;
- specified in the contract with the company.

The evaluation process of the GDPR implementation is conducted at the 139 offices (30%), in 92 cases by self-evaluation and the others by an external company. The evaluation tools are used in 32 offices. These includes:

- computer programs;
- information security risk analysis, data encryption programs, backup programs and fast recovery;
- forms, questionnaires, analyses;
- documentation review,
- training;
- security analysis;
- observation, interview, document analysis;
- self-control, functional control;
- planning, information gathering, analysis and evaluation, evaluation of the objectives implementation;
- analysis of resources and documents, observations, data sets;

- checking the legality, adequacy, purpose and scope of data processing; auditing, among others the area of data processing, access to the area; risk assessment; updating of data protection documentation, including authorizations; analysis of entrustment agreements; consents analysis; updating the content of the information obligation; analysis of data sets, etc.;
- verification card, information on the stand, application verification,
- ordinance;
- interviews with employees, case analysis, data sets;
- inventory of personal data processing processes, identification of risks and control mechanisms;
- risk management method.

Respondents were asked to assess the degree of office readiness for implementing changes resulting from the GDPR? (on a scale of 1 to 5, where 1 – no readiness, 5 – all GDPR requirements have been already implemented). Results are shown on Fig. 4.

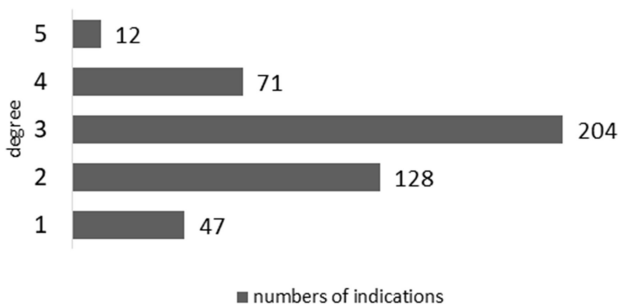


Fig. 4. Degrees of office readiness for implementing changes resulting from the GDPR. Source: own survey.

In the next question respondents were asked to specify the level of difficulty in implementing changes resulting from the GDPR to the office on a scale of 1 to 5 (1 – very easy, 5 – very difficult). Results are shown on Fig. 5. The most difficult for the respondents are: data protection impact assessment, data protection by design and by default and Data Protection Officer hiring. On the other hand a lot of respondents assessed DPO position as very simple change.

Among 462 offices, 216 (47%) declared that they use or plan to use the services of an external company to help in the implementation of requirements brought forward by the GDPR.

Figure 6 shows the answers on the question: Who is responsible for ensuring the security of personal data in the office?

The 18 respondents indicate also: data administrator (controller), contracted person, employees and external company, all office workers, data security administrator, municipality heads, unit manager and office manager.

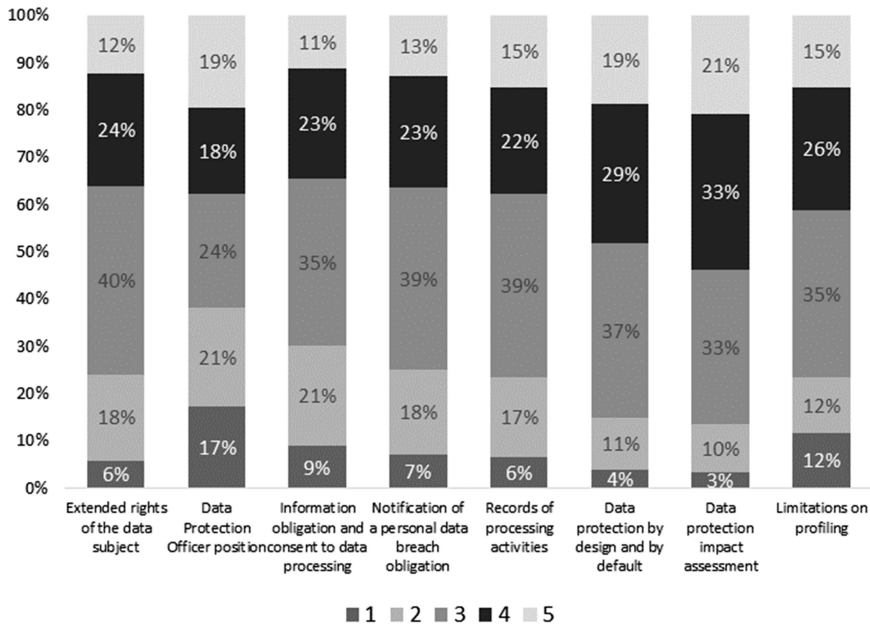


Fig. 5. The assessment of difficulty in implementing changes resulting from the GDPR. Source: own survey.

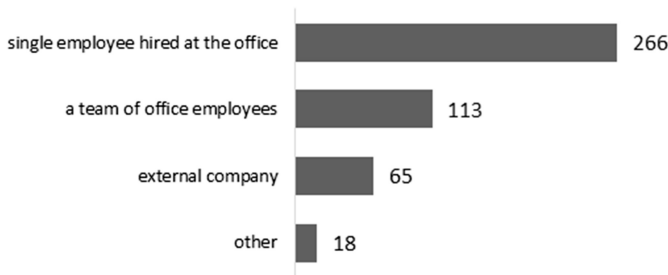


Fig. 6. Responsibility for ensuring the security of personal data in the office. Source: own survey.

Only 24 (5%) offices declared that there have been a case of personal data security breach during the last year (21 of them had one to 5 breaches and 3 offices – from 6 to 20 cases).

About one-third respondents receive support from higher organizations regarding the implementation of the GDPR. Table 2 presents types and sources of support.

Only 75 (16%) offices are conducting training on the changes resulting from the GDPR and all employees have been trained, 201 (44%) offices are conducting training but not all employees have been trained yet and 186 (40%) offices are not conducting such training.

Table 2. Types and sources of support. Source: own survey.

Type	Source
Training	conducted by for e.g. external company, voivodeship office, district office, the Poviats Association, Municipals Association, National Institute of Local Government, Regional Chamber of Accounts, Ministry of digitization, Foundation for the Development of Local Democracy, Regional Institute of Local Government and Administration, centers of education and self-government studies; regional projects
Information materials, brochure, interpretations, consultation, www	from the Inspector General for the Protection of Personal Data (GIODO in Polish), Association of Information Security Administrators
Conferences, webinars	GIODO, voivodeship office, higher organizations
Publications	from the Internet, specialized web pages devoted to GDPR, GIODO, LEX Wolters Kluwer, ABIExpert, Successpoint, legal guides on personal data protection, subscription to dedicated magazines
Consultations	with external companies, using the services of specialists in the personal data protection

Respondents were asked to indicate the biggest concern (in their opinions) in preparing the office for the GDPR implementation. They mentioned the following problems (grouped in legal, financial, organizational, essential and human aspects):

- legal – the Polish Personal Data Protection Act has not been adopted yet (during the article development process), the rules are unclear, the absence of specific legal acts, implementing regulations and specific guidelines;
- financial – the lack of sufficient financial resources for the GDPR implementation;
- organizational – the lack of time, excess of duties, lack of support from superior authorities, problem in finding qualified staff;
- essential - problems with the procedures implementation, preparation of documentation, risk analysis and assessment, implementation of tasks resulting from changes introduced in the GDPR, technical barriers, lack of tested solutions;
- human - resistance and reluctance against changes, lack of awareness of employees and management staff, lack of sufficient knowledge about GDPR.

4 Discussion and Conclusion

On the basis of the research it can be concluded, that the surveyed offices will have a huge problem with the implementation of changes resulting from the General Data Protection Regulation (GDPR) in the required time. A large group of respondents have not defined even the implementation strategy for the GDPR.

There is no doubt that all actions concerning GDPR implementation are taken too late. The readiness for implementing changes seems to be insufficient, especially taking into account the near deadline. At the same time responders' self-assessment of the readiness seems to be overstated. The degrees are more related to the choice of the middle element of scale instead of a reliable analysis of the situation at the office. Offices can only count on support from superior authorities in the field of training and information activities. The other alarming conclusion concerns immaturity of implementation approach itself. Only minor part of offices defined strategy, maturity measures or performed any evaluation of the process. This indicates a lack of a process approach.

As the biggest problems in GDPR implementation offices indicate: lack of Polish Personal Data Protection Act, unclear rules, the absence of specific legal acts, implementing regulations and specific guidelines. There is a fear that after the development and implementation of changes, the Act will introduce some additional rules/procedures and offices will have to adapt it again. Respondents listed also: lack of financial, time and human resources, problems with the procedures implementation and resistance and reluctance against changes by officers.

However, it should not be a surprise that the offices are not prepared to GDPR implementation, when even the Inspector General for the Protection of Personal Data declares that it is also not prepared for this Regulation [1].

References

1. Biekak-Jomaa, E.: Wdrożenie RODO w Polsce zagrożone. <https://www.giodo.gov.pl/pl/1520281/10380>. Accessed 20 Apr 2018
2. Ferrara, P., Spoto, F.: Static analysis for GDPR compliance. Paper presented at the CEUR Workshop Proceedings, vol. 2058 (2018)
3. Gellert, R.: Understanding the notion of risk in the General Data Protection Regulation. *Comput. Law Secur. Rev.* **34**(2), 279–288 (2018)
4. Kolah, A., Foss, B.: Unlocking the power of data under the new EU General Data Protection Regulation. *J. Direct Data Digit. Mark. Pract.* **16**(4), 270–274 (2015). <https://doi.org/10.1057/dddmp.2015.20>
5. Krystlik, J.: With GDPR, preparation is everything. *Comput. Fraud Secur.* **2017**(6), 5–8 (2017)
6. Lisiak-Felicka, D., Nowak, P.: Wybrane aspekty zarządzania bezpieczeństwem informacji w podmiotach prowadzących działalność leczniczą. *Przedsiębiorczość i Zarządzanie, Społeczna Akademia Nauk, Łódź-Warszawa* (2018). (in print)
7. O'Connor, Y., Rowan, W., Lynch, L., Heavin, C.: Privacy by design: informed consent and internet of things for smart health. *Procedia Comput. Sci.* **113**(2017), 653–658 (2017)
8. PWC: 10 najważniejszych zmian, które wprowadza RODO. <https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rod.html>. Accessed 20 Mar 2018
9. 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)

10. Romanou, A.: The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Comput. Law Secur. Rev.* **34**(1), 99–110 (2018)
11. Tikkinen-Piri, C., Rohunen, A., Markkula, J.: EU General Data Protection regulation: changes and implications for personal data collecting companies. *Comput. Law Secur. Rev.* **34**(1), 134–153 (2018)
12. Ustawa z 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz. U. z 1998 r. Nr 96, poz. 603)
13. Ustawa z 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 Nr 142, poz. 1592, z późn. zm.)
14. Ustawa z 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 1590 z późn. zm.)
15. Ustawa z 8 marca 1990 r. o samorządzie gminnym, (Dz. U. z 2001, nr 142, poz. 1591, z późn. zm.)
16. Voight, P., von dem Bussche, A.: The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer International Publishing AG (2017). <https://doi.org/10.1007/978-3-319-57959-7>
17. Zerlang, J.: GDPR: a milestone in convergence for cyber-security and compliance. *Netw. Secur.* **2017**(6), 8–11 (2017)