THE CLOUD COMPUTING APPROACH IN PUBLIC SECTOR

Anna KACZOROWSKA

Summary: In the society using more and more mobile technologies, the management of the key documentary processes (including also their use for interaction with clients, human resources management, as well as the management of finances, reporting and accountancy) in and between the public sector organizations is very difficult. The article shows that the cloud computing approach may significantly improve the management of information, especially the main documentary processes in offices, but requires special attention paid to legal issues, as well as the personal data security and protection. Besides, the type of a cloud best for the public sector was proposed, along with the components of a safe agreement with the cloud service provider.

Key words: public cloud computing, private cloud computing, hybrid cloud computing, PaaS, IaaS.

1. The cloud computing conditions in public administration

The public sector considers now a possibility of adapting the cloud computing from the private sector (as it once did with project management). The studies carried out by Microsoft on implementation of the cloud computing in private enterprises indicates that the savings of the site, time and especially the costs associated with the purchase of teleinformation infrastructure may reach as much as 80%. The forecast value of the IT sector incomes generated from the cloud services provision is to be almost doubled. In 2010 this value reached approx. 1.2 billion PLN, whereas in 2013 it was to grow to about 8.3 billion PLN [1].

The public administration entities are expected first of all to provide actually needed e-services to the more and more mobile society. As many as 83% of organizations from the public sector confirm [2] that they have access to such devices as smartfon or tablet, but their use is inhibited by obsolete information systems. In addition, the existing division between the technologies supplied to the front office and back office results in delays in access to necessary public information and threats to its security.

Report [2] shows also that the „big data" phenomenon (91% of the respondents) and cooperation with many suppliers largely affect the organization's processes management. Only 33% of the investigated organizations established the objectives for their documentary processes in a way which allows to overcome the problem of too many data. In the light of such results of the report the key processes in the organization may be encumbered with documents and may directly affect offices interactions with clients and employees.

The cloud service providers will not perform any public administration tasks but will only supply space on virtual disks and computing power of the processor (Infrastructure as a Service) or an operating platform (Platform as a Service), possibly with the implemented appropriate software (Software as a Service). So what will happen will exclusively be supplying the IT resources enabling accomplishment of public tasks.

In public sector the solutions based on cloud computing are used by the Central Registration and Information on Business (CEIDG), Public Information Bulletin (BIP) of the Prison Service and internal systems of making information available and documents circulation, e.g. in the General Directorate for National Roads and Highways (GDDKiA).

The benefits of the use of cloud computing in all sectors are:

- decreased investments in equipment and software;
- decreased personal costs of ICT departments;
- easier access to information;
- increased sharing of knowledge;
- assured permanent access to e-services for many recipients;
- scale economy.

On the other hand, the most important limitations which have to be considered in detail before using the cloud computing are: [3]:

- lack of impact on software (also its updatings) used by the provider of services;
- seizure of hardware or loss of financial liquidity of the provider of services;
- loss of control of access to employees' data and data flow, e.g. cloud federations;
- loss of control of the compliance with data protection requirements;
- increased risk of a change, loss, destruction or damage of data;
- non-liability to notification duty;
- higher vulnerability to hacking and hackers' attacks;
- poorer anti-virus protection;
- increased failures (frequent lack of access to resources);
- lack of economic profitability.

1.1. Specificity of cloud computing and its classifications

The concept of the cloud computing solution dates back to the year 1960 when the American computer scientist John McCarthy wrote that calculations might one day be organized as a public utility service. The name itself most probably comes from graphic presentations of clouds used for symbolic presentations of Internet in various studies.

In its contemporary meaning this term was for the first time used in 1997 during a lecture delivered by Ramnath Chellapp who defined the cloud computing as a paradigm in which the calculation services limit will be established by economic reasons and not by technological limitations.

The cloud computing is defined as a model of data processing in which many recipients provide IT solutions of high scalability in a mass way, in form of a service, by electronic medium which is Internet (such definition is presented by the Gartner Inc research centre [4]). Conceived like this, the cloud should not be understood as a new technology but rather as a new approach to IT solutions construction. Customers may obtain an access to a given network space, the computing power resources in almost real time, and release them when they are no longer needed. In other words, it is a service of using the co-shared IT resources.

The cloud phenomenon results from the present world economy situation and redefinition of the role of IT departments in organizations. The cloud allows for flexible adjustment to changes. The cloud computing helps to react "on an on-going basis", without incurring unnecessary costs on the demand for an additional space on servers, additional

hardware, licenses etc., and consequently allows to „have one's finger on the pulse", which is an important element of the competitive advantage.

Depending on the extent of the user's control of IT infrastructure and resources, three basic levels of cloud computing are singled out, as characterized in Table 1:

Tab. 1. Characteristics of the levels of cloud computing

No	Acronym of the name	Full name of the level	Characteristics of the level
1	IaaS	Infrastructure as a Service	The service as infrastructure in which the user uses hardware (virtual Internet disks, CPU power) through the Internet
2	PaaS	Platform as a Service	The service is a platform owing to which the user apart from infrastructure obtains access to the operating environment allowing for independent installation and launching of application
3	SaaS	Software as a Service	The service in this case consists in providing a functional software through the Internet browser. Apart from the hardware infrastructure, with the operating system environment the service client obtains also access to specific applications (spreadsheets, accounting software) the functioning of which rests with the service provider

At the IaaS level the user controls his data and software, whereas the basic part of the infrastructure, which consists of servering and data warehouses, is leased from the cloud provider [5].

The PaaS service (see tab. 1) provides the user with an access to virtual computer. The role of the cloud's provider is increased here, because he accounts for providing the working environment (comprising also an appropriate infrastructure and instruments for designing the software) for the client who will continue to control the data and software. Examples of such services are: Google App Engine or Microsoft Windows Azure.

The SaaS software (tab. 1), such as for example Microsoft Business Productivity Suite, Google Mail or Salesforce.com, does not use local computing resources and does not have to be installed at the end user.

Another classification distinguishes the following types of clouds: public, private, dedicated and hybrid. The concept of the public cloud stipulates that the user wholly uses the service of an external provider of the cloud and other third entities (e.g. suppliers of external applications launched in the cloud) [6, p. 24]. Such a cloud computing arouses fears of the users, i.e. public administration and its clients, for safety of their data.

Such fears are not legitimate in the case of the so called private cloud, where the whole infrastructure is physically located in the area controlled by the user which may be the public administration.

Another type of cloud computing, the dedicated cloud, enables giving to a given user's exclusive disposal a separate part of the cloud, e.g. in the form of physically allocated servers.

On the other hand, hybrid clouds combine the use and location of data of the key importance and confidential information – in private cloud and location and processing of public information or the information which does not require any special protection – in the public cloud.

The use of the public or dedicated cloud computing is not connected with taking over, by the cloud provider, any public tasks encumbering the state or self-governmental administration, but exclusively with delivery of IT resources for their implementation.

All existing applications of the cloud computing in public administration use first of all the private cloud, where all infrastructure is owned by administration entities, whereas in the case of CEIDG – by the Minister of Economy.

An example of the use of the public cloud is the pilot implementation of Office 365, available from Microsoft, by the Association of Polish Towns and Association of Polish Counties.

1.3. Legal limitations on the use of cloud computing in public administration

The act of 17 February 2005 on informatization of the activity of the entities which perform public tasks (UINF; [7]) and order [8] based on it do not exclude the possibility to use the public cloud, but the functioning of the cloud computing is not regulated clearly in the public law. However, this does not mean that once the storage and processing of data are transferred to the cloud, the regulations which determine the activities of respective public administration organs, establishing for them the information security requirements, will become invalid. Acts [7] and [8] assume that teleinformation systems used in the cloud should at least meet the technological requirements and those related to security and protection procedures stipulated in Polish standards (especially PN 2700) or those used by the European Union (EU), whereas where these are missing – the internationally acknowledged standards published by the Internet Engineering Task Force or World Wide Web Consortium (W3C).

UINF assumes that when providing the cloud computing it is sufficient that the service provider indicates the assumed standards and formats used in computer science without the obligation to reveal detailed technological data of applied teleinformation solutions.

However, the use of the cloud computing is tantamount to assignment of the control of IT resources to another entity or usually several entities with which the cloud provider cooperates. An important issue is then to establish the legal nature of the relationship connecting the cloud provider with the entity which is the IT resources disposer. Usually it will be a civil law relationship, but it is possible that the cloud provider for public organization will be another budgetary unit. In most cases, the relationship between the parties will be regulated by the agreement for providing services, to which regulations about the order apply.

Assignment of the control of IT resources is usually connected with revealing the personal data included in these resources, therefore the entities planning to use the cloud computing, especially the public cloud, should find out the type of that disclosure in the light of the *Act on personal data protection* ([9]; UODO). On the ground of this act, the following two ways of showing the personal data are singled out:

1. Entrusting the processing (art. 31 UODO, sec. 1 and 2) – the entity (processor) to which personal data processing was entrusted may process them to the extent and purpose stipulated in the agreement;
2. Availability – when information about natural persons is revealed, the administrator gives another entity access to personal data; assumingly, the public administration entity shows then the data needed by the entity to which they were made available.

In Poland for most of the services of data processing in the cloud the civil law agreement of entrusting the personal data processing applies. The cloud provider's task is usually mediation in giving access to technological infrastructure belonging to other entities with which (according to UODO) agreements of entrusting personal data processing should be concluded. What happens then is sub-entrusting, i.e. further entrusting of personal data processing. So legal relationships between the parties may be multi-level, where on the lowest level of that system there is more than one entity [18].

We deal with personal data availability when cloud providers, apart from payment for providing the service, want to obtain an additional benefit in form of a possibility to process personal data contained in the service client's resources, for instance if they want to carry out marketing research on them. The legal nature of the relationship between the service client and the service provider changes then, because the service provider is both the processor and administrator of personal data.

In the agreement concluded for using the cloud computing, we should take into account the (organizational and technological) security of personal data and a special emphasis should be put on the rights and obligations connected with notifying of the public administration entity about breaking the security rules of the entrusted personal data, e.g. in connection with the control carried out by the General Inspector of Personal Data (GIODO) at the service provider.

Pursuant to art. 36 sec. 2 of UODO the data administrator is to conduct the documentation describing the data processing method as well as the technical and organizational measures assuring the processed data protection [10]. The executory act specifying the requirements to conduct such documentation is [10]. The Polish legislator requires also, from those processing personal data by virtue of the entrusting agreement, that they conduct the documentation on processing of such data.

On the other hand, section 3 art. 36 of UODO [9] imposes on the data administrator or the information security administrator designated by him, the general obligation to supervise the compliance with the personal data protection rules, whereas sec. 1 enacts the general obligation to secure such data.

The mentioned regulations of UODO may be comprehensively interpreted by GIODO Office employees who during a possible control may e.g. consider whether or not the agreement for entrusting the personal data processing authorises the administrator to access to the documents related to security rules and technical measures applied in respective processing centres. A huge provided of the cloud from the USA or SAR (South African Republic) will probably refuse also incorporating into the agreements a clause enabling a securities audit at the processor's site.

Regulations of the *Act on protection of secret information* [11] confine the use of the cloud computing in a different form than the private cloud. Its entries exclude the use of the technical measures of the third entities whom the provider entrusts with data processing. What happens then is further entrusting of data, i.e. sub-entrusting. Furthermore, these

measures must be at a site which is strictly controlled by the entity which processes or stores secret information.

The provider of the cloud may also be an entity based in the third country (from art. 7, sec. 7 UODO in a country which does not belong to the European Economic Area (EOG), such as e.g. the USA and South African Republic). In case of huge cloud providers from outside the EOG it may be difficult to comply with the obligation to stick to the written form of the agreement of entrusting the personal data processing, as well as the obligation to specify in it the scope and purpose of entrusting. According to the Polish law, the requirement of conducting the personal data processing should be met both by the cloud provider based in the Republic of Poland and the one whose registered seat is outside the EOG territory. However, this requirement does not have to be met by service providers from other EOG countries, but regulations of these countries may impose on cloud providers the requirements identical with those which were used by the Polish legislator.

Implementation of the cloud computing generates one more problem connected with the use of regulations of the *Public procurement law* [12] which impose on the client the need to precisely estimate the demand for the computing power, disk space sizes or bandwidth. Because of the cyclical nature and type of activities performed by public administration entities, associated with their duty to submit reports, returns and declarations at a specified time, it is allowed to determine the quantity of expected operations in the system and subsequently adjust the ordered resources to such fluctuations. In the case of underestimation or overestimation of IT resources the encumbered party will be first of all the service client who covers the costs of unused resources in case of overestimation or increases the order in case of underestimation of the demand. The errors made while constructing the Terms of Reference may even undermine the whole procurement procedure and cause the need to carry it out again if appeals lodged by other participants of the proceedings are accepted.

Applied to legal problems associated with the use of cloud computing is opinion 5/12 adopted by the Working Group Art. 29 for Data Protection on 1 July 2012 relating to data processing in cloud computing (WP 196; [13]).

Aiming at a further legal regulation of the use of cloud computing, on 27 September 2012 the European Commission (EC) announced a strategy on cloud computing [14], where the tasks presented in table 2 are indicated.

Tab. 2. Tasks in the EC strategy relating to cloud computing

No	Task
1.	Solving the problem of a set of standards used by the cloud computing clients
2.	Establishing the standards of data transfer
3.	Promotion of certification mechanisms mutual for the EU for reliable providers of cloud services
4.	Development of a pattern of „secure and honest" conditions for cloud computing agreements, including agreements with a guaranteed level of services.
5.	Establishment of European partnership for cloud computing with participating member states and branch entities for the development of the European market of cloud computing
6.	Increase in the competitiveness of European providers of cloud services to provide cheaper and better solutions within e-government

The public sector organization which wants to use the hosting service or backup in cloud should know that such a service as Dropbox or Google Apps has its own rules of use. And so, from available, under itwa.pl/2a, conditions of Dropbox service use (under itwa.pl/2b there are analogical entries for Google Apps for companies) it results that the provider may terminate or suspend the service providing agreement at any time. Such an entry may be a severe obstacle, when the client decides to enforce his rights at court.

Dropbox rules indicate that the service provider is the supplier of the Safe Harbor (itwa.pl/2c) agreement concluded between the EU and the USA, guaranteeing that providers from the USA will use appropriate levels of data securing as required by the European Union's directive 95/46/EC. If Dropbox service is a party to Safe Harbor, it could seem that it is free from the problem of transferring the personal data outside the European Economic Area (EOG).

However, according to Working Group Art. 29, the data transferring entities should not rely only on declarations of the organization to which they transmit the data, but should independently receive confirmation that the service provider has certificate Safe Harbor and observes its rules. For this purpose, page http://safeharbor.export.gov may be used and it should be checked when the confidence in a given service provider becomes invalid.

According to art. 48 of act [9], GIODO's consent may be a premise authorising the transfer of personal data beyond the EOG. Another important issue is the obligation to assure an appropriate security within the protection of privacy as well as the rights and freedom of the person to which the data refer. In practice, administrators fulfill this obligation while concluding agreements including standard contractual clauses, with data recipients. Standard contractual clauses are ready patterns of agreements established by the Commission's Decision of 27 December 2004 (itwa.pl/2d), the use of which is considered by the personal data protection organs as the guarantee of the use of the protection rules for such data, mandatory in the EOG.

1.4. Cloud computing optimal for public administration

In view of the type of the data whose administrators are public sector organizations, the proposed optimum solution is the use of hybrid cloud computing where the information under special protection would be processed in private cloud computing, whereas the open information, such as e.g. the data from BIP, in public cloud computing.

Because of complicated relationships which arise between the service client, service provider and its co-operators, the use of cloud computing faces many legal obstacles. If, for example, the cloud provider is an entity based abroad, the relationship between the parties may be regulated by legal provisions of another country.

Directive [10] determines, among other, the indispensable minimum of information which should be contained in the policy of the personal data processing security, a part of which is a list of buildings, premises or their parts, which form an area where personal data are processed. Drawing up such a list would require from the service provider the information about precise localization of servers on which the entrusted personal data are processed. Some large cloud providers which do not belong to the EOG enable the service clients only to choose the world's region where the data will be processed, which in Polish legislation is too general information and does not allow to perform the obligation resulting from [10, § 4 item 1].

Agreement with the cloud computing provider is constructed so that in case of a dispute the contractual provisions may be enforced effectively. Elements which should be

contained in a secure agreement on cloud computing are presented in table 3. The agreement about entrusting of personal data should be concluded in writing, but very often such agreements are concluded on-line. Therefore, a problem may arise of a failure to stick to the form of the concluded agreement as required for evidence and not under invalidity rigour. However, a failure to stick to the form of the agreement may be controlled by GIODO. A potential post-GIODO-control obligation to remedy such infringement may be difficult or even impossible to complete, if the on-line agreement with the cloud provider was concluded so that he adopted standard conditions, i.e. the agreement was concluded by access.

If the cloud provider is based in a country within EOG, regulations allow for a possibility to draw up an agreement concluded in a form which is equal with the agreement concluded in writing, which facilitates the conclusion of an on-line agreement that is legally valid.

Tab. 3. Elements of a correctly constructed agreement with the cloud service provider

No	Element of the agreement	Description of element
1.	Detailed information for the provider on the client's demands	The information should refer mostly to applied agreements with a guaranteed level of services and to sanctions involving a possibility to summon the provider if the requirements are not met.
2.	The security measures with which the cloud service provider must assure the compliance with the client's demands, depending on the risks connected with processing and type of the data under protection.	First of all, concrete organizational and technical measures have to be specified
3.	The object and time framework of the cloud computing service as well as the scope, method and purpose of personal data processing.	The aims of entrusting the personal data are specific storage activities, including storage as such. In this case, the processing entity is not an administrator of entrusted data but only a contractor of certain activities carried out on the data for a purpose specified by their administrator. For personal data transferred to the cloud computing provider the types of processed personal data should be specified. The scope means the personal data categories which are subject to entrusting, e.g. electronic mail addresses.
4.	Conditions of the return and destruction of data after the service is provided	Secure deleting of personal data has to be ensured at the public administration entity's request
5.	The confidence clause binding the cloud service provider and his employees having access to the data	Only authorized people may have access to entrusted data

6.	Entry about the provider's obligation to support the client in exercising the rights of the person to which the processed data refer	This entry should refer to the scope of a given person's access to her/his data, their amendment or deleting
7.	Entry about the provider's non-transfer of the data to any third parties, unless the agreement stipulates involvement of other entities to which the service provision will be entrusted	The agreement should specify that the processing entity's subcontractors may be engaged only with a consent from the data administrator, i.e. the public administration entity. The processing entity has to regulate the cross-border data transmission, e.g. by signing agreements with engaged subcontractors, by virtue of standard contractual clauses 2010/87/EU
8.	Entry explaining the cloud service provider's obligations	What is meant here are obligations related to the service client notification about any data protection infringements which affect the client's data
9.	Remembering about the service provider's obligation to draw up a list of locations where the data may be processed	
10.	Remembering about the administrator's right to monitor the course of the service completion by its provider	The cloud service provider is obliged to cooperate to this end with the data administrator
11.	Entry about the provider's obligation to inform about significant changes related to a specific cloud service	E.g. notifying about implementation of additional functionality
12.	Entry about registration and control of important operations of personal data processing	This entry refers to the cloud service provider or entities which were sub-entrusted with its accomplishment
13.	Entry about notifying the service client about each legally binding application for personal data availability	Notifying rests with the law enforcement organ, it this is not forbidden
14.	Entry about the provider's assurance that his internal decisions within data organization and processing will comply with applicable national and international standards and legal requirements	This entry refers also to internal decisions made by sub-processing entities, if there are any.

Also the ENISA study may be helpful in constructing a correct agreement with the cloud computing provider [15].

Making the personal data available to the cloud processing entity is, according to the Polish law, very difficult, because it should have a consent of those to whom the data refer. Therefore, the cloud service provider may find it difficult to use the personal data which are subject to entrusting for his own purpose, because of the difficulty with getting the declarations.

Under the present legal situation it seems most advantageous to conclude civil law agreements with cloud computing providers based in the countries belonging to the EOG. It may be even more troublesome to conclude agreements with entities based in the territory of the Republic of Poland. On the other hand, the choice of the cloud provider from outside the EOG, as the one that is associated with the need to negotiate the compliance with all conditions specified in the Polish law, is now most difficult.

1.5. Continued public sector informatization through cloud computing

Implementation of private sector projects management enhanced the public sector informatization. There is these days little information about the projects implemented using the public cloud computing, or dedicated or hybrid cloud computing, owing to which the public administration informatization would be continued dynamically.

Expenditures on new information technologies within the public administration informatization are growing continuously. Paradoxically, the maintenance of teleinformation infrastructure costs more and more, as it becomes obsolete very fast. With the rapid development of technology, continuous investments in the development of employees are unavoidable. This is particularly difficult for small territorial self-government entities (JST) which more and more lag behind big offices as regards advancement of provided services. It is particularly visible in the EC's annual rankings [16] and despite a progress reached in recent years the level of provided e-government services in Poland continues to be below the average among the countries subjected to the study. In the conclusions from the study [16] of 2012 the EC discerned considerable differences in offices informatization level and emphasized this as one of the main reasons for insufficient development of e-government in Poland.

The conclusions from the study carried out within [16] inclined the Information Projects Centre (IPC) at the Ministry of Administration and Digitization (MAC) to initiate the project *Informatization of JST using the cloud computing processing technology*. This project enables a considerable reduction of the JST expenditures owing to replacement of some investment expenditures for current costs, as confirmed by the results of the ventures implemented among other in Finland, Slovenia, or Great Britain. The conclusions from implementations in other countries confirm that the foundation of a mutual teleinformation infrastructure allows to obtain in the entire administration the added value impossible to work out in single JST's information systems.

Without knowing whether or not JST would be interested in such a project, the CPI carried out, tentatively, a questionnaire poll. The poll, addressed to the JST, was available on the CPI's website during the period from 27 September to 12 October 2012. Passing over incomplete or erroneously completed questionnaires, 654 questionnaires were collected from the communes (over 60% of the questionnaires were filled in by the offices operating in the communes having up to 10,000 inhabitants), 6 from county starosty offices, and 3 filled in by marshals' offices.

The main question in the questionnaire was „whether or not the JST would like to participate in the initiative and be a user of the project's products." Over 38% gave affirmative answers, almost 80% of affirmative answers coming from small JST. Approximately 40% of the communes were unable to answer the key question asked in the initial questionnaire, mentioning as the main reason for the „I don't know" answer the lack of the JST's detailed knowledge about the innovative nature of the venture. This points to

the need to start the project with a comprehensive and well prepared promotional and informative campaign.

The Minister of Administration and Digitization entrusted the CPI with implementation of this project, and by virtue of an agreement between the Implementing Authority for European Programmes and Minister of Administration and Digitization, of 5 April 2013, the project with estimated budget of 120 million PLN obtained 85% subsidizing from the European Regional Development Fund within the Innovative Economy Operational Programme. The project's initial schedule assumes that the project will be completed in mid 2015.

The aim of the project is to launch integrated e-government services provided by JST for their clients, based on a consolidated teleinformation infrastructure of the type of a private cloud computing. The project assumes that this infrastructure will enable the JST the development of new and integration of already operating teleinformation systems, using the possibilities offered by the electronic Platform of Public Administration Services (ePUAP). Furthermore, the project stipulates a cohesion of the policy of implementing the documents management systems and their standardization.

Infrastructure and services it provides are to be wholly completed by the CPI. The services made available by self-governments will be based on a consolidated, centrally managed teleinformation infrastructure of the type of a private cloud computing. Besides, training courses for the JST employees will be conducted within the project.

Those implementing the project want to construct the primary computing centre, auxiliary centre and the system management centre, virtualized infrastructure for providing services in IaaS model, central, regional and local platforms available in PaaS model and ensuring the connection with ePUAP as well as web applications, often simple, of the type of text editor or electronic mail, as well as advanced CRM solutions, workflow, accountancy, group work etc. (available in SaaS model).

A formal basis which arranges the cooperation of CPI (MAC) and JST would be the entries of the so called Cooperation Line, i.e. simply agreements between MAC and JST. Within the project, the Steering Committee was appointed and the following work groups were launched:

- organizational-legal group to work out the entries of agreements with the JST addressing the issues of cooperation in project implementation as well as the principles of the maintenance and further development of the system;
- for electronic services – to draw up a document tentatively entitled as the *Plan of Development and Integration of Services*, presenting the plan of reaching the target state within administration electronic services provided through the cloud computing infrastructure;
- infrastructural, aimed at drawing up a document tentatively entitled as the *Plan of the Construction of Mutual Infrastructure,* presenting a plan of constructing a private cloud computing for Polish public administration.

When appointing the project's Steering Committee it was assumed that it would consist of: Minister of Administration and Digitization as a sponsor of the *Programme of Integrated Informatization of the State,* the Ministry Cabinet Committee for Digitization which supervises the programme, and the Project's Users Council.

Infrastructure and services resulting from the project will be developed owing to the resources owned by the CPI at the Ministry of Administration and Digitization, resources at the disposal of the data processing centres formed both by the central and self-governmental administration entities, and resources acquired through public procurement.

The first of the public procurement procedures will be the *Technical dialogue related to electronic services and teleinformation infrastruture of the private cloud computing in public administration.*

2. Conclusions

The mandatory legal regulations do not exclude the use of the public cloud computing in public administration.

Yet, the public sector in Poland does not maximise the benefits resulting from the use of cloud computing, which may result from non-cohesive documentary processes in which the technology does not support sufficiently the information flow and the clerks, because of obsolete practices, do not work as effectively as they could. Optimization of using this approach is necessary especially to maintain the balance between the office clerks' and clients' access to information and the confidential data protection.

According to study [2] only 47% of offices use cloud computing to share documents, 71% use them to enable a remote access to documents, and as many as 69% of investments in new technologies are carried out before the functionality of existing information systems is fully known. Only 44% of public entities may prove that their documentary processes are safe. Regular surveys of documentary processes may help identify the risks and enable a better sharing of public information in a safe way.

By using this modern and innovative approach, the public administration entities may significantly raise the level of provided services and ensure an appropriate level of data security and protection.

Cloud computing (if the agreement is constructed properly) according to the provisions of the *Act on public finances* [17] imposing the obligation of apt and economical spending of public funds, seems to be a good solution enabling reduction of costs with simultaneous performance of public tasks at an appropriate level.

The need to reduce the public administration costs will perhaps incline the Minister of Economy to take a favourable stand on implementing, in public sector, of information solutions based on storage and processing of data in the cloud provided by partners from the IT branch.

Literature

1. Raport Cloud Computing elastyczność, efektywność, bezpieczeństwo. Microsoft Polska, THINKTANK, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011.
2. Coleman Parkes Research: Badanie Ricoh Document Governance Index 2012. Ricoh Europe 2012.
3. Kluska M.: Hosting i backup danych urzędu w chmurze. IT w Administracji, nr 5, 2013, 32-34.
4. The What, Why, and When of Cloud Computing. Gartner Inc.
5. Pawłowicz W.: IaaS – zalety i wady wieku dojrzewania. Networld, 184, nr 11, 2011, 50-55.
6. Byrski J.: Cloud computing z perspektywy administracji publicznej. IT w Administracji, nr 1, 2013, 24-27.
7. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r.. Dz. U. 2005, nr 64, poz. 565 z późn. zm., http://www.polskieustawy.com/print.php?actid=3098&lang=&adate=20100729

8. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz. U. 2012, poz. 526, http://dziennikustaw.gov.pl/du/2012/526
9. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. 2002, nr 101, poz. 926 z późn. zm, http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883
10. Minister Spraw Wewnętrznych i Administracji: Rozporządzenie z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Dz. U. nr 100, poz. 1024.
11. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz. U. 2010, nr 182, poz. 1228, http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228
12. Marszałek Sejmu: Prawo zamówień publicznych. Dz. U. 2010, nr 113, poz. 759, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20101130759
13. Grupa Robocza Art. 29 ds. Ochrony Danych: Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej. 2012.
14. The European Commission: Cloud Computing Strategy. Brussels 2012, http://www.lewica24.pl/unia-europejska/1675-ke-oglasza-strategie-wobec-chmury-obliczeniowej.pdf
15. Procedure secure: ENISA's new guide for monitoring cloud computing contracts. ENISA 2012.
16. The European Commission: Digital Agenda Scoreboard, http://ec.europa.eu/digital-agenda/
17. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych. Dz. U. 2009, nr 157, poz. 1240 z późn. zm., http://isap.sejm.gov.pl/DetailsServlet?id=WDU20091571240
18. Kamiński M.: Przetwarzanie w chmurze a ochrona danych osobowych. IT w Administracji, nr 6, 2013, 38-41.

Dr Anna KACZOROWSKA
Katedra Informatyki na Wydziale Zarządzania
Uniwersytet Łódzki
90-237 Łódź, ul. Matejki 22/26
tel./fax.: (0-42) 635 50 45/635 50 17
e-mail: annak@wzmail.uni.lodz.pl