Czas informacji
Prawo nowych technologii • Informacja w administracji i gospodarce
ISSN 2081-6189 kwartalnik 2(14)/2013

Chmura zaufania

Michał Tabor

Zastosowanie dokumentów elektronicznych w postępowaniu administracyjnym
Mariusz Przybyszewski

Dotacje unijne na informatyzację administracji publicznej
Ewa Modzelewska

Informatyzacja mniej lub bardziej zintegrowana
Tomasz Kulisiewicz

Prawne aspekty Cloud Computing
Anna-Maria Dzięgiel

Koniec utopii
Edwin Bendyk

cpi
centrum promocji informatyki
www.cpi.com.pl

NAUKA

4 **Analiza interesariuszy w projekcie**
Dariusz Bogucki

15 **Zastosowanie dokumentów elektronicznych w postępowaniu administracyjnym**
Katarzyna Czajkowska-Matosiuk

36 **Elektroniczne usługi administracji**
Dorota Fleszer

46 **Dotacje unijne na informatyzację administracji publicznej**
Ewa Modzelewska

PUBLICYSTYKA I PRAKTYKA

55 **Chmura zaufania**
Michał Tabor

65 **(Nie tylko) dziura w jezdni, czyli o „inteligencji" rzeczy martwych**
Mieczysław T. Starkowski

70 **Informatyzacja mniej lub bardziej zintegrowana**
Tomasz Kulisiewicz

75 **Trzy oblicza e-administracji w Polsce**
Danuta Descours

PRAWO

79 **Prawne aspekty Cloud Computing**
Anna-Maria Dziegiel

87 **Składanie oświadczeń woli w formie elektronicznej**
Jacek Murzydło

STAŁE RUBRYKI

94 **Zarządzanie projektami: Rejestr ryzyka czy „lista strachu" kierownika projektu?**
Roman Bratek

101 **Metodyki zwinne a umowy wdrożeniowe – kilka uwag**
Bohdan Widła

106 **Ochrona danych osobowych: Czy definicja „administratora danych" wymaga zmian?**
Damian Karwala

FELIETON

112 **Koniec utopii**
Edwin Bendyk

KOMUNIKATY–co wokół słychać

114 **Relacja z konferencji Predictive Solutions, KORELACJE 2013**

115 **Relacja z Seminarinarium "Blaski i cienie przetwarzania w chmurze (Cloud Computing)"**

W kolejnym numerze:

- Udostępnianie informacji gospodarczej podmiotom publicznym Prawo własności wirtualnej
  - Anna Maria Dzięgiel
- Wiążące reguły korporacyjne dla przetwarzających dane osobowe (Processor Binding Corporate Rules)
  - Damian Karwala
- Elektroniczna księga wieczysta?
  - Katarzyna Czajkowska-Matosiuk
- Polityka bezpieczeństwa e-administracji
  - Ewa Modzelewska
- Analiza otoczenia przedsięwzięcia informatycznego
  - Dariusz Bogucki
- Jeszcze telefonia komórkowa, czy już bank
  - Agnieszka Zdanowska
- Informacja publiczna w świetle orzecznictwa sądów administracyjnych
  - Jacek Murzydło

Wiesław Paluszyński redaktor naczelny
wieslaw.paluszynski@czasinformacji.pl

Wiosną nasi czytelnicy mogli uczestniczyć w kilku seminariach Polskiej Izby Informatyki i Telekomunikacji pomagających uporządkować swą wiedzę w zakresie jakości oprogramowania i zarządzania ryzykiem. Ostatnie zaś dotyczyło usług świadczonych w modelu chmury obliczeniowej.

Niektóre z tych tematów zagościły też w tym zeszycie, gorąco polecamy. Zainteresowanych seminariami odsyłamy zaś na stronę internetową PIIT, gdzie znajdą prezentacje ze wspomnianych seminariów.

Lato zaczyna być słoneczne, a tu wszędzie dookoła chmury. Chmury ze strony Unii Europejskiej, chmury nasze własne, chmura dla samorządów zaserwowana przez Centrum Projektów Informatycznych. Jednym słowem jedna wielka chmura. A nasze przysłowie mówi „z wielkiej chmury mały deszcz". Aby w tym przypadku się nie sprawdziło!

Jednak temat jest ważny, więc przykładamy się do niego i piszemy o aspektach bezpieczeństwa w chmurze – Michał Tabor, a także o aspektach prawnych tej usługi -Anna-Maria Dzięgiel. Zwracam na to uwagę, usługi, a nie sprzętu i oprogramowania.

Ponieważ za chwile uszczęśliwi nas wszystkich realizacja wizji zintegrowanej informatyzacji w koncepcji Ministerstwa Administracji i Cyfryzacji „program Zintegrowanej Informatyzacji Państwa", poprosiliśmy Tomka Kulisiewicza, aby zbadał ten temat, zanim stosowne akty nabiorą mocy urzędowej. Zbadał i zdaje raport pod nazwą „Informatyzacja mniej lub bardziej zintegrowana". Polecam wszystkim, co planują brać udział w kolejnych etapach integrowania e-usług za unijne pieniądze. A na co poszły te pieniądze w administracji publicznej rozbiera na czynniki pierwsze Ewa Modzelewska. O kolejnych uwarunkowaniach e-administracji, a także o prawnych aspektach jej usług pisze dr Dorota Fleszer. Danuta Descours opowiada zaś o kilku uporządkowanych obliczach e-administracji.

Samorząd to też miasta, obszary niejednokrotnie wielkie i nie posądzane o objawy własnej inteligencji, a jednak!!!; takie objawy własnej inteligencji tych tworów nieożywionych znalazł Mieczysław Starkowski i dzieli się z nami swoimi obserwacjami.

Wreszcie praktyka, czyli realizacja idei i pomysłów na informatyzację; więc jak zawsze dr Dariusz Bogucki i unijne spojrzenie na interesariuszy w projekcie, Roman Bratek o rejestrze ryzyka, a także Bogdan Widła o metodykach zwinnych w kontekście umów wdrożeniowych.

Jak na okres wakacyjny wystarczy. A po wakacjach szykują nam się znaczne zmiany w prawie unijnym i krajowym, w obszarach zamówień publicznych, danych osobowych, identyfikacji i uwierzytelniania. Pojawiły się i poszły do konsultacji społecznych w regionach nowe programy w nowej perspektywie finansowej UE, jak „Polska Cyfrowa". Postaramy się nadążyć, a na razie życzę przyjemności z lektury i odpoczynku w ciszy przyrody, a także refleksji do czego zachęca nas Edwin Bendyk pisząc o „końcu Utopii".

Analiza interesariuszy w projekcie

dr inż. Dariusz Bogucki

Kiedy Redakcja *„Czasu Informacji”* poprosiła mnie o napisanie artykułu poświęconego angażowaniu interesariuszy w projekcie, przypomniałem sobie opinię, którą przeczytałem na portalu eGospodarka.pl: Stawiała ona tezę, że jednym z największych wyzwań zarządzania w XXI w jest docenienie roli interesariuszy (stakeholders) i ich wpływu na funkcjonowanie przedsięwzięć gospodarczych. Przemyślany plan działania, wiedza menedżerów i odpowiednie fundusze już nie wystarczą do sprawnej realizacji projektów czy wdrażania programów. Myślę, że nie tylko dlatego warto pochylić się nad tym tematem.

Po co to robimy?

Zacznijmy od tego, że termin **interesariusz** jest polskim tłumaczeniem anglojezycznego terminu „*stakeholders”* pochodzącego od określenia „*to have a stake in” („mieć interes w czymś*”) i jest mutacją terminu „*shareholder*” (akcjonariusz). Termin ten pojawił się oryginalnie w opracowaniu Stanford Research Institute z 1963 roku i oznaczał podmioty (osoby, społeczności, instytucje, organizacje, urzędy), które mogą wpływać na organizację lub pozostają pod wpływem jej działalności, względnie uważają, że organizacja taki wpływ na nich wywiera.

Analiza interesariuszy jest jednak dziedziną stosunkowo młodą: w 1984 roku prof. R. Edward Freeman opracował tzw. teorię interesariuszy, wg. której każde przedsięwzięcie realizowane przez organizację działa w danym środowisku społecznym z innymi jego uczestnikami. Freeman podkreślał, że organizacja powinna uwzględniać interesy wszystkich zainteresowanych stron działalności firmy, biorąc pod uwagę aspekt społeczny.

Pojęcie to od lat 90 zadomowiło się w metodykach projektowych jak PRINCE2® a zwłaszcza w metodykach związanych z zarządzaniem programami jak MSP®. Interesariusze są, bowiem nie przypadkiem postrzegani jako kluczowy czynnik sukcesu projektu / programu. Oznacza to, że:

- Na etapie inicjowania projektu / programu należy dokładnie rozpoznać oraz przeanalizować potrzeby i oczekiwania wszystkich grup interesariuszy, aby zwiększyć szanse na sukces projektu /programu;
- Każdy projekt / program wymaga odrębnej identyfikacji grup interesariuszy a następnie rozpoznania ich celów i stopnia zainteresowania realizacją przedsięwzięcia;
- Każdy projekt / program wymaga przeprowadzenia analizy grup poszczególnych interesariuszy (wewnętrznych oraz zewnętrznych) - ich roli, wpływu, siły oddziaływania oraz zainteresowań i celów a zwłaszcza wzajemnych powiązań;

Obecnie widać odchodzenie od statycznej analizy interesariuszy czy prostych metod zarządzania interesariuszami w stronę aktywnego procesu strategicznego budowania angażowania interesariuszy w przedsięwzięcie (patrz poniższy rysunek). Ten proces wiąże się bezpośrednio z obszarem zagadnień związanych z tzw. społeczną odpowiedzialnością biznesu (CSR – *Corporate Social Responsibility*). Jest to dynamicznie rozwijająca się koncepcja, według której

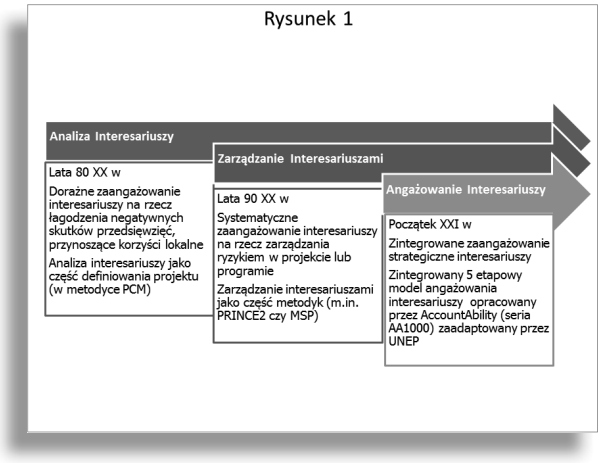
przedsiębiorstwa na etapie budowania strategii dobrowolnie uwzględniają interesy społeczne i ochronę środowiska, a także relacje z różnymi grupami interesariuszy. Według tego podejścia, bycie odpowiedzialnym nie oznacza tylko spełniania przez organizacje (a zwłaszcza przedsiębiorstwa) wszystkich wymogów formalnych i prawnych, ale oprócz również zwiększone inwestycje w zasoby ludzkie, w ochronę środowiska i relacje z interesariuszami, którzy mogą mieć faktyczny wpływ na efektywność działalności gospodarczej tych organizacji oraz ich innowacyjność. Zatem wydatki tego rodzaju należy traktować, jako inwestycję i źródło wiedzy, a nie, jako koszt, podobnie jak w przypadku zarządzania jakością czy ryzykiem.

Obecnie za najlepszy zbiór reguł z tego obszaru uważa się uznany standard **AA1000,** wypracowany w 1999 roku przez Instytut na rzecz Społecznej i Etycznej Odpowiedzialności (Institute of Social and Ethical AccountAbility). Został w 2005 zaadaptowany przez UNEP (Program Środowiskowy ONZ) co opisuje szczegółowo *„Podręcznik Angażowania Interesariuszy"* tom 1 i 2: Stakeholder Research Associates Canada Inc., UNEP, AccountAbility, 2005, wydanie polskie pod red. Bartosza Grucza, Bizarre, Warszawa 2012. Zajmiemy się jego charakterystyką w dalszej części artykułu.

Według wspomnianego standardu AA1000 zaangażowanie interesariuszy:

- Prowadzi do sprawiedliwszego i bardziej zrównoważonego rozwoju społecznego dzięki oddaniu głosu tym grupom, które powinny być uwzględnione w procesie podejmowania decyzji;
- Usprawnia zarządzanie reputacją organizacji i ryzykiem w przedsięwzięciu;
- Pozwala na uwspólnianie zasobów (wiedzy, ludzi, pieniędzy i technologii), dzięki czemu możliwe jest rozwiązanie problemów i osiągnięcie celów, które trudno byłoby osiągnąć pojedynczym organizacjom;
- Ułatwia zrozumienie złożonego kontekstu działania;
- Umożliwia uczenie się od interesariuszy, co przekłada się na ulepszenia procesów i produktów;

Rysunek 1



Rysunek 1: *Ewolucja procesu angażowania interesariuszy*
Źródło: opracowanie własne autora

- Informuje, edukuje i wpływa na interesariuszy, dzięki czemu mogą oni podejmować lepsze decyzje i działania mające wpływ na organizację i przedsięwzięcie,
- Ma pozytywny wkład w rozwój opartych na zaufaniu i przejrzystości relacji z interesariuszami.

Kim są interesariusze?

Niestety, nie ma uniwersalnej listy interesariuszy, którą da się zastosować, jako „pierwszy gotowiec" dla wszystkich projektów / programów. To, jacy (a może w jakich rolach) interesariusze wpływają lub odczuwają wpływ organizacji zależy od branży, specyfiki firmy, lokalizacji przedsięwzięcia a może przede wszystkim jego zakresu i charakteru.

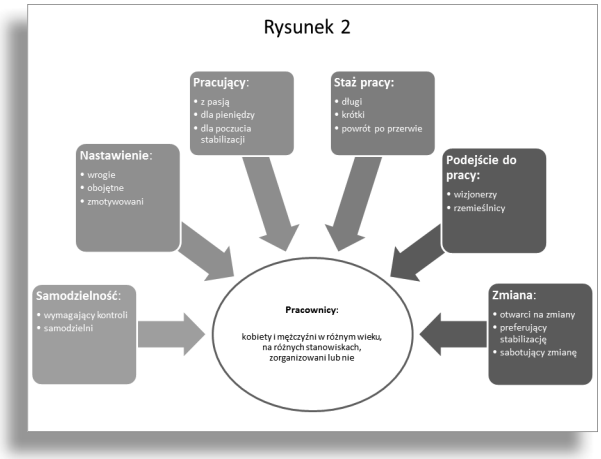
Najczęściej stosowane sposoby identyfikacji interesariuszy na podstawie charakterystyki podmiotów funkcjonujących w otoczeniu przedsięwzięcia, pod kątem ich:

- **Zobowiązań**: podmioty, wobec których mamy lub w przyszłości możemy mieć zobowiązania prawne, finansowe czy operacyjne, przewidziane w przepisach, kontraktach, strategiach czy kodeksach praktyki.
- **Wpływu**: podmioty, które obecnie lub w przyszłości mogą wpływać – czy to pozytywnie, czy negatywnie – na zdolność organizacji do osiągnięcia swoich celów. Mogą to być osoby wywierające wpływ nieformalny jak i osoby posiadające formalne uprawnienia w zakresie podejmowania decyzji.
- **Bliskości**: podmioty, z którymi organizacja ma do czynienia najwięcej:
  - Osoby z wewnętrza organizacji,
  - Podmioty, z którymi łączą organizację wieloletnie stosunki,
  - Podmioty, na których organizacja polega w zakresie swoich działań codziennych,
  - Mieszkańcy terenów objętych zakresem przedsięwzięcia itp.
- **Zależności:** osoby, które są w największym stopniu uzależnione od organizacji, np. pracownicy i ich rodziny, klienci, których bezpieczeństwo, źródło utrzymania, zdrowie czy dobrobyt zależy od produktów organizacji, czy też dostawcy, dla których jest ona głównym odbiorcą.
- **Przedstawicielstwa**: osoby, które na mocy uregulowań prawnych czy kultury/ tradycji reprezentują inne osoby; np. liderzy społeczności lokalnych, reprezentanci NGO, przedstawiciele związków zawodowych, doradcy, reprezentanci organizacji członkowskich itd.
- Wspomniany w poprzednim rozdziale prof. Freeman podzielił interesariuszy na dwie podstawowe grupy w związku z rożnym stopniu oddziaływania na przedsięwzięcie.
- **Interesariusze wewnętrzni:** osoby, instytucje, organizacje, których działania bezpośrednio wiążą się z danym projektem w szczególności:
  - Zespół projektowy / pracownicy zaangażowani w projekt;
  - Dostawcy;
  - Użytkownicy / Klienci;
  - Sponsorzy / Kierownictwo organizacji;
- **Interesariusze zewnętrzni:** podmioty pośrednio zależne / związane / zainteresowane wynikami projektu / działające w jego otoczeniu, jak:
  - Inni pracownicy organizacji;
  - Społeczność lokalna;
  - Partnerzy społeczni (stowarzyszenia i organizacje pozarządowe - NGO);
  - Instytucje wspierające przedsiębiorczość;
  - Związki zawodowe.

Kilka wymienionych powyżej grup warto scharakteryzować nieco szerzej.

Pracownicy

Jest „oczywistą oczywistością", że jest to w każdym przedsięwzięciu kluczowa grupa, bezpośrednio przyczyniająca się do jego sukcesu.



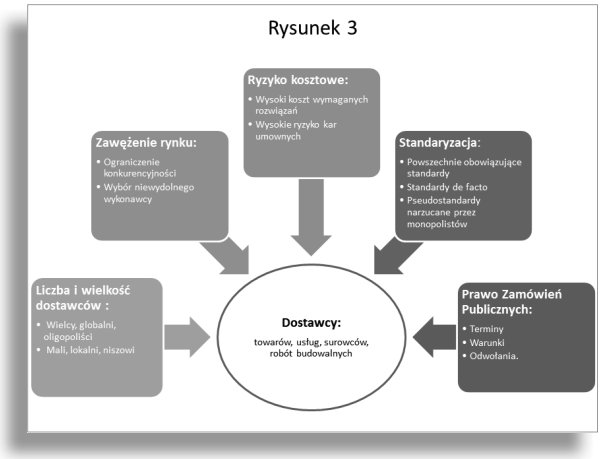
Rysunek 2: *Różne aspekty ryzyka związanego z angażowaniem pracowników*
Źródło: opracowanie własne autora

Skuteczne zaangażowanie pracowników w projekt niesie oczywistą wartość dodaną dla organizacji wyrażającą się m.in. większą lojalnością kadr, wkładem w rozwój organizacji, poczucie współodpowiedzialności za to, co się w niej dzieje czy dobrym wizerunkiem organizacji. Niesie też oczywiste korzyści dla pracownika: możliwości rozwoju, poczucie bycia częścią organizacji, poczuciem bezpieczeństwa i komfortu pracy, co skutkuje większą odwagą do wychodzenia z inicjatywą, pomysłami, kreatywnością.

Jest jednak grupa niezmiernie zróżnicowana, wobec której nie da się po prostu zastosować jednego schematu działania (patrz poniższy rysunek), co wiąże się z określonym ryzykiem projektowym:

Dostawcy

Dostawcy nie są jedynie wykonawcami naszych zleceń. To partnerzy, od których możemy zyskać cenną wiedzę, ale też oni mogą się



Rysunek 3: *Różne aspekty ryzyka związanego z angażowaniem dostawców*
Źródło: opracowanie własne autora

od nas wiele uczyć. Dzięki ścisłej i partnerskiej współpracy z dostawcami, możemy zyskać ich lojalność, a przez to obniżyć ryzyko związane z ciągłością zamówień.

Nie zapominajmy, że z ich punktu widzenia jesteśmy ważnym, ale jednym w z wielu elementów łańcucha dostaw. Współdziałanie na rzecz coraz lepszych standardów w łańcuchu dostaw, może prowadzić do innowacji i powstania wartości dodanej „po obydwu stronach lady". Pamiętajmy jednak, że dostawcy są BARDZO różni (patrz poniższy rysunek).

Organizacje pozarządowe

Ta heterogeniczna grupa określana jest bardzo wieloma terminami:

- Przede wszystkim mianem ***organizacji społeczeństwa obywatelskiego*** (ang. CSO, Civil Society Organisations).
- Używa się też terminu ***NGO***, który jest akronimem angielskiej nazwy: *non-governmental organisation*.
- Organizacje takie bywają też nazywane ***trzecim sektorem***, obok sektora ***publicznego*** (władz, administracji publicznej) i ***rynkowego*** (biznesu).

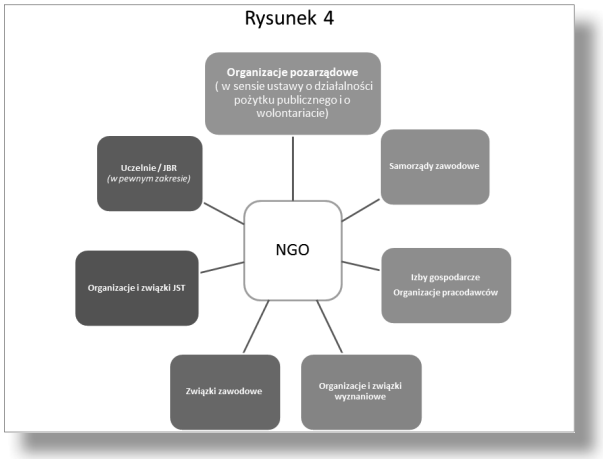
Specyfiką NGO jest działanie społecznie i nie dla zysku (not for profit). Nie oznacza to, że organizacje te nie mogą generować dochodów, ale zyski mogą zostać wykorzystane wyłącznie na cele zgodne z misją organizacji.

Warto pamiętać o olbrzymim zróżnicowaniu wewnątrz trzeciego sektora: Wśród organizacji pozarządowych możemy spotkać się z niewielkimi stowarzyszeniami czy fundacjami, jak i organizacjami globalnymi (patrz poniższy rysunek). Na szczególną uwagę zasługują tzw. **stowarzyszenia / fundacje korporacyjne**, które, pomimo iż formalnie zaliczane do organizacji pozarządowych są ściśle związane z biznesem

Dobre zaangażowanie organizacji trzeciego sektora daje BARDZO wiele:

- Dostęp do profesjonalnej wiedzy dotyczącej problemów społecznych, a także sposobów ich rozwiązywania;
- Pozyskanie partnera, który posiada wiedzę z zakresu budowania i zarządzania projektami społecznymi;
- Wykorzystanie doświadczenia organizacji pozarządowej w zakresie współpracy z wolontariuszami

Rysunek 4



Rysunek 4: *Podstawowe rodzaje organizacji trzeciego sektora spotykane w projektach*
Źródło: opracowanie własne autora

Trzeba jednak pamiętać, że może to być trudna współpraca:

- Oferty NGO nie są zazwyczaj sprofilowane pod kątem naszego przedsięwzięcia a często są wyrywkowe („w sumie interesuje nas Wasz projekt, ale nasza fundacja zajmuje się tylko X"), co podważa wiarygodność do wiedzy NGO i zniechęca do współpracy;
- Organizacje (zwłaszcza małe) nie komunikują się między sobą a wręcz rywalizują, co utrudnia współpracę firmy z kilkoma organizacjami naraz;
- Oczekiwania organizacji w stosunku do firm i administracji (zwłaszcza małych i silnie sprofilowanych w działaniu) ograniczają się często tylko do pieniędzy (postawa roszczeniowa);
- Zdarzają się NGO, które nie chcą poszerzać i rozwijać swoich kompetencji („i tak wiemy najlepiej");
- Projekty NGO są dość często uruchamiane bez rzetelnej analizy potencjalnych korzyści („inicjatywy serca"), ale też zdarzają się zbytnio nastawione na korzyści (zatracenie „idei", „ducha").

Co to jest standard AA1000?

AA1000 to tzw. uznany standard z obszaru społecznej odpowiedzialności biznesu, wypracowany w 1999 roku przez Instytut na rzecz Społecznej i Etycznej Odpowiedzialności (Institute of Social and Ethical AccountAbility). Jest on uważany za najbardziej rozwinięty i dopracowany standard współpracy z interesariuszami, włączający kwestie społeczne i etyczne do zarządzania strategicznego organizacji i jej działalności. To było powodem do tego, że w 2005 został zaadaptowany przez UNEP (Program Środowiskowy ONZ). Co ważne AA1000 budowany od samego początku był jako standard uniwersalny i może być stosowany:

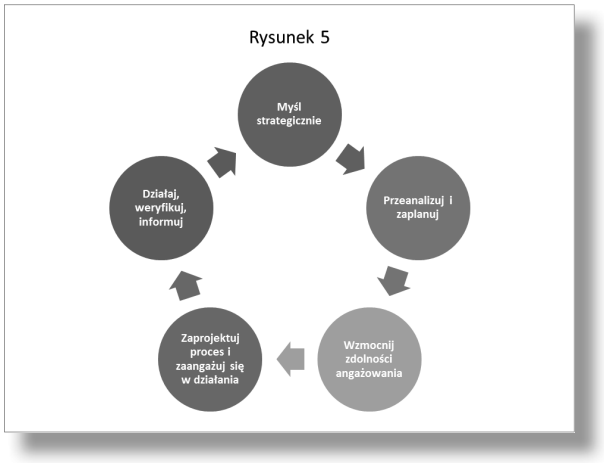
- Do analizy strategicznej wszelkich organizacji;
- Do zewnętrznej oceny przedsiębiorstwa w zakresie społecznej i etycznej odpowiedzialności biznesu;
- Do wypracowania zasad angażowania interesariuszy przez organizację na poziomie strategicznym, programów, projektów i operacyjnym;
- W procesie samodoskonalenia się organizacji

Istotą standardu AA1000 jest 5 etapowy cykl angażowania interesariuszy (patrz poniższy rysunek) opisany w poniższej tabeli:

Etap	Opis	Zadania
1 Myśl strategicznie	Identyfikacja strategicznych priorytetów organizacji dotyczących zaangażowania interesariuszy w dane przedsięwzięcie	• Sprawdź, kim są ci interesariusze • Zidentyfikuj i rozważ strategiczne zagrożenia, możliwości i cele związane z zaangażowaniem tych interesariuszy • Zidentyfikuj cele strategiczne i podstawowe zagadnienia oraz stopień ich ważności dla różnych grup interesariuszy. • Uszereguj priorytety
2 Przeanalizuj, zaplanuj	Stworzenie bazy wiedzy na temat organizacji i jej interesariuszy w celu uszeregowania priorytetów i opracowania planu zaangażowania	• Zbierz wiedze na temat przedstawicieli interesariuszy • Zbadaj możliwy zakres zaangażowania w kontekście analizy istniejących relacji, dostępnych zasobów i ograniczeń organizacyjnych. • Podejmij decyzje, co do rodzaju relacji, jaką chcesz nawiązać z nimi (stopnie zaangażowania)

Etap	Opis	Zadania
3 Wzmocnij zdolność angażowania	Poprawa umiejętności i wdrożenie rozwiązań umożliwiających organizacji skuteczne zaangażowanie w działania z interesariuszami	• Sprawdź na ile Twoja organizacja jest zdolna do zrozumienia zagadnień generowanych przez interesariuszy, efektywnego angażowania się i działania w ramach procesu zaangażowania • Znajdź mocne strony organizacji i zidentyfikuj luki • Zaplanuj działania wzmacniające strony silne i niwelujące luki
4 Zaprojektuj proces i zaangażuj się w działania	Zaplanowanie i przygotowanie działań związanych z zaangażowaniem interesariuszy	Bazując na wcześniejszych krokach, przygotuj konkretne rozwiązania dopasowane do uwarunkowań organizacji / projektu w formie tzw. planu zaangażowania
5 Działaj, weryfikuj, informuj	Przełożenie nowo nabytej wiedzy, perspektyw i porozumień na działania	• Realizuj zaplanowane działania • Przeanalizuj dotychczasowe wyniki procesu angażowania • Sprawdź, czy i co się zmieniło w trakcie procesu, • Wprowadź ew. korekty do przyjętego planu (nawrót do etapu 1)

Tabela1



Rysunek 5: *Pięcioetapowy cykl angażowania interesariuszy w standardzie AA1000*
Źródło: opracowanie własne autora, zgodne z podręcznikiem „The Stakeholder Engagement Manual".

Standard AA1000 opisują trzy uzupełniające się podręczniki[1]:

1) AA1000 Zasady Odpowiedzialności (AccountAbility Principles Standard - **AA1000APS**), który opisuje tzw. zasady przewodnie, które odnoszą się do całej serii:
   - **Włączania:** organizacja zna swoich interesariuszy, rozumie ich potrzeby oraz oczekiwania i odpowiednio angażuje ich. Realizacja tej zasady oznacza, że organizacja zobowiązuje się na każdym kroku badać i odzwierciedlać poglądy i potrzeby wszystkich grup interesariuszy. Nie oznacza to oczywiście zdania się na ich pomysły a analizowani i ew. korygowanie działań związanych z danym przedsięwzięciem. Opinie interesariuszy pozyskiwane są w procesie zaangażowania, który umożliwia im wypowiadanie ich bez obaw i ograniczeń. Co ważne zasada ta wymaga uwzględnienia również niemogących się wypowiedzieć interesariuszy, w tym przyszłych pokoleń czy środowiska.
     Zasada włączania przekłada się na następujące zasady realizacyjne:
   - **Istotności:** organizacja posiada wiedzę nie tylko na temat własnych interesów i priorytetów, ale i interesów i priorytetów interesariuszy;
   - **Kompletności:** organizacja w sposób świadomy zarządza swoim oddziaływaniem oraz wynikającymi z tego poglądami, potrzebami, sposobem postrzegania i oczekiwaniami interesariuszy;
   - **Zdolność do reagowania (odpowiadania):** organizacja spójnie i adekwatnie do sytuacji reaguje na kwestie zasadnicze dla interesariuszy i organizacji.
2) AA1000 Weryfikacja (AccountAbility Assurance Standard - **AA1000AS**), który opisuje sposoby weryfikacji zasad opisanych w AA1000APS i AA1000SES. Proces ten obejmuje to zarówno weryfikację działań przez zewnętrzny podmiot i jak i kontrolę wewnętrzną.
3) AA1000 Zaangażowanie Interesariuszy (AccountAbility Stakeholder Engagement Standard - **AA1000SES**), stanowiący główny element standardu.
   Standard AA1000SES jest typowym standardem narzędziowym „how to", pokazującym, w jaki sposób można przeprowadzić proces angażowania interesariuszy, w tym w formie dialogu. Podręcznik podaje liczne praktyczne wskazówki i jest przydatny dla każdego menedżera, który zajmuje się budowaniem relacji, nie tylko dla menedżera CSR.
   Standard może być wykorzystywany samodzielnie albo jako mechanizm do osiągnięcia wymagań związanych z angażowaniem interesariuszy określonych w innych standardach jak norma ISO 26000. Mechanizmy zaangażowania interesariuszy zawarte w standardzie AA1000SES obejmują zarówno płaszczyznę strategiczną jak i operacyjną.
   Standard określa jako warunek konieczny to że zaangażowanie interesariuszy zawsze musi zawsze służyć jakiemuś dobrze zdefiniowanemu celowi biznesowemu organizacji – cel może dotyczyć rozwoju lub poprawy określonego procesu lub określonej strategii. Standard AA1000SES precyzyjnie określa jak powinien wyglądać proces zaangażowania interesariuszy w rozwój lub poprawę wybranej strategii lub celu operacyjnego.
   Standard określa, że punktem wyjścia do uruchomienia procesu jest odpowiedzenie sobie na pytania wynikające z uznania zasady włączenia, jako podstawy działania w angażowanie interesariuszy w danym przedsięwzięciu:

1 Na potrzeby adaptacji standardu przez UNEP, standard został przeredagowany do postaci dwutomowego podręcznika: *„The Stakeholder Engagement Manual"*.

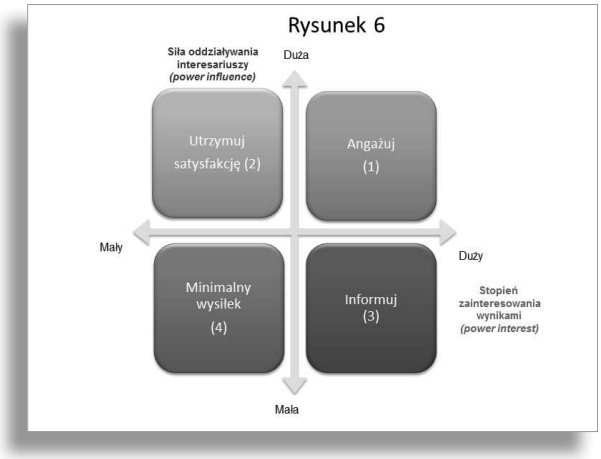
Pytanie	Co to oznacza w praktyce?
Czy nasze działania są szczere?	Czy rozmawiamy z interesariuszami tylko po to, by poprawić wizerunek organizacji? Czy też chcemy naprawdę uzyskać kompletny, uczciwy obraz faktycznego oddziaływania naszej organizacji?
Czy nasze działania są uczciwe i oparte na wiarygodnych informacjach?	Czy proces zaangażowania umożliwia uwzględnienie wszystkich interesariuszy, czy też ci szczególnie odczuwający wpływ naszej organizacji są ignorowani? Czy zastosowano procesy wewnętrzne i zewnętrzne, umożliwiające organizacji zdobycie faktycznej wiedzy na temat wpływu naszej organizacji oraz opinii interesariuszy?
Jakie to przyniesie efekty?	Co organizacja planuje zrobić w związku z wynikłymi w procesie dialogu z interesariuszami kwestiami? Jak to wpłynie na aspekty działania naszej organizacji i jakie to przyniesie korzyści? Czy istnieje wola wprowadzenia zmian koniecznych do wbudowania nowych zagadnień do procesów zarządzania i strategii?

Tabela 2

Jakie narzędzia mogą nam pomóc w procesie?

Wszystkie działania w stosunku do interesariuszy można pogrupować w trzy komplementarne kategorie:

1) **Informacyjne:**
   a) Specjalna strona internetowa
   b) Cotygodniowy lub comiesięczny newsletter
   c) Regularne informacje o postępach w projekcie (e-mail)
   d) Plakaty i ulotki
   e) Artykuły w (powszechnej / lokalnej / firmowej / branżowej) gazecie lub magazynie
   f) Wywiady prasowe, telewizyjne i radiowe
   g) Szkolenia i warsztaty na konkretne tematy
2) **Konsultacyjne:**
   a) Prosić interesariuszy o opinię w ankietach i kwestionariuszach
   b) Zaprosić interesariuszy na spotkanie startowe na początku procesu, zapytać o ewentualne pomysły, opinie, ryzyko, możliwości …
   c) Zaprosić przedstawiciela interesariuszy do rady doradczej w sprawie projektu
   d) Organizować regularne spotkania, żeby informować o postępach projektu, prosić o opinie i sugestie
3) **Angażujące:**
   a) Zaprosić przedstawiciela interesariuszy do zespołu wdrażającego projekt / komitetu sterującego
   b) Zaprosić przedstawiciela interesariuszy na spotkanie startowe, żeby wspólnie zadecydować o celach i działaniach do podjęcia w czasie przeprowadzania procesu
   c) Regularnie organizować spotkania, ażeby wspólnie podejmować decyzje odnośnie wdrażania kolejnych etapów projektu



Rysunek 6: *Macierz interesariuszy*
Źródło: opracowanie własne autora.

d) Zaangażować w konkretne kwestie dotyczące wdrażania projektu

Głównym narzędziem do określania jakie działania należy podejmować w stosunku do poszczególnych interesariuszy jest tzw. macierz interesariuszy klasyfikująca ich w dwóch wymiarach: pod kątem możliwości oddziaływania interesariuszy na przedsięwzięcie (tzw. power influence) i stponia zainteresowania jego wynikami (tzw. power interest). Można to zobrazować jak niżej:

Zgodnie z tym schematem wszystkich interesariuszy dzielimy na 4 grupy wedle, których planujemy strategię angażowania:

1. Interesariusze z **Grupy (1)** to kluczowi gracze w projekcie. Tych interesariuszy należy silnie zaangażować w projekcie i należy czynić wysiłki w celu ich pełnego usatysfakcjonowania. Ich głos musi być zawsze wysłuchany
2. **Grupa (2)** to grupa o dużej potencjalnej władzy, ale w ograniczonym zakresie wyrażający zainteresowanie jego wynikami. Należy uzyskać zadowolenie tych interesariuszy, lecz nie narzucać się zbędnymi informacjami;
3. Wobec interesariuszy **Grupy (3)** stosujemy odmienną taktykę: należy prowadzić z nimi aktywny dialog, aby mieć pewność, że nie powstają problemy;
4. **Grupa (4)** wymaga działań informacyjnych, ale i monitorujących. Sytuacja w przedsięwzięciu jest, bowiem zawsze dynamiczna i może się okazać, że niezbędna jest inna taktyka w stosunku do któregoś z interesariuszy zaliczanych do niej.

Oczywiście inny charakter będą miały działania w stosunku do interesariuszy pozytywnie nastawionych do projektu a inny nastawionych niechętnie.

W tym pierwszym przypadku należy dążyć do podjęcia aktywnej współpracy tak, aby z korzyścią dla przedsięwzięcia wykorzystać wiedze, zasoby, kontakty, autorytet interesariusza a w rezultacie stworzyć pozytywna koalicję zapewniającą przedsięwzięciu wsparcie.

W przypadku interesariuszy nastawionych niechętnie należy doprowadzić do zaangażowania ich do współpracy: oswoić, wzbudzić zaufanie, pokazać pozytywy, uwzględnić częściowo interesy, a w ostateczności (jeśli nie da się inaczej) dzięki sojusznikom ograniczyć ich wpływ.

Poniższa tabela prezentuje, jakie akcje należy przedsiębrać w stosunku do poszczególnych grup (pogrubiony krzyżyk oznacza dominującą kategorię działań):

Działania	Informujące	Konsultacyjne	Angażujące
Grupa 1	X	X	**X**
Grupa 2	X	**X**	
Grupa 3	**X**	X	
Grupa 4	**X**		

Tabela 3

dr inż. Dariusz Bogucki - teleinformatyk od ponad 15 lat informatyzujący administracje publiczną. Rzeczoznawca PTI. Wykładowca na Wydziale Prawa i Administracji Uniwerytetu Kardynała Stefana Wyszyńskiego

Zapraszamy do udziału

WARSZTATY

PRAWNE I PRAKTYCZNE ASPEKTY ROZPOWSZECHNIANIA INFORMACJI PRASOWYCH ORAZ MATERIAŁÓW PROMOCYJNYCH W INTERNECIE

Warszawa, 1.10.2013

W ramach dwóch bloków tematycznych omówione zostaną zagadnienia prawne oraz praktyczne dotyczące przygotowywania informacji handlowych oraz materiałów promocyjnych. W ramach pierwszej części warsztatów omówione zostaną między innymi najnowsze zmiany prawne dotyczące przesyłania informacji handlowych oraz najnowsze orzecznictwo dotyczące rozpowszechniania materiałów promocyjnych.

Pierwszą cześć warsztatów poprowadzi doświadczony radca prawny Roman Bieda. W ramach drugiej części warsztatów przedstawione zostaną praktyczne aspekty redagowania informacji w różnych formatach promocyjnych online - serwisach WWW, e-mailingach i newsletterach, reklamie display, a także mediach społecznościowych. Drugą część poprowadzi 15-letni praktyk w branży internetowej - trener, publicysta oraz konsultant Artur Maciorowski.

CEL WARSZTATÓW

W ramach szkolenia przedstawione zostaną między innymi:

- Zasady rozpowszechniania informacji handlowych (mailingu), w tym najnowsze zmiany prawne dotyczące przesyłania informacji handlowych,
- Zasady odpowiedzialności za przesyłanie niezamówionych informacji handlowych,
- Regulacje prawne dotyczące rozpowszechniania materiałów informacyjnych i promocyjnych,
- Dopuszczalne granice wypowiedzi promocyjnych,
- Najnowsze orzecznictwo i przykłady z praktyki dotyczące rozpowszechnienia informacji i tekstów promocyjnych w Internecie.
- Zasady redagowania treści w ramach różnych typów serwisów internetowych - firmowych, produktowych i landing pages
- Sposoby weryfikacji skuteczności informacji prezentowanych online, czyli ile, jak i w jaki sposób czytają użytkownicy Internetu
- Efektywne sposoby redagowania komunikatów reklamowych w ramach e-mailingów
- Sprawdzone praktyki budowania i publikacji treści w newsletterach
- Najnowsze trendy w zakresie tworzenia kreacji odsłonowych (display)
- Skuteczne metody komunikacji w mediach społecznościowych - najlepsze posty, efektywne treści i formaty w social media.

Więcej informacji: www.cpi.com.pl

Zastosowanie dokumentów elektronicznych w postępowaniu administracyjnym

Katarzyna Czajkowska-Matosiuk

Konieczność wprowadzenia do postępowania administracyjnego środków komunikacji elektronicznej spowodowana jest stałym rozwoje techniki i metod komunikacji międzyludzkiej. W spółczesnym świecie trudno wyobrazić sobie funkcjonowanie administracji publicznej bez uwzględnienia nowych rozwiązań w tym zakresie.

Zasada formy załatwiania spraw

Jedną z ogólnych zasad postępowania administracyjnego jest zasada formy załatwiania spraw. Jej treść posiada zatem charakter wiążący na każdym etapie postępowania. Uchybienie tej zasadzie stanowi naruszenie prawa i może stanowić samoistną podstawę uchylenia aktu wydanego w ramach dokonanego naruszenia.

Zasada formy załatwiania spraw określona została w treści art. 14. KPA. Zgodnie z tym przepisem, sprawy należy załatwiać w formie pisemnej lub w formie dokumentu elektronicznego w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, z późn. zm.) doręczanego środkami komunikacji elektronicznej. Sprawy mogą być załatwiane ustnie, gdy przemawia za tym interes strony, a przepis prawny nie stoi temu na przeszkodzie. Treść oraz istotne motywy takiego załatwienia powinny być utrwalone w aktach w formie protokołu lub podpisanej przez stronę adnotacji.

Wynika z tego, że istnieją dwie równoważne względem siebie formy czynności administracyjnych, tj.:

1) forma pisemna oraz
2) forma dokumentu elektronicznego (zgodnie z art. 3 pkt 2 Ustawy o informatyzacji, dokument elektroniczny to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych).

Jednocześnie ustawodawca nie dokonał zróżnicowania procesowego znaczenia wskazanych form. W szczególności nie uczynił formy dokumentu elektronicznego formą czynności podrzędną względem formy pisemnej. Należy zatem uznać, że forma dokumentu elektronicznego nie stanowi, na wzór formy ustnej, wyjątku od reguły stosowania formy pisemnej, lecz jest względem formy pisemnej równoważną a zarazem alternatywną kategorią formy czynności procesowych.

Uwaga!

Zastosowanie formy dokumentu elektronicznego nie powoduje jednak, że wszystkie czynności procesowe będą musiały być realizowane w tej formie.

Forma dokumentu elektronicznego może być zastosowana również odnośnie czynności, co do których ustawa nie wprowadza żadnej obowiązkowej formy. A zatem niedopuszczalność formy dokumentu elektronicznego będzie miała miejsce wyłącznie w przypadku czynności postępowania, co do których przepisy wprost zastrzegają jako wyłączną formę pisemną lub w przypadku

których zastosowanie formy dokumentu elektronicznego nie będzie możliwe z przyczyn technicznych.

Dobrym przykładem czynności dokonywanej w formie dokumentu elektronicznego jest decyzja administracyjna. Decyzja taka nie tylko może, lecz na skutek żądania strony również powinna zostać wydana w formie dokumentu elektronicznego. Z art. 107 § 1 KPA wynika, że decyzja administracyjna wydana w formie dokumentu elektronicznego powinna zawierać następującą treść:

1) oznaczenie organu administracji publicznej,
2) datę wydania,
3) oznaczenie strony lub stron,
4) powołanie podstawy prawnej,
5) rozstrzygnięcie,
6) uzasadnienie faktyczne i prawne,
7) pouczenie, czy i w jakim trybie służy od niej odwołanie.

Ponadto decyzja administracyjna w formie elektronicznej powinna zostać opatrzona tzw. bezpiecznym podpisem elektronicznym, weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, lub podpisem osobistym.

Innym przykładem formy administracyjnego dokumentu elektronicznego jest forma wezwania. Z art. 54 KPA wynika, że wezwanie wystosowane w formie dokumentu elektronicznego powinno zawierać:

1) nazwę i adres organu wzywającego,
2) imię i nazwisko wzywanego,
3) wskazanie, w jakiej sprawie oraz w jakim charakterze i w jakim celu zostaje wezwany,
4) wskazanie, czy wezwany powinien się stawić osobiście lub przez pełnomocnika, czy też może złożyć wyjaśnienie lub zeznanie na piśmie,
5) wskazanie terminu, do którego żądanie powinno być spełnione, albo dzień, godzinę i miejsce stawienia się wezwanego lub jego pełnomocnika,
6) określenie skutków prawnych niezastosowania się do wezwania.

Podobnie jak w przypadku decyzji wezwanie powinno zostać opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym.

Zgodnie z treścią Ustawy o informatyzacji oraz stosownych przepisów wykonawczych, w tym szczególnie Rozporządzenia prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych, dopuszcza się doręczenie dokumentów elektronicznych do podmiotu publicznego, w tym organu administracji publicznej:

1) za pomocą środków komunikacji elektronicznej, tj. za pomocą:
   a) elektronicznej skrzynki podawczej,
   b) na adres poczty elektronicznej organu administracyjnego;
2) poprzez doręczenie informatycznego nośnika danych zawierającego zapis dokumentu elektronicznego.

Pojęcie środków komunikacji elektronicznej oznacza rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

Wybór metody komunikacji elektronicznej

Uznanie przez ustawodawcę formy dokumentu elektronicznego, jako formy czynności procesowej alternatywnej

i równoważnej względem formy pisemnej, nie oznacza dowolności jej stosowania. Prawo wyboru formy dokumentu przysługuje adresatowi działań administracyjnych, tj. stronie lub innemu uczestnikowi postępowania. Osoba ta dysponuje dwojakiego rodzaju uprawnieniami:

1) prawem posługiwania się względem organu administracyjnego formą dokumentu elektronicznego bez konieczności uzyskania w tym względzie uprzedniej zgody organu,
2) prawem do decydowania o możliwości doręczania jej przez organ pism procesowych w formie dokumentu elektronicznego.

O ile więc organ administracyjny nie może się przeciwstawić praktyce doręczania pism w formie dokumentu elektronicznego, o tyle adresat pisma procesowego doręczanego przez organ administracyjny pozostaje wyłącznym dysponentem prawa decydowania o możliwości doręczenia tego pisma w formie dokumentu elektronicznego.

Powyższe uprawnienie wynika z art. 39^{1} § 1 KPA. Zgodnie z tym przepisem, doręczenie następuje za pomocą środków komunikacji elektronicznej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, zpóźn. zm.), jeżeli strona lub inny uczestnik postępowania wystąpił do organu administracji publicznej o doręczenie albo wyraził zgodę na doręczenie mu pism za pomocą tych środków

Jeżeli zatem strona lub inny uczestnik postępowania wystąpił do organu administracji publicznej o doręczanie mu pism za pomocą środków komunikacji elektronicznej lub wyraził zgodę na tego rodzaju doręczanie, to organ administracji publicznej jest zobowiązany zastosować tę metodę.

Wynikają z tego dwie istotne zasady:

1) złożenie oświadczenia w przedmiocie doręczania pism organu za pomocą środków komunikacji elektronicznej poza tokiem postępowania jest nieskuteczne i nie wiąże organu administracji publicznej,
2) oświadczenie wniesione skutecznie wiąże wyłącznie od momentu jego złożenia do zakończenia sprawy decyzją ostateczną.

Oświadczenie w przedmiocie doręczania przez organ administracyjny pism za pomocą środków komunikacji elektronicznej może zostać wyrażone na dwa sposoby:

1) poprzez żądanie, tj. wystąpienie do organu administracji publicznej o doręczanie pism za pomocą środków komunikacji elektronicznej,
2) poprzez zgodę, tj. pozytywną odpowiedź na propozycję organu doręczania pism za pomocą środków komunikacji elektronicznej.

Żądanie doręczania pism za pomocą środków komunikacji elektronicznej może zostać wniesione wraz z podaniem o wszczęcie postępowania, jak również w postaci odrębnego dokumentu składanego jednocześnie, lecz niezależnie względem dokumentu podania lub zupełnie odrębnie w toku postępowania, przy czym należy uznać możliwość zintegrowania treści żądania z dokumentem zawierającym żądanie dotyczące określonej czynności procesowej, w tym również czynności innej niż żądanie wszczęcia postępowania (np. żądanie zawieszenia postępowania). Żądanie to możne zostać doręczone zarówno w formie dokumentu elektronicznego, jak również w formie pisemnej lub może zostać wyrażone w formie ustnej i podlegać zaprotokołowaniu.

Celem wywołania zamierzonego skutku, żądanie powinno spełniać wymagania formalne właściwe dla podania, tj. zgodnie z art. 63 powinno zawierać:

1) wskazanie osoby, od której pochodzi,
2) adres tej osoby,
3) treść żądania, zawierającą w tym przypadku wskazanie adresu elektronicznego do doręczeń.

W praktyce zdarzają się jednak istotne problemy związane z załatwianiem spraw w formie dokumentu elektronicznego, zwłaszcza w przypadku wielu stron postępowania. Współuczestnictwo wielu stron w ramach jednego postępowania może skutkować żądaniem doręczenia pism za pomocą środków komunikacji elektronicznej wyrażonym wyłącznie przez niektóre strony. W takiej sytuacji organ administracyjny jest zobowiązany zadość uczynić wniesionemu żądaniu i dokonać doręczeń pism za pomocą środków komunikacji elektronicznej. Względem pozostałych stron organ administracyjny pozostanie zobligowany dokonywać doręczeń w formie pisemnej. Problem powstaje, gdy to samo pismo ma zostać doręczone stronie, która wniosła o doręczenie pism za pomocą środków komunikacji elektronicznej oraz stronie, która takiego żądania nie złożyła.

Jako przykład można wskazać decyzję administracyjną. Każde z doręcznych pism, tj. zarówno pisma w formie pisemnej, jak i pisma w formie dokumentu elektronicznego, będzie stanowić równoważny egzemplarz pisma dokumentującego tę samą czynność. Zgodnie z treścią art. 107 KPA każda decyzja powinna zawierać m.in. datę wydania oraz powinna zostać opatrzona podpisem, odpowiednio, własnoręcznym lub bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub podpisem osobistym. Biorąc pod uwagę, że data wydania decyzji stanowi datę złożenia podpisu na decyzji, należy przestrzec przez niezgodnością na linii data wydania decyzji wskazana w decyzji opatrzonej podpisem własnoręcznym, a data złożenia podpisu elektronicznego na decyzji w formie dokumentu elektronicznego. O ile bowiem złożenie podpisu własnoręcznego nie daje możliwości zweryfikowania daty jego złożenia, a co za tym idzie, wskazanie tej daty w treści decyzji należy uznać za prawnie doniosłe, o tyle charakter podpisu elektronicznego pozwala na weryfikację daty jego złożenia, a co za tym idzie, data wskazana w treści decyzji nie ma prawnego znaczenia. W konsekwencji wygenerowanie dwóch egzemplarzy tej samej decyzji o tożsamej dacie jej wydania, ustalonej w ramach jej treści, przy jednoczesnym złożeniu podpisu elektronicznego w dacie późniejszej może spowodować wątpliwości w przedmiocie kwalifikacji egzemplarza decyzji w formie dokumentu elektronicznego oraz egzemplarza decyzji w formie pisemnej, jako egzemplarzy tej samej decyzji. Odmienność dat wydania decyzji powinna skutkować co najmniej sprostowaniem przez organ administracji publicznej oczywistej omyłki co do daty uwidocznionej na egzemplarzu decyzji w formie pisemnej.

Dodatkowo należy zauważyć, że brak jednolitości w przedmiocie wyboru metody doręczenia pism procesowych powinien stanowić szczególną podstawę do wystąpienia przez organ administracyjny względem podmiotów, które nie zażądały doręczania za pomocą środków komunikacji elektronicznej, o zgodę na tego rodzaju doręczanie. U podstaw wystąpienia o zgodę stoi w tym przypadku zasada szybkości postępowania. Niewątpliwie bowiem szybkość postępowania pozostaje uzależniona od tempa działań dyktowanych mniej dynamiczną mechaniką doręczeń, tj. doręczeń dokumentu w formie pisemnej. Tym samym korzyść wynikająca z charakteru komunikacji elektronicznej względem osób, które wystąpiły z żądaniem doręczania pism za pomocą środków komunikacji elektronicznej, będzie miała charakter iluzoryczny.

Doręczanie pisma procesowego

Zasady doręczania dokumentu elektronicznego przez organ administracyjny regulują przepisy art. 46 § 3-6 KPA. Przede wszystkim należy rozróżnić metodę doręczania pisma przez organ administracji publicznej do podmiotu publicznego od metody doręczenia pisma kierowanego do strony lub innego uczestnika postępowania. Zgodnie z art. 46 § 6 KPA doręczenie dokumentu w formie dokumentu elektronicznego do podmiotu publicznego, w rozumieniu przepisów Ustawy o informatyzacji, następuje przez elektroniczną skrzynkę podawczą tego podmiotu. Tymczasem doręczenie pisma procesowego w formie dokutemu elektronicznego, względem strony lub innego uczestnika postępowania administracyjnego, następuje w ramach złożonej procedury udostępnienia dokumentu.

Etapy tej procedury określa art. 46 § 4 KPA, zgodnie z którym w celu doręczenia dokumentu w formie dokumentu elektronicznego organ administracji publicznej przesyła na adres elektroniczny adresata informację zawierającą:

1) wskazanie, że adresat może odebrać dokument w formie dokumentu elektronicznego;
2) wskazanie adresu elektronicznego, z którego adresat może pobrać dokument i pod którym powinien dokonać potwierdzenia doręczenia dokumentu;
3) pouczenie dotyczące sposobu odbioru dokumentu, a szczególnie sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu administracji publicznej oraz informacji o wymogu podpisania urzędowego poświadczenia odbioru, w sposób wskazany w art. 20a Ustawy o informatyzacji.

A zatem proces doręczenia pisma w formie dokumentu elektronicznego nie polega na przesłaniu dokumentu na adres elektroniczny adresata. Na adres elektroniczny adresata zostaje przesłana wyłącznie informacja o możliwości oraz zasadach pobrania pisma, które niezmiennie pozostaje w systemie teleinformatycznym organu administracyjnego. Szczegółowe zasady pobrania pisma określa Rozporządzenie prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

Zgodnie z treścią § 14-16 rozporządzenia poświadczenie doręczenia jest udostępniane przez system informatyczny podmiotu publicznego w celu umożliwienia podpisania tego poświadczenia przez adresata dokumentu elektronicznego i zawiera:

1) pełną nazwę podmiotu publicznego, który doręcza dokument elektroniczny;
2) pełną nazwę podmiotu, któremu podmiot publiczny doręcza dokument elektroniczny;
3) oznaczenie sprawy;
4) jednoznaczne oznaczenie pisma, którego dotyczy;
5) w przypadku podpisania poświadczenia doręczenia - datę i czas podpisania, rozumiane jako data i czas doręczenia dokumentu elektronicznego.

Adresat dokumentu elektronicznego potwierdza jego odebranie przez opatrzenie poświadczenia doręczenia podpisem elektronicznym umożliwiającym identyfikację podpisującego, tj.

1) bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu,
2) podpisem potwierdzonym profilem zaufanym ePUAP lub
3) podpisem osobistym.

Po opatrzeniu poświadczenia doręczenia podpisem elektronicznym, system teleinformatyczny służący do obsługi doręczeń bezpośrednio po zakończeniu procesu weryfikacji podpisu elektronicznego adresata:

1) udostępnia adresatowi do pobrania doręczany dokument elektroniczny wraz z podpisanym przez niego poświadczeniem doręczenia;
2) udostępnia organowi doręczającemu podpisane poświadczenie doręczenia.

Co istotne, zgodnie z § 6 rozporządzenia, w przypadku niepotwierdzenia doręczenia, system teleinformatyczny organu administracyjnego, służący do obsługi doręczeń, powinien dokonać automatycznego wygenerowania informacji wskazującej, że poświadczenie doręczenia nie zostało potwierdzone.

Doręczenie pisma w formie dokumentu elektronicznego jest traktowane przez ustawodawcę jako dokonywane przy wykorzystaniu techniki doręczenia o ograniczonej gwarancji niezawodności. Tym samym doręczenie pisma za pomocą środków komunikacji elektronicznej może odnieść skutek jedynie poprzez potwierdzenie poświadczenia doręczenia przez adresata pisma. Zgodnie z treścią art. 46 § 3 KPA w przypadku doręczenia pisma za pomocą środków komunikacji elektronicznej doręczenie jest skuteczne, jeżeli w terminie 7 dni od dnia wysłania pisma organ administracji publicznej otrzyma potwierdzenie doręczenia pisma. W razie nieotrzymania takiego potwierdzenia organ doręcza pismo w sposób określony w przepisach niniejszego rozdziału dla pisma w formie innej niż forma dokumentu elektronicznego.

Treść regulacji art. 46 § 3 KPA stanowi przejaw ograniczonego zaufania ustawodawcy do technologii komunikacji elektronicznej. Brak potwierdzenia poświadczenia doręczenia w terminie siedmiu dni od dnia wysłania informacji o możliwości i zasadach odbioru pisma, czyni doręczenie pisma w formie dokumentu elektronicznego doręczeniem nieskutecznym. Celem doręczenia pisma organ administracyjny jest zobowiązany dokonać sporządzenia kolejnego egzemplarza pisma, tym razem w formie pisemnej i w takiej też postaci dokonać jego doręczenia. Dokument w formie pisemnej będzie stanowił oryginalny, kolejny egzemplarz tego samego pisma, tj. pisma istniejącego dotychczas w postaci egzemplarza w formie dokumentu elektronicznego. Należy zwrócić uwagę na konieczną zgodność daty dokonania czynności, uzewnętrznionej w każdym z egzemplarzy, z tym zastrzeżeniem, że data uwidoczniona w treści egzemplarza w formie pisemnej powinna być zgodna nie tyle z datą wskazaną w treści egzemplarza w formie elektronicznej, lecz datą opatrzenia go podpisem elektronicznym.

Doręczenie w formie pisemnej należy uznać za jednostkowe. Oznacza to, że kolejne pismo organ administracyjny jest niezmiennie zobowiązany doręczyć w formie dokumentu elektronicznego. Nieskuteczne doręczenie danego pisma w formie dokumentu elektronicznego nie wyłącza obowiązku stosowania elektronicznej metody doręczeń, aktywowanej na skutek oświadczenia strony lub innego uczestnika postępowania. Doręczenie w formie pisemnej jest dopuszczalne jedynie na zasadzie zabezpieczenia doręczenia pisma, którego doręczenie w formie dokumentu elektronicznego okazało się nieskuteczne. Jednocześnie należy podkreślić niedopuszczalność kwalifikacji nieskutecznego doręczenia, za pomocą środków komunikacji elektronicznej, jako doręczenia niebyłego. Fakt podjęcia próby doręczenia ma bowiem istotne znacznie dla oceny czynności procesowych jako podejmowanych w sposób ekonomiczny i terminowy. Nieskuteczne doręczanie dokumentu elektronicznego może mieć zatem szczególne znacznie dla oceny zasadności

potencjalnego zażalenia na niezałatwienie sprawy w terminie lub zażalenia na przewlekłość prowadzenia postępowania.

Wezwanie

Stosownie do obowiązujących przepisów, wezwanie powinno mieć formę pisemną lub formę dokumentu elektronicznego. Celem dokonania prawidłowego i skutecznego wezwania niezbędne jest jednak ustalenie jego treści w ramach określonych elementów formalnych. Zgodnie z art. 54 § 1 i § 2 KPA w wezwaniu należy wskazać:

1) nazwę i adres organu wzywającego,
2) imię i nazwisko wzywanego,
3) w jakiej sprawie oraz w jakim charakterze i w jakim celu zostaje wezwany,
4) czy wezwany powinien się stawić osobiście lub przez pełnomocnika, czy też może złożyć wyjaśnienie lub zeznanie na piśmie,
5) termin, do którego żądanie powinno być spełnione, albo dzień, godzinę i miejsce stawienia się wezwanego lub jego pełnomocnika,
6) skutki prawne niezastosowania się do wezwania.

Tak ustalona treść powinna zostać dodatkowo opatrzona podpisem pracownika organu wzywającego, z podaniem imienia, nazwiska i stanowiska służbowego podpisującego lub, jeżeli wezwanie posiada formę dokumentu elektronicznego, powinno być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym. Możliwość doręczenia wezwania w formie dokumentu elektronicznego nie budzi zatem najmniejszych wątpliwości.

Jednakże w myśl art. 50 § 1 KPA, organ administracji publicznej może wzywać osoby do udziału w podejmowanych czynnościach i do złożenia wyjaśnień lub zeznań osobiście, przez pełnomocnika lub na piśmie, jeżeli jest to niezbędne dla rozstrzygnięcia sprawy lub dla wykonywania czynności urzędowych. Zakres wezwania zostaje zatem ograniczony wyłącznie do udziału w czynnościach procesowych i do złożenia wyjaśnień:

1) w drodze osobistego stawiennictwa,
2) działania przez pełnomocnika,
3) na piśmie.

Przepis ten nie przewiduje zatem możliwości wezwania do złożenia wyjaśnień w formie dokumentu elektronicznego.

Zestawienie powyższych regulacji prowadzi do następujących wniosków:

1) organ administracyjny nie może dokonać skutecznego wezwania osoby do złożenia wyjaśnień w formie dokumentu elektronicznego, nawet jeżeli zostały spełnione wymagania 39^1 KPA W przypadku dokonania takiego wezwania wezwany nie jest zobowiązany do uczynienia mu zadość, zaś organ administracyjny nie jest uprawniony do zastosowania jakiejkolwiek sankcji;
2) wezwany do złożenia wyjaśnień na piśmie jest uprawniony do złożenia wyjaśnień również w formie dokumentu elektronicznego.

Zachowanie terminu

Podstawową metodą dokonania czynności procesowej jest jej osobista realizacja przed organem administracyjnym albo jej przedłożenie w formie pisemnej na dzienniku podawczym. W takim przypadku dowodem na okoliczność zachowania terminu staje się data dokonania czynności wskazana w protokole lub umieszczona na dokumencie prezentata, której dokonuje osoba przyjmująca na dzienniku podawczym.

Ponadto czynność procesowa adresowana względem organu administracyjnego może być dokonana w formie pisemnej w sposób pośredni poprzez:
1) nadanie pisma w polskiej placówce pocztowej operatora publicznego,
2) złożenie w polskim urzędzie konsularnym,
3) złożenie przez żołnierza w dowództwie jednostki wojskowej,
4) złożenie przez członka załogi statku morskiego kapitanowi statku,
5) złożenie przez osobę pozbawioną wolności w administracji zakładu karnego.

Zgodnie z treścią art. 57 § 5 pkt 2-6 KPA zachowanie terminu w przypadku pisma składanego w jeden z wyżej wymienionych sposobów nastąpi, jeżeli złożenie lub nadanie pisma zostanie dokonane przed upływem terminu. Dowodem na okoliczność zachowania terminu będzie w tym przypadku, odpowiednio, data stempla pocztowego lub potwierdzenie wniesienia pisma dokonane przez właściwy podmiot. Tak zaprojektowany system doręczeń gwarantuje, co do zasady, że dochowanie należytej staranności ze strony osoby wnoszącej pismo wywoła skutek w postaci zachowania terminu. Jedyna przesłanka zachowania terminu, tj. przesłanka nadania lub złożenia pisma przed upływem terminu, pozostaje zatem w domenie działań osoby dokonującej czynności.

W przeciwieństwie do zasad zachowania terminu czynności dokonywanej w formie pisemnej lub ustanej, regulacja zachowania terminu w przypadku czynności dokonywanej w formie dokumentu elektronicznego odchodzi od zasady ścisłego powiązania skutku z elementem należytej staranności. Zgodnie z treścią art. 57 § 5 pkt 1 KPA termin uważa się za zachowany, jeżeli przed jego upływem pismo zostało wysłane w formie dokumentu elektronicznego do organu administracji publicznej, a nadawca otrzymał urzędowe poświadczenie odbioru.

Celem zachowania terminu konieczna jest zatem realizacja dwóch wymogów:
1) wniesienia pisma przed upływem terminu oraz
2) otrzymania przed upływem terminu urzędowego poświadczenia odbioru.

Co istotne zarówno wniesienie pisma, jak i otrzymanie urzędowego poświadczenia odbioru przez organ administracyjny tego pisma powinny nastąpić przed upływem terminu dla dokonania czynności, co oznacza, że brak realizacji chociażby jednego z nich powoduje niezachowanie terminu.

Zgodnie z regulacją § 13 Rozporządzenia prezesa Rady Ministrów w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych, w przypadku odebrania dokumentu elektronicznego przez elektroniczną skrzynkę podawczą podmiotu publicznego urzędowego poświadczenia odbioru (zwane w rozporządzeniu poświadczeniem przedłożenia) jest automatycznie tworzone i udostępniane nadawcy tego dokumentu przez system teleinformatyczny służący do obsługi doręczeń. Za udostępnienie nadawcy urzędowego poświadczenia odbioru uważa się szczególnie jego przekazanie do pozostającej w dyspozycji odbiorcy poświadczenia skrytki w ramach systemu teleinformatycznego podmiotu publicznego służącego do obsługi doręczeń.

Jeżeli nie jest możliwe udostępnienie automatycznie wytworzonego urzędowego poświadczenia odbioru w powyższy sposób, poświadczenie to wysyłane jest na adres elektroniczny wskazany przez wnoszącego, z tym że może to być:
1) adres poczty elektronicznej albo
2) inny adres elektroniczny, pod warunkiem, że jest obsługiwany przez system teleinformatyczny służący do obsługi doręczeń.

A zatem bezawaryjne funkcjonowanie urządzeń transmisji elektronicznej oraz systemu teleinformatycznego organu administracyjnego powinno zapewnić automatyczne wygenerowanie i doręczenie urzędowego poświadczenia odbioru w ciągu tzw. logicznej sekundy. Należy jednak zwrócić uwagę, że ogół wskazanych uwarunkowań pozostaje poza sferą ingerencji osoby dokonującej czynności. Oznacza to, że nawet przy zachowaniu należytej staranności może dojść do sytuacji, w której hipoteza art. 57 § 5 pkt 1 KPA nie zostanie zrealizowana, a tym samym dokonana czynność nie zostanie uznana za czynność dokonaną z zachowaniem terminu.

Na koniec należy doprecyzować charakter urzędowego poświadczenia odbioru, o którym mowa w treści art. 57 § 5 pkt 1 KPA. Ustawowa definicja urzędowego poświadczenia odbioru została zawarta w treści art. 3 pkt 20 Ustawy o informatyzacji. Zgodnie z jego treścią urzędowe poświadczenie odbioru to dane elektroniczne dołączone do dokumentu elektronicznego doręczonego podmiotowi publicznemu lub połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna. Urzędowe poświadczenie odbioru powinno określać: pełną nazwę podmiotu publicznego, któremu doręczono dokument elektroniczny, datę i godzinę doręczenia dokumentu elektronicznego, rozumiane jako data i czas wprowadzenia albo przeniesienia dokumentu elektronicznego do systemu teleinformatycznego podmiotu publicznego, datę i godzinę wytworzenia urzędowego poświadczenia odbioru. Należy zwrócić uwagę, że tak rozumiane urzędowe poświadczenie obioru dotyczy pism kierowanych do podmiotu publicznego, a zatem stanowi ono dowód otrzymania pisma przez organ administracyjny.

Wszczęcie postępowania

Zgodnie z treścią art. 61 §1 KPA § 1 postępowanie administracyjne wszczyna się na żądanie strony lub z urzędu. Analiza stosowania formy dokumentu elektronicznego w postępowaniu administracyjnym wymaga rozważenia stosowalności tej formy na potrzeby każdego ze sposobów wszczęcia postępowania. Jednocześnie należy zastrzec, że charakter postępowania w danej sprawie, tj. postępowania wnioskowego lub wszczynanego z urzędu, pozostaje determinowany przepisami prawa materialnego.

Wszczęcie postępowania z urzędu oznacza wszczęcie postępowania z inicjatywy organu, przy czym przepisy Kodeksu nie przewidują wydania na tę okoliczność aktu administracyjnego. Bezspornie natomiast, zgodnie z treścią art. 61 § 4 KPA o wszczęciu postępowania z urzędu lub na żądanie jednej ze stron, należy zawiadomić wszystkie osoby będące stronami w sprawie. Praktyka działań organów administracyjnych dowodzi, że zawiadomienie o wszczęciu postępowania stanowi zasadniczo pierwszą czynność postępowania wszczętego z urzędu.

Z orzecznictwa…

„Wobec faktu, że KPA nie rozstrzyga sposobu ustalenia daty wszczęcia postępowania administracyjnego z urzędu za datę taką można uznać dzień pierwszej czynności dokonanej w sprawie, której postępowanie dotyczy, przez organ do tego uprawniony, działający w granicach przysługujących mu kompetencji, pod warunkiem, że o czynności tej powiadomiono w sprawie".

Wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 1981 r., sygn.: SA 678/81.

Mając powyższe na względzie, należy stwierdzić, że pierwszą czynnością dokonaną w sprawie, w której postępowanie zostało wszczęte z urzędu, może być zarówno zawiadomienie skierowane do strony, jak również czynność, której adresatem jest podmiot inny niż strona, byleby strona o tej czynności

została powiadomiona. Jednak czynność inicjująca postępowanie wszczęte z urzędu nie może mieć formy dokumentu elektronicznego. Zasadnicze znacznie w tej mierze ma regulacja art. 39^1 § 1 KPA, warunkująca dopuszczalność doręczeń pism w formie dokumentu elektronicznego od żądania lub zgody na tego rodzaju doręczenia. Oczywistym jest, że w przypadku postępowania wszczętego z urzędu organ administracyjny nie dysponuje stosownym oświadczeniem, a co za tym idzie, za jedyną dopuszczalną metodę doręczeń należy uznać doręczenia w formie pisemnej.

W szczególności prawa do dokonania doręczenia za pomocą środków komunikacji elektronicznej nie można wywodzić z oświadczenia wyrażonego w tym względzie w toku poprzedniego postępowania administracyjnego lub poza postępowaniem administracyjnym. Oświadczenie, o którym mowa w treści art. 39^1 § 1 KPA, stanowi oświadczenie jednokrotnie wiążące, tzn. wiążące wyłącznie w toku postępowania, w ramach którego zostało wyrażone, tj. wyłącznie od daty jego złożenia w toku postępowania do daty zakończenia sprawy decyzją ostateczną. W konsekwencji, dokonując pierwszej czynności w sprawie, w której postępowanie zostało wszczęte z urzędu, organ powinien dokonać jej w formie innej niż forma dokumentu elektronicznego, tj. w formie pisemnej lub ustnej. Dążąc do wdrożenia w ramy wszczętego postępowania metody doręczeń za pomocą środków komunikacji elektronicznej, organ administracyjny, dokując pierwszej czynności, może wystąpić na mocy art. 39^1 §1 KPA do strony postępowania o zgodę na doręczanie jej pism za pomocą środków komunikacji elektronicznej.

Wszczęcie postępowania wnioskowego oznacza podjęcie postępowania na żądanie przedłożone przez stronę w rozumieniu art. 28 KPA Tym samym powyższego wymogu nie spełnia żądanie przedłożone do organu administracyjnego przez podmiot na prawach strony (organizację społeczną, prokuratora, Rzecznika Praw Obywatelskich). Żądanie wszczęcia postępowania administracyjnego, wniesione przez podmiot na prawach strony, może odnosić się wyłącznie do postępowań wszczynanych z urzędu bądź w drodze wyjątku do postępowania wnioskowego, które na mocy art. 61 § 2 KPA może zostać przez organ administracyjny wszczęte z urzędu ze względu na szczególnie ważny interes strony. Bez względu jednak na okoliczności, wszczęcie postępowania na żądanie podmiotu na prawach strony pozostaje kwalifikowane jako wszczęcie postępowania z urzędu, ze wszystkimi tego konsekwencjami[1].

Zasady wnoszenia podań w formie dokumentu elektronicznego reguluje art. 63 KPA Biorąc pod uwagę, że zagadnienie wniesienia podania w formie dokumentu elektronicznego stanowi przedmiot odrębnej szczegółowej analizy, w tym miejscu należy jedynie odnieść się do metody wniesienia podania. Zgodnie z treścią art. 63 § 1 KPA podstawową metodę wniesienia podania w formie dokumentu elektronicznego stanowi wniesienie podania za pomocą środków komunikacji elektronicznej przez elektroniczną skrzynkę podawczą. Ponadto za wniesienie podania w formie dokumentu elektronicznego należy również uznać wniesienie podania za pomocą telefaksu. Celem skutecznego wniesienia podania w formie dokumentu elektronicznego podanie to musi spełniać wymaganie określone regulacją art. 63 § 2 i § 3a KPA, tj. podanie powinno zawierać co najmniej:

1) wskazanie osoby, od której pochodzi,
2) jej adres,

1 *R. Kędziora*; Kodeks … op. cit.

3) żądanie oraz
4) czynić zadość innym wymaganiom ustalonym w przepisach szczególnych.

Dodatkowo podanie to powinno zawierać dane w ustalonym formacie, zawartym we wzorze podania określonym w odrębnych przepisach, jeżeli te przepisy nakazują wnoszenie podań według określonego wzoru. Ponadto treść podania powinna ulec personalizacji w drodze mechanizmów, o których mowa w treści art. 20a ust. 1 albo ust 2 Ustawy o informatyzacji, tj. powinno zostać opatrzone:

1) bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub
2) podpisem potwierdzonym profilem zaufanym ePUAP, lub
3) podpisem osobistym.

Wszczęcie postępowania wnioskowego wymaga ustalenia daty jego wszczęcia. Reguła art. 61 KPA normująca datę wszczęcia postępowania w formie innej niż forma dokumentu elektronicznego stanowi: datą wszczęcia postępowania na żądanie strony jest dzień doręczenia żądania organowi administracji publicznej.

Ustawodawca wiąże datę wszczęcia postępowania z możliwością zapoznania się przez organ z treścią podania. Należy zauważyć, że możliwość ta pozostaje warunkowana wewnętrznymi ustaleniami o charakterze organizacyjnym, np. regulaminem organizacyjnym urzędu gminy określającym godziny funkcjonowania urzędu. Tym samym data wszczęcia postępowania na żądanie strony pozostaje w ścisłej korelacji z regulacją pracy urzędu administracyjnego. Celem skutecznego doręczenia podania organowi administracyjnemu podanie to powinno bowiem zostać złożone na dzienniku podawczym w urzędzie. Zakończenie godzin pracy organu administracyjnego oznacza niemożność skutecznego wszczęcia postępowania wnioskowego, aż do momentu ponownego podjęcia pracy, tj. otwarcia urzędu, szczególnie zaś podjęcia pracy przez pracowników realizujących czynności w ramach funkcji dziennika podawczego[2].

W przeciwieństwie do powyższej regulacji, wszczęcie postępowania na żądanie wniesione w formie dokumentu elektronicznego pozostaje niezależne względem zasad organizacji pracy urzędu. Zgodnie z treścią art. 61 § 3a KPA: datą wszczęcia postępowania na żądanie strony wniesione drogą elektroniczną jest dzień wprowadzenia żądania do systemu teleinformatycznego organu administracji publicznej.

Przede wszystkim należy zauważyć, że data wszczęcia postępowania na żądanie wniesione w formie dokumentu elektronicznego nie odnosi się do doręczenia żądania organowi administracji publicznej. Momentem konstytuującym datę wszczęcia postępowania jest data wprowadzenia żądania do systemu teleinformatycznego organu administracji publicznej, tj. zapisania dokumentu elektronicznego na serwerze obsługującym system teleinformatyczny organu administracyjnego. Za skuteczne należy uznać wniesienie podania również poza godzinami pracy urzędu. Należy w tym miejscu zastrzec, że powyższa okoliczność nie skutkuje odliczeniem dni, w których urząd nie pracował, od terminu do załatwienia sprawy. Powyższa okoliczność nie realizuje bowiem hipotezy art. 35 § 5 KPA, zgodnie z którym do terminów załatwienia sprawy nie wlicza się terminów przewidzianych w przepisach prawa dla dokonania określonych czynności,

2 *Ibidem*.

okresów zawieszenia postępowania oraz okresów opóźnień spowodowanych z winy strony albo z przyczyn niezależnych od organu. Wniesienie podania do systemu teleinformatycznego organu administracyjnego poza godzinami pracy urzędu nie stanowi w szczególności ostatniego z wyżej wymienionych przypadków umożliwiających wydłużenie terminu załatwienia sprawy, tj. nie stanowi przyczyny niezależnej od organu. Nieurzędowanie w określonych dniach tygodnia, z wyjątkiem dni wolnych ustawowo od pracy, pozostaje w kompetencji organizacyjnej organu administracyjnego. Przykładowo, zgodnie z art. 33 ust. 2 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U. z 2001 r. Nr 142, poz. 1591 ze zm.) organizację i zasady funkcjonowania urzędu gminy określa regulamin organizacyjny, nadany przez wójta, w drodze zarządzenia. Za równie dyskusyjną należy uznać możliwość niewliczania do terminu załatwienia sprawy dni wolnych od pracy, tj.; dni wskazanych w treści Ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 1951 r. Nr 4, poz. 28 ze zm.). O ile bowiem niewykonywanie pracy jest w tym przypadku regulowane ustawowo, o tyle możliwość odliczenia tych dni od terminu do załatwienia sprawy wydaje się stać w sprzeczności względem regulacji art. 57 § 4 KPA Przepis ten reguluje znaczenie dni wolnych dla biegu terminu jedynie w ten sposób, że jeżeli koniec terminu przypada na dzień ustawowo wolny od pracy, za ostatni dzień terminu uważa się najbliższy następny dzień powszedni. Wnioskując a contrario, do terminu wlicza się dni wolne od pracy występujące w toku biegu tego terminu. Konkludując, dni, w których organ nie pracował, należy wliczyć do terminu załatwienia sprawy. Tym samym żądanie wniesione w formie dokumentu elektronicznego nie tylko skutecznie wszczyna postępowanie administracyjne w dacie wprowadzenia żądania do systemu teleinformatycznego organu administracji publicznej, lecz jednocześnie w tym dniu skutecznie uruchamia bieg terminu do zakończenia postępowania.

Wniesienie podania

Zgodnie z art. 63 § 1 KPA podania (żądania, wyjaśnienia, odwołania, zażalenia) mogą być wnoszone pisemnie, telegraficznie, za pomocą telefaksu lub ustnie do protokołu, a także za pomocą innych środków komunikacji elektronicznej przez elektroniczną skrzynkę podawczą organu administracji publicznej utworzoną na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Regulacja ta odnosi się do podań rozumianych jako: żądania, wyjaśnienia, odwołania, zażalenia. Zakresem art. 63 § 1 należy dodatkowo objąć działania procesowe mające na celu zainicjowanie określonych działań organu w ramach postępowania administracyjnego, tj. realizujące funkcję żądania, których nazwa nie została literalnie ujęta w ramy art. 63 § 1. Są to, przykładowo, czynności, takie jak:

1) prośba (np. art. 58 § 1 KPA - prośba o przywrócenie terminu)
2) wystąpienia (art. 98 § 1 KPA - wystąpienie o zawieszenie postępowania, art. 105 § 2 KPA - wystąpienie o umorzenie postępowania),
3) zwrócenie się (art. 98 § 2 KPA - zwrócenie się o podjęcie zawieszonego postępowania,
4) wniosek (art. 127 § 3 KPA - wniosek o ponowne rozpatrzenie sprawy).

Przepis art. 63 § 1 KPA nie dotyczy natomiast skarg i wniosków. Zasady ich wnoszenia podlegają bowiem odrębnej regulacji, tj. Rozporządzeniu Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz.U. z 2002 r. Nr 5, poz. 46), wydanego na podstawie delegacji art. 226 KPA

Ustawa o informatyzacji, wraz przepisami wykonawczymi, przewiduje dwie podstawowe kategorie doręczenia dokumentu elektronicznego, tj.:

1) doręczenie za pomocą środków komunikacji elektronicznej, przy czym doręczenie to może nastąpić na adres elektronicznej skrzynki podawczej lub na adres poczty elektronicznej podmiotu publicznego,
2) doręczenie na informatycznym nosiku danych. Regulacja art. 14 KPA, stanowiąca zasadę ogólną postępowania administracyjnego, ogranicza zakres dopuszczalnych metod doręczenia dokumentu elektronicznego poprzez wskazanie, jako metody wyłącznie dopuszczalnej, doręczenia dokumentu elektronicznego za pomocą środków komunikacji elektronicznej.

Przepis art. 63 § 1 KPA wprowadza w tej mierze obostrzenie. Zgodnie z treścią art. 63 § 1 KPA podanie wnoszone w formie dokumentu elektronicznego powinno zostać wniesione za pomocą środków komunikacji elektronicznej przez elektroniczną skrzynkę podawczą. Powyższe ograniczenie sprawia, że podanie wniesione za pomocą środków komunikacji elektronicznych na adres elektroniczny inny niż adres elektronicznej skrzynki podawczej stanowi podanie niewniesione. Za podanie niewniesione należy zatem szczególnie uznać podanie wprowadzone na adres poczty elektronicznej organu administracyjnego. Jednocześnie należy zastrzec, że obowiązek wniesienia podania w formie dokumentu elektronicznego na adres elektronicznej skrzynki podawczej organu administracyjnego nie stanowi elementu formalnego podania jako czynności prawnej. Tym samym wniesienie podania w formie dokumentu elektronicznego na adres elektroniczny inny niż adres elektronicznej skrzynki podawczej organu administracyjnego nie może zostać poczytane za brak formalny podania, co oznacza brak podstaw prawnych do wezwania wnoszącego o uzupełnienie braku podania. Funkcjonowanie elektronicznej skrzynki podawczej zostało uregulowane w ramach aktu wykonawczego do Ustawy o informatyzacji, tj. w powoływanym niejednokrotnie Rozporządzeniu prezesa Rady Ministrów w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. Ponieważ zasady funkcjonowania elektronicznej skrzynki podawczej stanowią przedmiot odrębnej analizy, w tym miejscu należy jedynie odnotować, że adres elektronicznej skrzynki podawczej powinien zostać podany do informacji na stronach podmiotowych Biuletynu Informacji Publicznej. Elektroniczne skrzynki podawcze, których adresy zostały udostępnione na stronie Biuletynu, powinny zapewniać bezpośrednie doręczanie dokumentów w oparciu o formularze elektroniczne powiązane z tymi skrzynkami lub wzory dokumentów elektronicznych zamieszczonych w centralnym repozytorium wzorów prowadzonym przez ministra właściwego do spraw informatyzacji[3].

Określona w ramach art. 63 § 1 KPA możliwość wniesienia podania w formie dokumentu elektronicznego za pomocą środków komunikacji elektronicznej może także polegać na wniesieniu podania za pomocą telefaksu. Zgodnie z art. 2 pkt 5 Ustawy o świadczeniu usług drogą elektroniczną pojęcie środków komunikacji elektronicznej oznacza rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę

3 *M. Wierzbowski*; Kodeks … op. cit.

elektroniczną. Z kolei zgodnie z art. 2 pkt 3 powołanej ustawy, system teleinformatyczny oznacza zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu Ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 ze zm.).

Obecne rozwiązania techniczne pozwalają na wysłanie i odbiór faksu za pomocą systemu teleinformatycznego. Z treści art. 63 § 1 KPA wynika, że istnieje możliwość wniesienia podania za pomocą środków komunikacji elektronicznej, przez elektroniczną skrzynkę podawczą organu administracyjnego, czyni to w drodze wyrażenia: „a także za pomocą innych środków komunikacji elektronicznej przez elektroniczną skrzynkę podawczą organu administracji publicznej". Posłużenie się słowem „innych" wskazuje na uprzednie wymienienie środka komunikacji elektronicznej w ramach formułowanego katalogu sposobów wniesienia podania. Biorąc pod uwagę, że katalog ten obejmuje wniesienie podania: pisemnie, telegraficznie, za pomocą telefaksu lub ustnie do protokołu, za sposób podlegający kwalifikacji środka komunikacji elektronicznej należy uznać wniesienia podania za pomocą telefaksu. Wyodrębnienie kategorii telefaksu względem kategorii innych środków komunikacji elektronicznej znajduje uzasadnienie w dwojakiej możliwości jego funkcjonowania. Użycie telefaksu może, lecz nie musi, polegać na zapewnieniu indywidualnego porozumiewania się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi. Przesłanie faksu może jednak również polegać na transmisji danych w ramach systemu telekomunikacyjnego. Pojęcie systemu telekomunikacyjnego nie znajduje odzwierciedlenia w postaci ustawowej definicji. Tym niemniej w literaturze wskazuje się, że system telekomunikacyjny to „zespół współpracujących urządzeń, programów i procedur stosowany w celu przekazywania danych pomiędzy miejscami ich przetwarzania lub przechowywania na dowolną odległość".

Podanie wniesione w sposób określony w treści art. 63 § 1 KPA powinno mieć formę:
1) pisemną,
2) dokumentu elektronicznego lub
3) ustną.

Podanie takie powinno również zawierać co najmniej:
1) wskazanie osoby, od której pochodzi,
2) jej adres,
3) żądanie

a także czynić zadość innym wymaganiom ustalonym w przepisach szczególnych.

A zatem podanie w formie dokumentu elektronicznego powinno zawierać:
1) mechaniczne wskazanie (np. w postaci edytowanego tekstu) w treści podania danych identyfikujących wnoszącego podanie, tj. imię i nazwisko osoby fizycznej lub nazwę osoby prawnej,
2) żądanie, tj. oświadczenie woli o treści mającej znaczenie prawne oraz
3) adres wnoszącego, przy czym przez adres wskazany w treści podania należy uznać adres zamieszkania lub siedziby wnoszącego.

Zgodnie z art. 63 § 3a pkt 1 KPA podanie wniesione w formie dokumentu elektronicznego powinno zostać opatrzone:
1) bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu,
2) podpisem potwierdzonym profilem zaufanym ePUAP lub
3) podpisem osobistym. Ponadto podmiot publiczny, który używa do realizacji zadań publicznych systemów

teleinformatycznych, może umożliwiać użytkownikom identyfikację w tym systemie przez zastosowanie innych technologii, chyba że przepisy odrębne przewidują obowiązek dokonania czynności w siedzibie podmiotu publicznego.

Uwaga!

Brak realizacji któregokolwiek z wyżej wymienionych elementów stanowi brak formalny podania w rozumieniu art. 64 KPA. Zgodnie z treścią art. 64 KPA § 1. Jeżeli w podaniu nie wskazano adresu wnoszącego i nie ma możności ustalenia tego adresu na podstawie posiadanych danych, podanie pozostawia się bez rozpoznania. § 2. Jeżeli podanie nie czyni zadość innym wymaganiom ustalonym w przepisach prawa, należy wezwać wnoszącego do usunięcia braków w terminie siedmiu dni z pouczeniem, że nieusunięcie tych braków spowoduje pozostawienie podania bez rozpoznania.

Zgodnie z treścią art. 64 § 4 KPA w przypadku wniesienia podania w formie dokumentu elektronicznego organ jest obowiązany potwierdzić wniesienie podania przez doręczenie urzędowego poświadczenia odbioru na wskazany przez wnoszącego adres elektroniczny. Za udostępnienie potwierdzenia wniesienia podania uważa się w szczególności jego przekazanie do pozostającej w dyspozycji odbiorcy potwierdzenia skrytki w ramach systemu teleinformatycznego organu administracyjnego służącego do obsługi doręczeń. Jeżeli nie jest możliwe udostępnienie automatycznie wytworzonego potwierdzenia wniesienia podania w sposób powyższy, potwierdzenie to wysyłane jest na adres elektroniczny wskazany przez wnoszącego, z tym że może to być:

1) adres poczty elektronicznej albo
2) inny adres elektroniczny, pod warunkiem, że jest obsługiwany przez system teleinformatyczny służący do obsługi doręczeń.

Skarga do sądu administracyjnego

Zgodnie z art. 54 § 1 Ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (tekst jedn.: Dz.U. z 2012 r., poz. 270; dalej: PostSądAdmU) skargę do sądu administracyjnego wnosi się za pośrednictwem organu, którego działanie lub bezczynność są przedmiotem skargi. W świetle obowiązujących przepisów prawnych wniesienie do sądu administracyjnego skargi w formie dokumentu elektronicznego należy uznać za niedopuszczalne ze względu na brak podstawy prawnej. Przepisy PostSądAdmU regulujące wnoszenie pism procesowych nie odnoszą się do formy dokumentu elektronicznego, jak również nie posługują się pojęciem środków komunikacji elektronicznej.

Uwaga!

Z przepisów tych wynika, że nie ma możliwości wniesienia do sądu administracyjnego skargi w formie dokumentu elektronicznego.

Dostęp do akt sprawy

Zasady dostępności oraz zakres uprawnień przysługujących stronie w zakresie posługiwania się aktami sprawy zostały uregulowane w art. 73 § 1-2 KPA. Zgodnie z tymi przepisami, strona ma prawo wglądu w akta sprawy, sporządzania z nich notatek, kopii lub odpisów. Prawo to przysługuje również po zakończeniu postępowania. Powyższe czynności są dokonywane w lokalu organu administracji publicznej w obecności pracownika tego organu. Ponadto strona może żądać uwierzytelnienia odpisów lub kopii akt sprawy lub wydania jej z akt sprawy uwierzytelnionych odpisów, o ile jest to uzasadnione jej ważnym interesem.

Obowiązek zapewnienia stronie dostępu do akt w sposób zgodny z art. 73 § 1-2 KPA może zostać ograniczony wyłącznie

przepisem prawa, a tym samym prawo dostępu nie może ulec wyłączeniu lub zawężeniu ze względu na formę dokumentów znajdujących się w aktach sprawy. Szczególnie prawa tego nie wyłącza występowanie w aktach sprawy dokumentu elektronicznego. W takim przypadku organ powinien zapewnić stronie dostęp do akt sprawy poprzez sporządzenie w formie pisemnej uwierzytelnionych odpisów dokumentów elektronicznych. Strona ma bowiem prawo dostępu do dokumentacji oryginalnej lub w randze oryginału, co oznacza, że przedłożenie nie-uwierzytelnionych kopii dokumentów nie realizuje prawa strony.

Ustawodawca dopuszcza jednak alternatywny tryb realizacji prawa dostępu. Zgodnie z treścią art. 73 § 4 KPA w przypadku pism w formie dokumentu elektronicznego wnoszonych do organu administracji publicznej lub przez niego doręczanych organ może zapewnić stronie dostęp do nich w swoim systemie teleinformatycznym, po identyfikacji strony w sposób określony w przepisach Ustawy o informatyzacji. Organ administracji publicznej może zatem zapewnić dostęp do akt sprawy poprzez organizację stosownego stanowiska dostępu w siedzibie urzędu lub poprzez organizację funkcji dostępu sieciowego do akt dokumentacji elektronicznej znajdującej się w systemie teleinformatycznym urzędu. Dostęp ten powinien być warunkowany identyfikacją osoby za pomocą podstawowych mechanizmów uwierzytelnienia, o których mowa w Ustawie o informatyzacji, tj. za pomocą:

1) bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu,
2) podpisu potwierdzonego profilem zaufanym ePUAP lub
3) podpisu osobistego.

Zgodnie z art. 20a Ustawy o informatyzacji podmiot publiczny, który używa do realizacji zadań publicznych systemów teleinformatycznych, może też umożliwiać użytkownikom identyfikację w tym systemie przez zastosowanie innych technologii, chyba że przepisy odrębne przewidują obowiązek dokonania czynności w siedzibie podmiotu publicznego.

Zapewnienie przez organ administracji publicznej dostępu do akt sprawy w swoim systemie teleinformatycznym ma charakter fakultatywny oraz niewiążący. Przepis art. 73 § 3 KPA stanowi jedynie podstawę prawną dla tego rodzaju działań organizacyjnych, nie kształtując po stronie organu obowiązku ich realizacji. Z drugiej strony zapewnienie przez organ administracji publicznej dostępu do akt sprawy w swoim systemie teleinformatycznym nie wiąże strony.

A zatem nawet w przypadku, gdy organ administracji publicznej zapewni dostęp do akt sprawy w swoim systemie teleinformatycznym, strona ma prawo skutecznie żądać wglądu do akt sprawy na zasadzie wglądu do akt w formie pisemnej. Jednocześnie w sytuacji, w której strona żąda dostępu do akt sprawy w systemie teleinformatycznym organu, zaś organ administracji zapewnia dostęp do akt sprawy wyłącznie na zasadzie wglądu do akt w formie pisemnej, nie można mówić o odmowie dostępu do akt sprawy. Organ administracyjny nie będzie zatem zobowiązany do wydania na podstawie art. 74 § 2 KPA postanowienia o odmowie dostępu do akt sprawy.

Uwaga!

Zapewnienie przez organ administracyjny efektywnych rozwiązań organizacyjnych ma charakter wyłącznie techniczny i nie podlega zaskarżeniu.

Wydanie i doręczenie decyzji administracyjnej

Forma decyzji administracyjnej stanowi kwalifikowaną formę czynności prawnej, tj. formę konwencjonalną. Celem skutecznego wydania decyzji organ administracyjny jest zobowiązany dokonać wyrażenia jej treści w ramach jednej z podstawowych form czynności, o których mowa w treści art. 14 KPA, tj.:

1) w formie pisemnej,
2) w formie dokumentu elektronicznego lub
3) w formie ustnej.

Wydanie decyzji postaje jednocześnie kwalifikowane sumą elementów formalnoprawnych odnoszących się od jej treści oraz konstrukcji. Katalog tych elementów kształtuje art. 107 § 1 KPA. W zakresie elementów konstrukcyjnych decyzja powinna zawierać:

1) oznaczenie organu administracji publicznej,
2) datę wydania,
3) oznaczenie strony lub stron,
4) powołanie podstawy prawnej,
5) rozstrzygnięcie,
6) uzasadnienie faktyczne i prawne,
7) pouczenie, czy i w jakim trybie służy od niej odwołanie,
8) jeżeli w stosunku do decyzji może być wniesione powództwo do sądu powszechnego lub skarga do sądu administracyjnego, powinna zawierać ponadto pouczenie o dopuszczalności wniesienia powództwa lub skargi.

Jeżeli treść decyzji została wyrażona w formie pisemnej, decyzja powinna zostać opatrzona podpisem własnoręcznym. Jeżeli treść decyzji została natomiast wyrażona w formie dokumentu elektronicznego, powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym. Określony w treści art. 107 § 1 KPA katalog mechanizmów uwierzytelnienia decyzji wydanej w formie dokumentu elektronicznego stanowi katalog zamknięty i odrębny względem regulacji Ustawy o informatyzacji. Tym samym za niedopuszczalne należy uznać opatrzenie decyzji podpisem potwierdzonym profilem zaufanym ePUAP Jednocześnie należy podkreślić zasadniczą różnicę w zakresie funkcjonalności podpisu elektronicznego względem podpisu osobistego. Zgodnie z treścią art. 20 ust. 2 Ustawy o podpisie elektronicznym certyfikat służący do weryfikacji podpisu elektronicznego, oprócz danych identyfikujących osobę fizyczną składającą podpis, może zawierać również informację czy osoba składająca podpis działa jako organ władzy publicznej. Tymczasem treść adekwatnych regulacji Ustawy o dowodach osobistych, tj. art. 19 ustawy, nie przewiduje możliwości zawarcia podobnych danych w treści certyfikatu podpisu osobistego. Powyższy brak czyni podpis osobisty narzędziem o mniejszym zakresie funkcjonalności niż podpis elektroniczny. W przypadku opatrzenia decyzji podpisem osobistym za jedyną uwierzytelnioną informację należy uznać identyfikację tożsamości osoby składającej podpis. Wszelkie inne informacje, takie jak pełniona funkcja lub upoważnienie do wydania decyzji, z konieczności zostają wyrażone wyłącznie w ramach edytowanej treści decyzji. Tymczasem opatrzenie decyzji za pomocą bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu może skutkować wierzytelną identyfikacją tożsamości osoby jak również wierzytelnym ustaleniem realizowanej funkcji, a co za tym idzie, oznaczeniem organu administracyjnego. Jednocześnie należy zastrzec, że pomimo mniejszego zakresu funkcjonalności, posłużenie się podpisem osobistym jest w pełni skuteczne.

W świetle obowiązujących przepisów prawa, w tym art. 107 KPA oraz szczególnie Rozporządzenia prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt

oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U z 2011 r. Nr 14, poz. 67), celem oznaczenia organu administracyjnego nie jest konieczne oznaczenie go w sposób wierzytelny, tj. np. poprzez posłużenie się pieczęcią, o której mowa w treści art. 16c ust. 2 Ustawy z dnia 31 stycznia 1980 r. o godle, barwach i hymnie Rzeczypospolitej Polskiej oraz o pieczęciach państwowych (Dz.U. z 1980 r. Nr 7, poz. 18 ze zm.). Biorąc powyższe pod uwagę, oznaczenie organu administracyjnego na zasadzie edytorskiej w ramach treści decyzji, należy uznać za realizujące wymagania art. 107 KPA

Opatrzenie decyzji wydanej w formie dokumentu elektronicznego w sposób inny aniżeli określony w art. 107 § 1 KPA, należy uznać za brak złożenia podpisu, tj. brak realizacji wymogu personalizacji treści decyzji. Brak opatrzenia decyzji bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub podpisem osobistym oznacza nie-wydawanie decyzji administracyjnej.

Z orzecznictwa…

Pisma zawierające rozstrzygnięcia w sprawie załatwianej w drodze decyzji są decyzjami, pomimo nie posiadania w pełni formy przewidzianej w art. 107 par. 1 KPA, jeśli tylko zawierają minimum elementów niezbędnych do zakwalifikowania ich jako decyzji. Do takich elementów należy zaliczyć: oznaczenie organu administracji państwowej wydającego akt, wskazanie adresata aktu, rozstrzygnięcie o istocie sprawy oraz podpis osoby reprezentującej organ administracji.

Wyrok Naczelnego Sądu Administracyjnego z dnia 20 lipca 1981 r„ sygn.: SA 1163/81

Brak któregokolwiek z powyższych elementów powoduje, że wydane pismo nie stanowi decyzji administracyjnej, zaś postępowanie administracyjne nie może zostać uznane za zakończone.

Przepis art. 107 § 1 KPA reguluje wyłącznie zasady sporządzenia decyzji administracyjnej. Tymczasem celem wywołania skutku prawnego decyzja administracyjna powinna zostać doręczona stronie postępowania. Zasady doręczania decyzji administracyjnej podlegają odrębnej regulacji art. 109 § 1 KPA Przepis art. 109 § 1 KPA przesądza w sposób ostateczny o możliwości zakończenia postępowania administracyjnego decyzją w formie dokumentu elektronicznego. Zgodnie z jego treścią decyzję doręcza się stronom na piśmie lub za pomocą środków komunikacji elektronicznej.

Wydanie i doręczenie postanowienia administracyjnego

Odnośnie formy wydania oraz metody doręczenia postanowienia administracyjnego stosuje się te same zasady, co w przypadku wydania i doręczenia decyzji administracyjnej. Celem skutecznego wydania postanowienia organ administracyjny jest zobowiązany dokonać wyrażenia jej treści w ramach jednej z podstawowych form czynności, o których mowa w treści art. 14 KPA, tj.: formy pisemnej, formy dokumentu elektronicznego lub formy ustnej.

Postanowienie powinno zawierać:
1) oznaczenie organu administracji publicznej,
2) datę wydania,
3) oznaczenie strony lub stron albo innych osób biorących udział w postępowaniu,
4) powołanie podstawy prawnej,
5) rozstrzygnięcie,
6) uzasadnienie faktyczne i prawne,
7) pouczenie, czy i w jakim trybie służy na nie zażalenie lub skarga do sądu administracyjnego, oraz podpis z podaniem imienia i nazwiska oraz stanowiska.

Ponadto, zgodnie z art. 124 § 2 oraz art. 125 § 3 KPA, jeżeli na postanowienie służy zażalenie lub skarga do sądu administracyjnego albo gdy wydane zostało na skutek zażalenia na postanowienie, postanowienie to powinno zawierać uzasadnienie faktyczne i prawne oraz stosowne pouczenie. Celem wydania postanowienia jego treść powinna ulec personalizacji. Jeżeli treść postanowienia została wyrażona w formie pisemnej, postanowienie powinno zostać opatrzone podpisem własnoręcznym. Jeżeli treść postanowienia została natomiast wyrażona w formie dokumentu elektronicznego, powinno zostać opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym. Określony w treści art. 124 § 1 KPA katalog mechanizmów uwierzytelnienia postanowienia wydanego w formie dokumentu elektronicznego stanowi katalog zamknięty i odrębny względem regulacji Ustawy o informatyzacji. Tym samym za niedopuszczalne należy uznać opatrzenie postanowienia podpisem potwierdzonym profilem zaufanym ePUAP.

Zasady doręczania postanowienia administracyjnego podlegają odrębnej regulacji, tj. art. 125 § 1 KPA Zgodnie z jego treścią postanowienia, od których służy stronom zażalenie lub skarga do sądu administracyjnego, doręcza się stronom na piśmie lub za pomocą środków komunikacji elektronicznej. Obowiązek doręczenia postanowień obejmuje postanowienia adresowane jedynie do stron, które jednocześnie podlegają zażaleniu lub skardze do sądu administracyjnego. Ograniczenie o charakterze podmiotowym, tj. wyłączające obowiązek doręczenia postanowień adresowanych do innych niż strona uczestników postępowania, należy uznać za bezzasadne i bezskuteczne. Każdy adresat postanowienia, na które służy zażalenie lub skarga do sądu administracyjnego, powinien zostać powiadomiony zarówno o treści, jak i o środku prawnym zaskarżenia postanowienia oraz o trybie jego wniesienia. Za rozstrzygający w tej mierze należy szczególnie uznać art. 53 § 1 PostSądAdmU, zgodnie z którym skargę wnosi się w terminie trzydziestu dni od dnia doręczenia skarżącemu rozstrzygnięcia w sprawie, tj. od dnia doręczenia decyzji administracyjnej oraz postanowień wydanych w administracyjnym postępowaniu jurysdykcyjnym, egzekucyjnym i zabezpieczającym. Za wyłącznie wiążące należy zatem uznać ograniczenie obowiązku doręczania postanowień mające charter przedmiotowy. Obowiązek doręczania postanowień zostaje wyłączony względem postanowień niezaskarżalnych, tj. postanowień, od których nie służy zażalenie lub skarga do sądu administracyjnego. Wyłączenie obowiązku doręczenia nie oznacza jednak wyłączenia możliwości doręczenia. Należy zatem zastrzec, że w przypadku doręczenia przez organ administracji publicznej postanowienia niezaskarżalnego, doręczenie takie pozostaje poza dyspozycją art. 125 KPA W konsekwencji doręczenie postanowienia niezaskarżalnego nie jest determinowane dedykowaną regułą art. 125 § 1 KPA, lecz podlega ogólnej zasadzie art. 14 KPA, co oznacza możliwość doręczenia postanowienia niezaskarżalnego zarówno w formie pisemnej, jak i w formie dokumentu elektronicznego doręczanego za pomocą środków komunikacji elektronicznej. Doręczenie postanowienie za pomocą środków komunikacji elektronicznej pozostaje oczywiście warunkowane wolą strony lub innego uczestnika postępowania, wyrażoną na podstawie art. 39^{1} § 1 KPA[4].

Orzeczenie blankietowe

Konstrukcja orzeczenia blankietowego stanowi jedną z najnowszych konstrukcji postępowania administracyjnego. Istota orzeczenia blankietowego oraz podstawa prawna jego wydania

4 *M. Jachowicz, M. Kotulski*; Forma … op. cit.,

zostały unormowane w ramach art. 138 § 4 KPA, w rozdziale 10 działu II Kodeksu postępowania administracyjnego, tj. regulującym tematykę odwołania od decyzji administracyjnej. Ze względu jednak na treść art. 144 KPA, zgodnie z którym w sprawach nieuregulowanych w rozdziale dotyczącym zażaleń, do zażaleń mają zastosowanie odpowiednie przepisy dotyczące odwołań, regulacja art. 138 § 4 KPA powinna znaleźć zastosowanie również w przypadku weryfikacji postanowień administracyjnych.

Zgodnie z treścią art. 138 § 4 KPA, jeżeli przepisy przewidują wydanie decyzji na blankiecie urzędowym, w tym za pomocą środków komunikacji elektronicznej, a istnieją podstawy do zmiany zaskarżonej decyzji, organ odwoławczy uchyla decyzję i zobowiązuje organ pierwszej instancji do wydania decyzji o określonej treści.

Zastosowanie konstrukcji orzeczenia blankietowego oznacza, że organ odwoławczy, dostrzegając konieczność zmiany zaskarżonej decyzji orzeka o uchyleniu zaskarżonej decyzji w całości lub części i jednocześnie zobowiązuje organ pierwszej instancji do wydania decyzji o treści ustalonej w ramach decyzji odwoławczej. Należy uznać, że decyzja odwoławcza powinna wiążąco określać nie tylko rozstrzygnięcie przyszłej decyzji organu pierwszej instancji, lecz również treść uzasadnienia. Realizując nałożone zobowiązanie, organ pierwszej instancji nie ma prawa do merytorycznej ingerencji w treść formułowanej decyzji. Kompetencja organu pierwszej instancji zostaje w tym przypadku ograniczona do czynności formalnego wydania własnej decyzji, tj. decyzji wydanej w pierwszej instancji, z wyłączeniem możliwości władczego kreowania treści tej decyzji.

Wydanie zaświadczenia

Postępowanie w sprawie wydania zaświadczenia ma charakter uproszczony. Zgodnie z art. 219 KPA odmowa wydania zaświadczenia bądź zaświadczenia o treści żądanej przez osobę ubiegającą się o nie następuje w drodze postanowienia, na które służy zażalenie. Do postępowania w sprawie wydawania zaświadczeń stosuje się zasadę ogólną art. 14 § 1 KPA, zgodnie, z którą sprawy należy załatwiać w formie pisemnej lub w formie dokumentu elektronicznego w rozumieniu doręczanego środkami komunikacji elektronicznej.

Zgodnie z art. 217 § 4 KPA zaświadczenie wydaje się w formie dokumentu elektronicznego, opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym, jeżeli zażąda tego osoba ubiegająca się o zaświadczenie. Przepis art. 217 § 4 KPA zawiera zatem dwojakiego rodzaju regulacje. Po pierwsze, potwierdza dopuszczalność wydania zaświadczenia w formie dokumentu elektronicznego. Po drugie, uzależnia zastosowanie formy dokumentu elektronicznego od żądania osoby ubiegającej się o wydanie zaświadczenia. A zatem wyrażenie żądania wydania zaświadczenia w formie dokumentu elektronicznego stanowi samoistną podstawę do wydania zaświadczenia w tej formie i doręczenia go za pomocą środków komunikacji elektronicznej.

Problematyka zastosowania dokumentu elektronicznego w postępowaniu w sprawie wydania zaświadczenia znajduje ponadto wyraz w treści art. 220 § 1 KPA, odnoszącego się do rejestrów publicznych prowadzonych na podstawie Ustawy o informatyzacji oraz do wymiany informacji na zasadach określonych w tej ustawie Zgodnie z treścią art. 220 § 1 organ administracji publicznej nie może żądać zaświadczenia ani oświadczenia na potwierdzenie faktów lub stanu prawnego, jeżeli:

1) znane są one organowi z urzędu,
2) możliwe są do ustalenia przez organ na podstawie:
   a) posiadanych przez niego ewidencji, rejestrów lub innych danych,
   b) rejestrów publicznych posiadanych przez inne podmioty publiczne, do których organ ma dostęp w drodze elektronicznej na zasadach określonych w przepisach

Ustawy o informatyzacji,

c) wymiany informacji z innym podmiotem publicznym na zasadach określonych w przepisach o informatyzacji działalności podmiotów realizujących zadania publiczne,
d) przedstawionych przez zainteresowanego do wglądu dokumentów urzędowych (dowodu osobistego, dowodów rejestracyjnych i innych).

Przyjmowanie i rozpatrywanie skarg i wniosków

Problematyka formy dokumentu elektronicznego w zakresie przyjmowania oraz rozpatrywania skarg i wniosków została uregulowana w Rozporządzeniu Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków. Przepisem dopuszczającym możliwość zastosowania środków komunikacji elektronicznej jest przepis § 5, zgodnie z którym skargi i wnioski mogą być wnoszone pisemnie, telegraficznie lub za pomocą dalekopisu, telefaksu, poczty elektronicznej, a także ustnie do protokołu.

Przepis § 5 rozporządzenia dopuszcza złożenie skargi lub wniosku w formie dokumentu elektronicznego jedynie na adres poczty elektronicznej organu administracyjnego lub za pomocą telefaksu. Przepis ten ma charakter obowiązujący. Tym samym skarga lub wniosek złożone w sposób odmienny od ustalonego w regulacji § 5 może stanowić skargę lub wniosek wniesione nieskutecznie.

Funkcja skargi i wniosku powoduje, że ani wniosek, ani skarga nie wymagają dla swojej skuteczności złożenia podpisu. Powyższa reguła wynika z treści § 8 ust. 1 rozporządzenia, zgodnie z którym skargi i wnioski niezawierające imienia i nazwiska (nazwy) oraz adresu wnoszącego pozostawia się bez rozpoznania. Z kolei § 8 ust. 2 wskazuje, że jeżeli z treści skargi lub wniosku nie można należycie ustalić ich przedmiotu, wzywa się wnoszącego skargę lub wniosek do złożenia, w terminie siedmiu dni od dnia otrzymania wezwania, wyjaśnienia lub uzupełnienia, z pouczeniem, że nieusunięcie tych braków spowoduje pozostawienie skargi lub wniosku bez rozpoznania.

Uwaga!

Brak podpisu nie skutkuje pozostawieniem skargi lub wniosku bez rozpoznania.

Specyfika postępowania ze skargi lub wniosku sprawia, że postępowanie to nie ma charakteru postępowania prowadzonego w indywidualnej sprawie administracyjnej, zaś skarżącemu lub wnioskodawcy nie przysługuje status strony. O załatwieniu skargi lub wniosku osoba ta jest wyłącznie zawiadamiana. Zgodnie z art. 238 § 1 KPA zawiadomienie o sposobie załatwienia skargi powinno zawierać:

1) oznaczenie organu, od którego pochodzi,
2) wskazanie, w jaki sposób skarga została załatwiona oraz
3) podpis z podaniem imienia, nazwiska i stanowiska służbowego osoby upoważnionej do załatwienia skargi lub, jeżeli zawiadomienie sporządzone zostało w formie dokumentu elektronicznego, powinno być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem osobistym.

Ponadto zawiadomienie o odmownym załatwieniu skargi powinno zawierać uzasadnienie faktyczne i prawne oraz pouczenie o treści art. 239 KPA. Zawiadomienie o załatwieniu skargi lub wniosku może zatem mieć formę dokumentu elektronicznego.

Katarzyna Czajkowska-Matosiuk - doktorantka na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, autorka kilkudziesięciu artykułów i podręczników prawniczych.

Elektroniczne usługi administracji

dr Dorota Fleszer

Rozwój nowoczesnych technologii komunikacyjnych i informacyjnych staje się główną przyczyną zmian nie tylko w stosunkach międzyludzkich, ale także w życiu społecznym i gospodarczym. Coraz większe znaczenie przypisuje się komunikacji elektronicznej i - co się z tym wiąże - możliwości jakie daje korzystanie z Internetu. W konsekwencji z jednej strony od osoby chcącej aktywne funkcjonować w sferze zawodowej i społecznej wymaga się umiejętności związanych z korzystaniem z narzędzi informatycznych, z drugiej zaś ona sama wysoko ceni możliwość załatwiania swoich spraw przez Internet. Przedstawiona zależność stawia przed administracją publiczną wyzwanie. Niezbędne bowiem staje się uwzględnienie w stosowanych procedurach i metodach działania możliwości wykorzystywania nowych technologii i narzędzi informatycznych. Ma to istotne znaczenie nie tylko dla podniesienia sprawności działania administracji publicznej, jakości świadczonych przez nią usług, ale także ma ogromny wkład w rozwój społeczeństwa informacyjnego.

Przedmiotem niniejszej publikacji jest analiza problematyki wykorzystania środków komunikacji elektronicznej w realizacji zadań publicznych. Nie dokonuję analizy zasad, którymi należy się kierować przy ustalaniu rodzaju zadań publicznych podlegających elektronicznej realizacji. Pomijam również kwestie związane z organizacją świadczenia elektronicznych usług publicznych przez adminisrację, a także zagadnienie wymogów jakie stawiane są programom informatycznym za pomocą których realizowane są zadania publiczne.

E-usługa

W potocznym rozumieniu termin e-usługi utożsamiany jest z elektronicznym świadczeniem usług dostępnych *on-line* 24/7 (dwadzieścia cztery godziny na dobę, siedem dni w tygodniu). Jeżeli usługi świadczone są z pominięciem kontaktu osobowego, to mówimy o usługach sieciowych (*web services*)[1].

Ustawodawca w art. 2 pkt. 4 ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[2] - dalej u.ś.u.d.e. wyznaczając zakres pojęcia usługi świadczonej drogą elektroniczną kładzie jednak szczególny nacisk na inne elementy niż brak ograniczeń czasowych ich realizacji. Otóż według definicji legalnej zawartej w cyt. przepisie mianem usługi świadczonej drogą elektroniczną określa się wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową i przechowywania danych, która jest w całości nadawana, odbierana lub

1 M. Sakowicz, *Zastosowanie nowych technologii informacyjno-komunikacyjnych w rządzeniu i zarządzaniu administracja publiczną* (w :) red. J. Osiński, *Administracja publiczna na progu XXI wieku. Wyzwania i oczekiwania,* Szkoła Główna Handlowa w Warszawie. Warszawa 2008 r., s. 79

2 Dz.U. Nr 144 poz.1204 z 2002 r. z późn. zm.

transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.

Zatem do uznania - co szczególnie podkreśla P. Litwiński - że mamy do czynienia z e-usługą konieczne jest łączne spełnienie następujących przesłanek:

- wykonanie usługi powinno nastąpić bez jednoczesnej obecności stron,
- wykonanie usługi powinno nastąpić przez wysłanie i odbieranie danych za pomocą systemów teleinformatycznych,
- usługa powinna być świadczona na indywidualne żądanie stron, nadawanie, odbieranie i transmitowanie danych w ramach usługi świadczonej drogą elektroniczną powinno nastąpić za pośrednictwem sieci telekomunikacyjnych w rozumieniu ustawy - Prawo telekomunikacyjne[3].

Natomiast według M. Świerczyńskiego w pojęciu usług świadczonych drogą elektroniczną mieści się szereg działań prowadzonych on-line (na przykład usługa wyszukiwania różnego rodzaju treści w Internecie, przesyłania i przechowywania danych, oferowania informacji handlowych, zawieranie umów on-line). Wymóg braku jednoczesnej obecności obu stron oznacza, iż usługa pierwotnie jest wysyłana oraz odbierana za pomocą urządzeń elektronicznych przeznaczonych do przechowywania lub przetwarzania przekazywanych danych. Nie ma wtedy potrzeby fizycznej obecności usługodawcy i usługobiorcy w jedynym miejscu. W pewnych sytuacjach możemy mieć do czynienia z usługą świadczoną na odległość również w sytuacji, gdy strony znajdują się (fizycznie) w jednym miejscu - chodzi na przykład o dokonanie rezerwacji samochodu przy użyciu telefonu komórkowego łączącego się z witryną internetową sklepu, w którym się znajdują[4]. Podziela ten pogląd K. Korus. Autor twierdzi, że przepisy u.ś.u.d.e. stosuje się do wykonywania świadczeń *on-line*, czyli za pomocą sieci telekomunikacyjnych; stosuje się do usług wykonywanych bez jednoczesnej obecności stron, lecz na indywidualne żądanie odbiorcy, czyli usługa *point-to-point,* a nie usługa dla wszystkich odbiorców, tzw. *point-to-multipoint* (np. telewizja, radio). Nie ma również znaczenia, czy usługa jest odpłatna[5]. Uwzględniając powyższe stanowiska uzasadnione będzie przyjęcie za uzasadnioną tezę sformułowaną przez E. Modzelewską. Według niej e-usługa tworzy sieć wzajemnych oddziaływań zachodzących w przestrzeni cyfrowej między usługodawcą i usługobiorcą. Istotą *sevice design* jest dotarcie do największej liczby usługobiorców, dostosowując proces projektowania usługi (m.in. interfejsu) do indywidualnych potrzeb obywatela. Jest to możliwe, gdyż dana usługa zawiera bogatą, kompletną, harmonijną bazę danych zawierająca wszystko, co jednostkę może zainteresować w określonym temacie. Ponadto w nowoczesnym ujęciu metodycznym projektowanie e-usług jest realnym wpływaniem na pozytywne emocje naszych użytkowników poprzez odpowiednio dobrane narzędzia i techniki[6]. Dodatkowo Autorka stoi na stanowisku, że niezbędne jest zidentyfikowanie trzech głównych imperatywów, które ułatwiają „myślenie o e-usłudze". Pierwszy imperatyw to traktowanie ludzi

3 P. Litwiński, *Świadczenie usług drogą elektroniczną* (w:) red. P. Podrecki, Prawo Internetu, , Warszawa 2007.s. 173

4 M. Świerczyński, *Komentarz do art. 2 ustawy o świadczeniu usług drogą elektroniczną*, LEX,

5 K. Korus, *Umowy i inne czynności prawne w obrocie elektronicznym* (w:) M. Chudzik, A. Frań, A. Grzywacz, K. Korus, M. Spyra, *Prawo handlu elektronicznego*, Bydgoszcz–Kraków 2005, s. 97 i n.

6 E. Modzelewska, *Światowe trendy w projektowaniu e-usług dla administracji publicznej*, „Czas Informacji. Prawo Nowych Technologii. Informacja w administracji i gospodarce" Nr 1 z 2012 r. s. 83-84

jako zasadniczego elementu usług. Coraz częściej zdarza się, że sam usługobiorca staje się podwykonawcą usługi (*co-operation*), częścią multidyscyplinarnego zespołu, dlatego niezbędne jest zaprojektowanie jego udziału w tym procesie. Drugi imperatyw definiowany jest jako tworzenie sieci umożliwiających świadczenie usług. Obecnie możliwości w rozwoju systemów technologii informacyjno-komunikacyjnych pozwalają wykorzystać sieci społeczne we wszystkich sektorach, również w sektorze publicznym. Trzeci imperatyw charakteryzuje się zrównoważonym rozwojem jako jednym z aspektów ostatecznego wyniku. Istotne jest patrzenie w kategoriach długofalowego procesu, gdyż usługi są działaniami o charakterze ciągłym i bieżącym. Kluczowe jest badanie ekosystemu usług na płaszczyźnie ekonomicznej, społecznej oraz środowiskowej[7].

Świadczenie e-usług wyzwaniem dla administracji publicznej

Nie podlega dyskusji fakt, że rewolucja cyfrowa, która ma obecnie miejsce, rosnąca europejska i światowa konkurencja powoduje, że usługi administracji elektronicznej zaczynają odgrywać coraz istotniejszą rolę, zarówno dla państwa, jak i społeczeństwa[8]. W konsekwencji „współczesna (w znaczeniu nowoczesna) administracja i biurokracja podlega wielu nowym i nieznanym dotąd procesom, a w tym:

- automatyzacji – w związku z zastępowaniem tradycyjnych czynności manualnych pracą maszyn i urządzeń biurowych, zwłaszcza obliczeniowych i komunikacyjnych,
- komputeryzacji – w związku z wyposażaniem biur i poszczególnych stanowisk pracy w urządzenia komputerowe i współpracujące z nimi urządzenia peryferyjne,
- informatyzacji – w związku z wdrażaniem do urzędów dedykowanych aplikacji realizujących ustalone procedury, tworzonych pod kątem ich specyfiki i dostosowanych do szczegółowych wymogów działania,
- elektronizacji - w związku z zastępowaniem tradycyjnych dokumentów papierowych dokumentami elektronicznymi oraz tradycyjnej drogi wymiany dokumentów – drogą elektroniczną,
- internalizacji – w związku upowszechnianiem się łączności sieciowej, a zwłaszcza internetowej, do przekazywania informacji i wymiany dokumentów – drogą elektroniczną,
- integracji – w związku z wdrażaniem zintegrowanych systemów informatycznych obejmujących całokształt załatwianych w urzędzie i dokonywanych w nim czynności,
- standaryzacji- w związku z coraz większym opracowywaniem i stosowaniem jednolitych procedur, wzorów formularzy załatwiania poszczególnych spraw,
- upublicznieniu – w związku z szerokim udostępnieniem informacji dotyczących realizacji zadań publicznych, które nie podlegają ochronie prawnej w zakresie ich poufności,
- monitorowaniu – w związku z manualnym lub automatycznym odnotowywaniem coraz większej liczby czynności urzędowych w systemach informatycznych urzędu,
- specjalizacji – w związku z przyznawaniem poszczególnym urzędnikom ściśle określonego zakresu obowiązków i odpowiadającym im uprawnień w systemach informatycznych urzędów,
- polaryzacji- w związku z tendencją do likwidacji informatycznych struktur pośrednich na rzecz wzmocnienia szczebli centralnych i lokalnych, powiązanych ze sobą teleinformatycznie,

7 E. Modzelewska, *Światowe trendy w projektowaniu e-usług*…, op. cit. s. 81

8 A. Budziewicz- Guźlecka, *Rozwój usług e-government w Polsce*, http://web.ae.katowice.pl/stanley/konferencja/pdf/Budziewicz-Guzlecka.pdf, data pobrania 31.07.2012 r.s.4

- podrożeniu – w związku z koniecznością finansowania droższych urządzeń i aplikacji oraz ponoszenia rosnących wydatków ma eksploatowanie i serwisowanie,
- dynamizacji – w związku z wykonywaniem coraz większej liczby czynności w tym samym lub coraz krótszym czasie, za pomoc na nowo dostosowywanych do tego celu struktur,
- ekspansji – w związku z ciągłym poszerzaniem zakresu elektronicznie gromadzonych informacji, a tym samym ze zwiększeniem zainteresowania obywatelem, jego sprawami i działaniami[9].

Jednocześnie, jak słusznie zauważa A. Jaxy-Dębicka, nowoczesne technologie tworzą nowe kanały pozyskiwania bardziej precyzyjnych informacji, zaś dzięki zastosowaniu nowoczesnych systemów przetwarzania i analizy danych poszerzają dotychczasowe możliwości wykorzystania informacji. Pozwalają one również na znaczące poprawienie wydajności praktyk administracyjnych poprzez zminimalizowanie czasu oczekiwania na usługę, elastyczniejsze godziny dostępu oraz skrócenie czasu oczekiwania na odpowiedź. Wprowadzanie tych technologii pociąga za sobą duże wydatki, jednak doświadczenia zarówno sektora publicznego, jak i prywatnego pokazują, że stosunkowo szybko uzyskuje się znaczną obniżkę kosztów ponoszonych przez organizacje na codzienną działalność[10]. Zgodzić się także należy z I. Adamską, że dynamiczny rozwój technologiczny, którego jesteśmy świadkami na przestrzeni ostatnich lat, spowodował znaczny wzrost nakładów finansowych na rozwój technologii informacyjnych. Dzięki zastosowaniu narzędzi informatycznych możliwie jest szybkie i skuteczne wykonywanie zadań z różnych dziedzin[11]. Zresztą - jak słusznie zauważa A. Monarcha-Matlak - obywatele i przedsiębiorcy przyzwyczaili się już do korzystania z komercyjnych produktów *on-line* i oczekują od swoich rządów i administracji ofert usług o wysokiej jakości i użyteczności. W miarę jak ujawniają się nowe możliwości technologiczne, zwiększa się liczba wyzwań na przyszłość, łatwy dostęp do kompleksowego łatwego w obsłudze zestawu usług *e-gov* jest marzeniem obywateli, przedsiębiorców i urzędników[12]. Uwzględniając powyższe z perspektywy administracji publicznej zasadne jest zastosowanie technologii informacyjno-komunikacyjnych dla usprawnienia i podniesienia jakości działań na rzecz dobra publicznego w celu realizacji legitymizujących się poparciem społecznym zadań państwa. W sektorze publicznym wykorzystanie nowoczesnych technologii informacyjnych i komunikacyjnych stało się kluczowym czynnikiem modernizacji administracji publicznej oraz przeobrażeń społecznych. We współczesnym świecie administracja w zasadzie nie ma wyboru[13]. W praktyce oznacza to przejście od administracji procedur do administracji rezultatów, głoszącej postulat koncentracji działań wokół potrzeb i oczekiwań obywatela – klienta[14].

Jednak warto podkreślić, że informatyzacja administracji publicznej jest procesem złożonym. Nie można jej sprowadzać tylko do zmiany narzędzia służącego do wykonywania zadań publicznych. Niezbędne jest

9 J. Janowski, *Administracja elektroniczna. Kształtowanie się informatycznego prawa administracyjnego i elektronicznego postępowania administracyjnego w Polsce,* Warszawa 2009 s. 29-30

10 A. Jaxa Dębicka, *Sprawne państwo,* Wydawnictwo Oficyna a Wolters Kluwer Warszawa 2008 r. s. 228

11 I. Adamska, *Problemy w projektach informatycznych realizowanych na potrzeby administracji publicznej*, „Czas Informacji" z 2011 Nr 2 s. 104

12 A. Monarcha-Matlak, *Obowiązki administracji* …, op. cit. s. 170

13A. Jaxa-Dębska, *Sprawne państwo..., op. cit.* s. 228

14 A. Jaxa-Dębska, *Sprawne państwo..., op. cit.* s. 229

przeprowadzenie szeregu działań mających na celu przygotowanie nie tylko urzędników do stosowania nowych form realizacji zadań, ale także stworzenie odpowiedniej infrastruktury informatycznej. „Od stopnia kultury informatycznej urzędników oraz od stopnia opanowania umiejętności związanych z obsługą urządzeń informatycznych może zależeć w przyszłości szybkość wdrażania nowych systemów, programów, a także efektywność codziennego ich stosowania w pracy urzędu[15]". Powszechnie zauważa się i często przypomina, że e-administracja wymaga: komputeryzacji stanowisk pracy, digilatalizacji dokumentów urzędowych, osieciowanych pomieszczeń biurowych, zintegrowania baz danych, algorytmizacji procedur administracyjnych, automatyzacji sterowania obiegiem dokumentów, udostępniania informacji w sieci, elektronicznej weryfikacji tożsamości urzędnika i petenta oraz funkcjonowania centrów dostępu do sieci[16]. W konsekwencji *e-government* obejmuje wykorzystanie technologii informacyjnych i komunikacyjnych w administracji publicznej w powiązaniu ze zmianami natury organizacyjnej i zdobywaniem nowych umiejętności w celu poprawienia jakości świadczonych usług publicznych, procesów demokratycznych praz polityki państwa[17]. Na inny aspekt tego zagadnienia zwraca uwagę W. Iszkowski. Autor twierdzi, że dla realizacji zadań publicznych w formie elektronicznej pierwszym celem informatyzowania administracji powinna być pełna dostępność usług elektronicznych dla urzędników obsługujących obywateli w urzędach. Dopiero w drugiej kolejności część z tych usług – tych najbardziej potrzebnych obywatelom – powinna być dostępna przez Internet[18]. Moim zdaniem, działania na rzecz rozwoju e-usług administracji nie powinny koncentrować się tylko na rozwiązywaniu problemów natury informatycznej. Są one oczywiście istotne i bez ich usunięcia dalszy rozwój szeroko rozumianej elektronicznej administracji jest niemożliwy. Najlepsze jednak nawet rozwiązania informatyczne znajdą pełnego i skutecznego stosowania, jeśli nie będą ich obsługiwały odpowiednio przeszkoleni i zmotywowani urzędnicy. Dlatego też szczególny nacisk należy położyć na włączenie w organizację realizacji e-usług pracowników merytorycznych, a zwłaszcza ich szkolenie i tym samym podnoszenie ich umiejetności.

Zgadzam się tezą sformułowaną przez K. Kłosowską, że do powstania w pełni zinformatyzowanej administracji niezbędne jest zintegrowanie tzw. *front office* z *back office*. *Front office* oznacza sferę zewnętrzną administracji (kontakt na linii urząd-obywatel), zaś *back office* to sfera wewnętrzna administracji (to sfera niedostępna dla administracji), gdzie dokonuje się przetwarzania dostarczanych informacji, tu też następuje wprowadzenie do systemu teleinformatycznego danego urzędu danych, które zostały dostarczone w tradycyjnej formie. Samo wdrażanie technik informatycznych w sferze wewnętrznej działalności administracji, stosowanie narzędzi informatycznych (oznaczających odpowiedni sprzęt jak i oprogramowanie) w wewnętrznych strukturach i procesach administracyjnych jest jedynie utworzeniem biurokracji wirtualnej[19]. Również E. Modzelewska twierdzi, że proces transformacji administracji w kierunku e-administracji nie sprowadza się wyłącznie do stworzenia

15 A. Monarcha-Matlak, *Obowiązki administracji* …, op. cit. s. 176
16 W. Cellary, *Zarządzanie informacją zamiast zarządzania dokumentami drogą do transformacji administracji,* „Elektroniczna Administracja" z 2007 r. Nr 5 s. 2
17 M. Sakowicz, *Zastosowanie nowych*
18 W. Iszkowski, *Jesteśmy już społeczeństwem informacyjnym*, „Czas Informacji" z 2010 Nr 1 s.51
19 K. Kłosowska, *Ewolucja czynności faktycznych administracji* …, op. cit. s. 167

serwisu internetowego, za pomocą którego świadczone są usługi. Niezbędne są wewnętrzne procesy administracyjne, które pozwolą wyodrębnić tzw. *front office*, będący quasi-działem obsługi klienta, przyjmujący zlecenia oraz *back office,* zajmujący się wewnętrznymi procesami administracyjnymi, który w sposób zautomatyzowany umożliwia prowadzanie do systemu danych[20]. Podziela te poglądy M. Sakowicz. Stoi on na stanowisku, zgodnie z którym e-urząd skupia się przede wszystkim na e-administracji oraz e--usługach. Obszary te najlepiej jest przedstawić za pomocą części składowych e-urzędu, tj. *front-office*, *back-office* oraz wyodrębnianego niekiedy dodatkowo *middle-office*. *Front-office* to część nowej infrastruktury urzędu odpowiedzialna za bezpośredni kontakt z obywatelem i przekazywanie (otrzymywanie) informacji, danych, dokumentów w relacjach z podmiotami zewnętrznymi. *Back-office* to część urzędu zajmująca się gromadzeniem informacji, na którą składają się systemy informacyjne, np. GIS (system informacji przestrzennej), rejestry, archiwa, bazy danych oraz hurtownie danych. Z kolei *middle-office* to część nowej infrastruktury przeznaczonej do bezpośredniego wspomagania pracy urzędników w przetwarzaniu informacji i wyborze decyzji[21]. Ujmując rzecz inaczej - podczas gdy e-usługi skupiają się na zewnętrznych relacjach, e-administracja odnosi się do wewnętrznej organizacji pracy urzędu: wprowadzania elektronicznego przepływu dokumentów, systemów informatycznych wspomagających przepływ informacji (intranet) oraz podejmowania decyzji[22]. Wydaje się zatem za słuszne postawienie wniosku, że nie jest możliwie realizowanie e-usług przez administrację publiczną bez jej uprzedniego przygotowania i funkcjonowania pod względem informatycznym. Wykorzystanie narzędzi i systemów teleinformatycznych w ramach realizowania zadań przez administrację publiczną jest tutaj niezbędne.

E-usługi administracji publicznej

Wymaga podkreślenia, że co do zasady dla realizacji usług z wykorzystaniem środków komunikacji elektronicznej ustawodawca nie przewiduje odrębnej procedury i nie określa katalogu innych, odrębnych wymagań, spełnienie których jest niezbędne dla załatwienia konkretnej sprawy w trybie on-line. Jak słusznie jednak zauważa E. Walczyk zasadnicza różnica to brak konieczności osobistego stawiennictwa w celu złożenia pism. Natomiast tym co sprawia, że obywatel ma pewność, iż załatwia sprawę urzędową, jest elektroniczna postać formularza wniosku, który urząd udostępnia do wypełnienia wniosku. Wniosek ten nie różni się właściwie niczym od jego wersji papierowej, którą obywatel składa osobiście w urzędzie, jeśli decyduje się na tradycyjną ścieżkę załatwienia danej sprawy, ze względu np. na brak dostępu do Internetu[23]. Także J. Janowskiego zwraca uwagę, że tym, co wyróżnia elektroniczne czynności prawne i urzędowe od dokonywanych tradycyjnie, jest elektroniczny i sieciowy zarazem sposób składania (udostępniania, przekazywania, doręczania, przesyłania, transmitowania) składających się na nie oświadczeń woli i wiedzy. Dokonywanie czynności prawnych przez wymianę danych w postaci elektronicznej pomiędzy systemami informatycznymi i za pomocą sieci teleinformatycznych, stanowi faktyczną

20 E. Modzelewska, *Światowe trendy w projektowaniu e-usług*…, op. cit. s. 84

21 M. Sakowicz, *Modernizacja samorządu terytorialnego w procesie integracji Polski z Unią Europejską*, Szkoła Główna Handlowa w Warszawie, Warszawa 2007 r. s. 154

22 M. Sakowicz, *Zastosowanie nowych technologii*…, op. cit. s. 79

23 E. Walczyk, Usługi administracji publicznej na ePUAP, (w:) ePUAP w praktyce, Wydawnictwo Presscom sp. z o.o. Wrocław 2011, s. 52, http://www.itwadministracji.pl/files/File/jdej1g40abp2un/1g753fj0abp35h/ePUAP_w_praktyce.pdf z dnia 31.07.2012 r.

i decydująca podstawę wyodrębnienia elektronicznego obrotu prawnego, rzutującą na jego odmienność od obrotu tradycyjnego[24].

W doktrynie ugruntowany został podział e-usług na trzy rodzaje:

- usługi informacyjne - komunikacja jednokierunkowa - obejmują informacje tematycznie sklasyfikowane i udostępniane na żądanie zainteresowanego (np. strony www),
- usługi komunikacyjne - komunikacja dwukierunkowa – umożliwiające wzajemną wymianę informacji między obywatelem a instytucjami publicznymi,
- usługi transakcyjne - pozwalające pozyskać produkty sektora informacyjnego, wpływać na efekty ich działania (np. formularze podatkowe, ankiety, głosowania) [25].

W zasadzie taki sam podział e-usług dokonuje M. Sakowicz, z tym że Autor większy nacisk kładzie na etapy ich realizacji *on-line* z punktu widzenia obywatela. I tak, pierwszym z nich jest faza informacyjna. Podczas niej interesant dowiaduje się o usługach, z kim ma się kontaktować w sprawie szczegółów, jak wypełnić formularze, dokonać transakcji. W drugiej fazie – tzw. zawarcia umowy (*contracting*) – użytkownik wie, co chce zrobić, a więc przystępuje do ściągnięcia formularza lub wypełnienia go *on-line*. Czasami pomiędzy dwoma stronami odbywają się negocjacje w celu zawarcia odpowiedniej umowy wiążącej obydwie strony. W przypadku transakcji zawieranych *on-line* istotnym elementem są kwestie bezpieczeństwa oraz potwierdzenia autentyczności. W kolejnej fazie świadczenia usługi i dokonania transakcji rezultat pracy transferowany jest do interesanta, który z kolei płaci za serwis. Ostatnim etapem jest faza potransakcyjna, podczas której podmioty mogą złożyć skargę, odwołać się od decyzji. Na uwagę zasługuje jeszcze użyteczność tego systemu, rozumiana jako zakres użycia produktu, mając na uwadze zamierzony cel: założona efektywność, sprawność i satysfakcję. Efektywność odnosi się do dokładności i kompletności, z jaką użytkownik osiąga zamierzone cele. Sprawność (*efficiency*) określa koszty w stosunku do zasobów, natomiast satysfakcja – poziom komfortu i pozytywnego nastawienia do produktu[25].

Z kolei A. Budziewicz-Guźlecka w sporządzonym przez siebie podziale e-usług kieruje się kryterium dostępności usług publicznych *online* uwzględniających formy komunikacji. Stosownie zatem wyróżnia:

- poziom 1 – informacyjny, oznacza dostępność *online* informacji niezbędnej do rozpoczęcia jakiegoś procesu,
- poziom 2 – jednokierunkowy, oznacza możliwość pobierania formularzy z oficjalnej strony podmiotu publicznego, aby po wydrukowaniu móc rozpocząć proces związany z daną usługą
- poziom 3 – dwukierunkowy, oznacza możliwość wypełnienia formularza na oficjalnej stronie podmiotu publicznego, niezbędny system autentyfikacji osoby
- poziom 4 – w pełni elektroniczny transakcyjny system, udostępniający usługi w całości poprzez sieć, włączając podejmowanie decyzji oraz dostarczanie jej. Nie jest potrzebna forma papierowa na żadnym z etapów realizacji usługi

24 J. Janowski, *Elektroniczny obrót prawny*…, op. cit. s. 74

25 za A. Budziewicz, Rola e- usług administracji publicznej w Polsce w rozwoju społeczno-gospodarczym, http://www.sceno.edu.pl/print_content.php?dsid=&cms_id=1714&ctr=c&tr=&lang=pl z 10.05.2013

26 M. Sakowicz, *Modernizacja samorządu terytorialnego*…, op. cit. s. 159-160 i podana tam literatura

Dodatkowo mówi się o poziomie 0, który oznacza brak jakichkolwiek stron www lub istniejące strony nie zawierają informacji związanych z badanymi usługami[27].

Inaczej w tej kwestii podziału e-usług administracji publicznej wypowiada się P. Lipiński. Otóż stoi on na stanowisku, że w zależności od stopnia rozwoju e-administracji usługi te mogą być świadczone na czterech różnych poziomach:

- stopień pierwszy (tzw. informacja *on-line*) – możliwość wyszukania informacji o danym urzędzie oraz świadczonych tam usługach na jego stronie internetowej,
- stopień drugi (tzw. interakcja jednokierunkowa) – możliwość wyszukania informacji oraz pobrania oficjalnych formularzy ze strony internetowej urzędu,
- stopień trzeci (tzw. interakcja dwukierunkowa) – możliwość wyszukania informacji, pobrania oraz odesłania wypełnionych formularzy za pomocą Internetu,
- stopień czwarty (tzw. transakcja) – pełna obsługa procesu, czyli możliwość dokonania wszystkich czynności niezbędnych do załatwiania danej sprawy urzędowej drogą elektroniczną – od uzyskania informacji, poprzez pobranie odpowiednich formularzy, ich odesłanie po wypełnieniu i złożeniu podpisu elektronicznego, aż do uiszczenia wymaganych opłat oraz otrzymania oficjalnego pozwolenia, zaświadczenia lub innego dokumentu, o który dana osoba/firma występuje[28].

Natomiast pomiar efektywności projektu oparty jest na kilku miarach w zakresie świadczenia usług publicznych:

- I miara czasowa – czas od zgłoszenia zapotrzebowania do zakończenia realizacji usługi publicznej
- II miara czasowa – czas „zainwestowany" przez obywatela lub przedstawiciela firmy w uzyskanie usługi np. czas dwukrotnej podróży z domu do urzędu i z powrotem, wypełnienia wniosku, czekania w kolejce do kasy i w kolejce do urzędnika
- I miara kosztowa – koszt poniesiony przez obywatela lub przedstawiciela firmy na uzyskanie usługi np. kosztów dojazdu do urzędu i opłat skarbowych
- II miara kosztowa – koszt ponoszony przez państwo na świadczenie usługi publicznej[29].

Bariery rozwoju e-usług administracji publicznej

Wobec stosowania ICT wyróżnia się cztery postawy (4 x „i" - ignorancja, izolacja, idealizacja, integracja). Pierwsza postawa przejawia się w ignorowaniu narzędzi ICT. Jest to wynikiem braku podstawowych informacji o nowoczesnych technologiach. Druga postawa to postrzeganie ICT jako oddzielnego procesu reform, jako problem natury technicznej, a nie strukturalnej, za który odpowiedzialność ponoszą informatycy. Trzecia traktuje technologie ICT jako „lek na całe zło". Takie idealistyczne spojrzenie jest właściwe osobom słabo obeznanym z nowoczesną technologią, wierzącym, że pomogą one rozwiązać wszystkie problemy administracji. Czwarta postawa wiąże się z naturalnym włączeniem ICT do codziennej praktyki administracyjnej. Jest to postawa, która gwarantuje osiągnięcie pożądanych efektów w zakresie

27 A. Budziewicz- Guźlecka, *Rozwój usług e-government w Polsce*.., op. cit. s. 6-7

28 P. Lipiński, *E-administracja sposobem na usprawnienie funkcjonowania organów administracji publicznej w Polsce* , ksu.parp.gov.pl/res/pl/pk/pakiety.../07/e_administracja.doc z 10.05.2013, s. 1, Z. Stempnakowski, *Administracja elektroniczna,* (w:) red. A. Szewczyk, *Społeczeństwo informacyjne-problemy rozwoju,* Wydawnictwo Difin sp. z o.o. Warszawa 2007 r. s. 53

29 M. Sakowicz, *Modernizacja samorządu terytorialnego* …, op. cit. s. 157

zastosowania ICT[30]. Z kolei M. Madejczyk jako bariery skutecznego wdrożenia elektronicznych usług uważa przede wszystkim:

- brak przyzwyczajeń społeczeństwa (uświadomionej potrzeby) ich wykorzystywania i związany z tym brak świadomości zawartych w nich możliwości,
- koszty dostępu do technologii usług elektronicznych (Internet, zestawy do podpisu elektronicznego) oraz co najważniejsze,
- ułomności uwarunkowań prawnych ich świadczenia przez administrację publiczną[31].

Warto w tym miejscu zauważyć, że znaczące przeszkody we wprowadzeniu e-usług generuje sama administracja. Nie podlega dyskusji, że wykorzystanie nowych technologii informacyjno-komunikacyjnych (ICT) łączy się z całościową modernizacją funkcjonowania urzędów administracji. Przejście z pracy papierowej na elektroniczną może wywoływać opór i stanowić utrudnienie dla części pracowników. Praca z dokumentami elektronicznymi stawia wyższe wymagania pracownikom administracji[32]. Wiąże się to potrzebą przedstawienia klasyfikacji postaw urzędników wobec nowoczesnych technologii informacyjnych i komunikacyjnych[33]. Barierą we wdrożeniu elektronicznych usług administracji jest również konstrukcja formalna procedur administracyjnych. Konieczność dołączania do wniosku określonych załączników, podawania w podaniu wielu informacji (często nie dość precyzyjnie skonstruowanych) nie zachęca do korzystania z formy elektronicznej do załatwienia sprawy administracyjnej. „Dodatkowo brak koordynacji w skali kraju doprowadziło do rozproszenia systemów informacyjnych jednostek administracji publicznej, budowanych w oderwaniu od innych systemów informacyjnych, bez dzielenia się wiedzą i doświadczeniem. Wynikiem takiego działania jest fragmentacja rynku usług publicznych *on-line*[34]".

Z kolei D. Chromicka zauważa, że informatyzację wdrażają i propagują osoby, które często nie wyobrażają sobie funkcjonowania bez wykorzystywania nowoczesnych rozwiązań. Przekonani o ich niezbędności zapominają o tym, że nadal wiele osób ma trudności z obsługą komputera (i pracą z edytorem tekstu), skanera czy faksu, nie posiada konta poczty elektronicznej, czy konta w banku elektronicznym i nie jest świadoma skutków użycia bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu, a co więcej, wcale nie jest zainteresowana poszerzaniem swojej wiedzy w tym zakresie[35]. Wciąż jeszcze przecież spora część społeczeństwa pozostaje wykluczona cyfrowo czy też z braku infrastruktury, czy też z braku umiejętności wykorzystania dostępnej technologii[36].

Wydaje się, że pomimo nie tylko trudności natury organizacyjnej ale też oporu ze strony samych urzędników i obaw obywateli

30 A. Monarcha-Matlak, *Obowiązki administracji*…, op. cit. s. 166

31 M. Madejczyk, *Dokument elektroniczny w administracji publicznej Wykorzystajmy szansę*, Elektroniczna Administracja lipiec – sierpień 2007,s. 15

32 A. Monarcha – Matlak, *Obowiązki administracji* …, op.cit. s. 203 - 204

33 A. Dębicka, M. Dmochowski, *Nowoczesne technologie informacyjne i komunikacyjne jako czynnik profesjonalizacji administracji publicznej* (w:) A. Dębicka, M. Dmochowski, B. Kudrycka, *Profesjonalizm w administracji publicznej*, Białystok 2004, s. 360 i n. i cytowana tam literatura.

34 I. Adamska, *Problemy w projektach informatycznych*…, op. cit. s. 104

35 D. Chromicka, *Instrukcje kancelaryjne w e-administarcji* (w:) red. G. Szpor, *Prawne problemy informatyzacji administracji,* Warszawa 2008, s. 64-65

36 I. Adamska, *Problemy w projektach informatycznych*…, op. cit. s. 104

we wprowadzaniu i funkcjonowaniu elektronicznej administracji od tego procesu nie ma odwrotu. Jego skutkiem będzie tworzenie e-urzędów. Jest to naturalna konsekwencja rozwoju społeczeństwa informacyjnego, w którym coraz większą rolę odgrywa informatyka i Internet. Postulować zatem należy o przenoszenie coraz większej ilości usług realizowanych przez administrację do sfery elektronicznej ale po wcześniejszym dopracowaniu wymagań formalnych aby można było w pełni z tych usług korzystać. Oczywiście o tym, jak szybko ten proces będzie postępował zależy w dużej mierze od obywateli – od tego, czy z tych proponowanych nowoczesnych form realizacji usług będą korzystali. Wymaga to bowiem niewątpliwie pewnej dojrzałości i odpowiedniego poziomu umiejętności.

Streszczenie

Coraz powszechniejsze wykorzystywanie w praktycznej każdej dziedzinie życia społecznego nowoczesnych technologii komunikacyjnych i realizowanie za jej ich pośrednictwem usług do tej pory świadczonych z użyciem form tradycyjnych (poczta, osobiste stawiennictwo) stanowi dla administracji publicznej poważne wyzwanie. Niezbędna staje się bowiem taka modyfikacja dotychczas realizowanych zadań, procedur, metod działania, aby realne stało się również korzystanie przez administrację publiczną z nowych technologii i narzędzi informatycznych. Szczególny nacisk należy tutaj położyć na stosowanie środków komunikacji elektronicznej i Internetu. Ma to także istotne znaczenie w procesie budowania społeczeństwa informacyjnego. Tylko bowiem dzięki temu administracja publiczna może szybciej, łatwiej i taniej wykonywać przypisane jej ustawowo zadania.

Electronic public services

The increasing presence of modern communication technologies in practically every area of social life and using them to provide services that so far were rendered by traditional forms (post, personal appearance) constitute a great challenge for the public administration. It is necessary to conduct modification of the currently implementing tasks, procedures and methods of operation so as to enable the public administration to use new technologies and IT tools. A special emphasis should be placed on the use of electronic communications and the Internet. It is also important in the process of creating information society. Only by meeting these conditions, the public administration can faster, easier and cheaper perform the tasks assigned to it by law.

dr Dorota Fleszer - Absolwentka Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach. Jest pracownikiem naukowym na Wydziale Prawa Wyższej Szkoły Humanitas w Sosnowcu oraz urzędnikiem samorządowym. Zajmuje się problematyką informacji w administracji i administracją publiczną.

Zapraszamy do udziału

SEMINARIUM

LXI edycja seminarium w cyklu AKADEMIA PRAWA KOMPUTEROWEGO

TAJEMNICE FIRMOWE I NIEUCZCIWA KONKURENCJA

ASPEKTY PRAWNE I ORGANIZACYJNE

Warszawa, 27.08.2013

Więcej informacji: www.cpi.com.pl

Dotacje unijne na informatyzację administracji publicznej

Ewa Modzelewska

Z jakich unijnych programów pomocowych korzystają instytucje administracji publicznej? Czy w ramach tych środków może zostać dofinansowany proces informatyzacji urzędów? Jakie zadania i koszty kwalifikowalne stanowią najczęściej przedmiot wsparcia?

W niniejszym opracowaniu podjęto próbę analizy źródeł finansowania organów administracji publicznej stwarzających możliwość świadczenia usług drogą elektroniczną, usprawniających obsługę obywatela i przedsiębiorcy w urzędzie. W ostatnich kilku latach zauważalny jest wzrost interakcji pomiędzy urzędami a obywatelami za pomocą systemów teleinformatycznych w publicznych sieciach telekomunikacyjnych. Elektroniczna administracja to nie tylko nowoczesne technologie, ale budowanie całości doświadczeń e-obywatela w oparciu o daną usługę publiczną, począwszy od zyskania świadomości o istnieniu usługi, a skończywszy na zaprzestaniu korzystania z niej, poprzez wszystkie „punkty styku", czyli określone rodzaje interakcji obywatela z instytucjami administracji publicznej. Dzięki stworzonej sieci wzajemnych oddziaływań zachodzących w przestrzeni cyfrowej pomiędzy usługodawcą –urzędem, a usługobiorcą – obywatelem można wygenerować e-usługę, która będzie zindywidualizowana, z bogatym zasobem informacyjnym.

Na podstawie wyników badań dot. wpływu informatyzacji na działania administracji publicznej w Polsce w 2011 r. przeprowadzonych przez MSWiA wspólnie z instytutem badawczym ARC Rynek i Opinia można stwierdzić, iż „elektroniczny system zarządzania dokumentacją posiada większość urzędów marszałkowskich i powiatowych. Dzięki niemu możliwa jest elektroniczna wymiana akt danej sprawy w obrębie urzędu, czyli np. przekazanie innej komórce organizacyjnej sprawy on-line (z tej formy korzysta 77% urzędów administracji rządowej i 71% samorządowej). Jak wynika z badania, najczęściej z elektronicznego systemu zarządzania dokumentacją korzystają urzędy z województw śląskiego (71%) i dolnośląskiego (70%), a najrzadziej z województwa świętokrzyskiego (11%). Plany wdrożenia tego systemu zadeklarowało ponad 80% urzędów, które obecnie z takiego systemu nie korzystają. Około co piąty planuje jego wprowadzenie do końca 2011 roku, a prawie co drugi – w przyszłym roku (…)".„Obecnie 28% urzędów posiada zapasowe łącze z Internetem na wypadek awarii łącza głównego, a jego przepustowość w prawie 70% przypadków przekracza 2 Mb/s. W łącze zapasowe częściej wyposażone są urzędy administracji rządowej (43%) niż samorządowej (28%). Sporą różnicę w tym zakresie daje się zauważyć w zależności od lokalizacji – w województwie kujawsko-pomorskim co drugi urząd posiada łącze zapasowe, natomiast w województwie podlaskim mniej niż co dziesiąty[1]".

Fundusze na czasie, czyli wielka e-rewolucja w urzędach

„143 mln zł przewidziano w projekcie budżetu na 2013 r. na zadania związane z informatyzacją; ponad 100 mln zł z tej

1 V. Szymanek, *Wyposażenie gospodarstw domowych w komputery i Internet,* [w:] *Społeczeństwo informacyjne w liczbach,* Departament Społeczeństwa Informacyjnego Ministerstwa Administracji i Cyfryzacji, Warszawa 2012, s. 20.

puli będzie przeznaczone na informatyzację administracji publicznej. Z kolei ponad 75 mld zł zaplanowano na współfinansowanie programów unijnych[2]".

Jednostki administracji publicznej najczęściej przeznaczają dofinansowanie z UE na rozwój i tworzenie elektronicznych narzędzi przesyłania informacji pomiędzy samymi urzędami administracji publicznej, na budowę i rozwój elektronicznych platform usług publicznych w formie e-usług, na informatyzację urzędu. Wydatkami kwalifikowalnymi w ramach projektów informatycznych dedykowanych administracji publicznej są m.in.:

- zakup sprzętu komputerowego,
- zakup oprogramowania,
- budowę, rozbudowę i modernizację infrastruktury informatycznej,
- serwis informatyczny
- tworzenie promocyjnych stron internetowych gminy lub powiatu.

Najczęściej urzędy administracji publicznej ubiegają się o środki na inwestycję informatyczne z Regionalnych Programów Operacyjnych. Osią dofinansowanie jest: udostępnienie i tworzenie usług publicznych – e-urząd oraz udostępnienie i utworzenie sieci, usług i punktów dostępowych dla mieszkańców, podniesienie jakości usług świadczonych przez urzędy, wzrost dostępności i zakresu e-usług, wykorzystanie nowoczesnych systemów informatycznych w zakresie obiegu dokumentów, monitorowania postępu spraw obywateli, kontroli i weryfikacji postępowań administracyjnych, monitoring środowiskowy, tworzenia społeczeństwa informacyjnego.

Jak wynika z tabeli, wszystkie działania zdywersyfikowanych wedle województw mają na celu budowanie i wdrażanie platform elektronicznych dla zintegrowanego systemu wspomagania zarządzania na poziomie

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
dolnośląskie	2	Rozwój społeczeństwa informacyjnego na Dolnym Śląsku „Społeczeństwo informacyjne"	**Wspieranie konkurencyjności regionu poprzez rozwój szeroko rozumianej regionalnej i lokalnej infrastruktury społeczeństwa informacyjnego.**	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**2.1 Infrastruktura społeczeństwa informacyjnego** **2.2 Rozwój usług elektronicznych**
kujawsko-pomorskie	4	Rozwój infrastruktury społeczeństwa informacyjnego	Zwiększenie dostępu do szerokopasmowej sieci informatycznej oraz stosowanie w usługach i gospodarce technologii informacyjnych i komunikacyjnych	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**Działanie 4.1 Rozwój infrastruktury ICT** **Działanie 4.2 Rozwój usług i aplikacji dla ludności** **Działanie 4.3 Rozwój komercyjnych e-usług**

2 http://www.portalsamorzadowy.pl/prawo-i-finanse/ile-w-2013r-na-informatyzacje-ile-na-unijne-dotacje,37891_0.html [dostęp 26.06.2013]

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
łódzkie	4	Społeczeństwo informacyjne	Zapewnienie i zwiększenie dostępności do nowoczesnych technologii ICT, poprawę umiejętności posługiwania się narzędziami ICT oraz do przeciwdziałanie wykluczeniu cyfrowemu mieszkańców regionu.	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**Działanie 4.1 Infrastruktura społeczeństwa informacyjnego** **Działanie 4.3 E--technologie dla przedsiębiorstw**
lubelskie	2	Infrastruktura ekonomiczna	Ułatwienie dostępu przedsiębiorstwom do zewnętrznych źródeł finansowania; Zwiększenie wykorzystania potencjału regionalnych uczelni i jednostek naukowych poprzez inicjowanie współpracy sektora B+R z sektorem MŚP; wsparcie instytucji otoczenia biznesu poprzez inwestycje i doradztwo; promocję gospodarczą przedsiębiorstw województwa lubelskiego, w tym ułatwianie nawiązywania kontaktów i współpracy z innymi podmiotami.	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**Działanie 2.4. Marketing gospodarczy**
lubuskie	1	Rozwój infrastruktury wzmacniającej konkurencyjność regionu	Poprawa stanu infrastruktury transportowej w województwie Budowa społeczeństwa opartego na wiedzy Zwiększenie atrakcyjności inwestycyjnej województwa	50% całkowitych kwalifikowalnych wydatków projektu (dot. wydatków inwestycyjnych i wydatków poniesionych na prace przygotowawcze) 45% całkowitych kwalifikowalnych wydatków projektu w ramach cross-financingu (intensywność może być zwiększona o dodatkowe 10 punktów procentowych brutto, jeżeli szkolenie jest przeznaczone dla pracowników w gorszym położeniu	**1.1 Poprawa stanu regionalnej infrastruktury transportowej** **1.2 Tworzenie obszarów aktywności gospodarczej i promocja gospodarcza** **1.3 Rozwój społeczeństwa informacyjnego**
małopolskie	1	Warunki dla rozwoju społeczeństwa opartego na wiedzy	Wspieranie rozwoju Województwa Małopolskiego poprzez rozbudowę regionalnej i lokalnej infrastruktury społeczeństwa informacyjnego, a także zwiększenie wykorzystania Internetu oraz innych technologii informacyjnych i komunikacyjnych (ICT) do świadczenia usług publicznych.	Projekty realizowane w ramach osi priorytetowej uzyskają wsparcie w wysokości do 85% kosztów kwalifikowanych.	**Działanie 1.2 Rozwój społeczeństwa informacyjnego**

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
mazowieckie	2	Przyspieszenie e-rozwoju Mazowsza	Rozwój społeczeństwa informacyjnego poprzez wsparcie dla przedsięwzięć wynikających ze Strategii e-Rozwoju Województwa Mazowieckiego na lata 2007-2013.	Maksymalny udział środków UE w wydatkach kwalifikowalnych na poziomie projektu):85 proc. Minimalny wkład własny beneficjenta: 3 proc. dla jednostek samorządu terytorialnego i ich jednostek organizacyjnych, gdy nie występuje pomoc publiczna.	**Działanie 2.1. Przeciwdziałanie wykluczeniu społecznemu** **Działanie 2.2. Rozwój e-usług**
opolskie	2	Społeczeństwo informacyjne	Stworzenie technicznych warunków do powszechnego wykorzystania narzędzi ICT w życiu gospodarczym, publicznym i indywidualnym podmiotów i mieszkańców regionu. Promowanie społeczeństwa informacyjnego poprzez rozwój modułów informacyjnych usług *e-goverment* na rzecz podniesienia konkurencyjności regionu.	Maksymalny udział środków UE w wydatkach kwalifikowanych na poziomie projektu: - projekty nie objęte pomocą publiczną – maks. 85%, - projekty objęte pomocą publiczną – 50% - dla projektów realizowanych przez państwowe jednostki budżetowe - 100% Minimalna/maksymalna wysokość wsparcia - od 1,2 mln PLN. Maksymalny udział środków UE w wydatkach kwalifikowanych na poziomie projektu: - 100%, - dla projektów realizowanych przez państwowe jednostki budżetowe – 85% Minimalna/maksymalna kwota wsparcia od 200 tys. PLN	**Działanie 2.1 Infrastruktura dla wykorzystania narzędzi ICT** **Działanie 2.2 Moduły informacyjne, platformy e-usług i bazy danych**
podkarpackie	2	Infrastruktura techniczna	Poprawa dostępności i atrakcyjności inwestycyjnej regionu poprzez realizację przedsięwzięć w sferze komunikacyjnej, informatycznej i energetycznej. Realizacja tego celu będzie następować poprzez cele szczegółowe: poprawę powiązań komunikacyjnych i systemu komunikacji publicznej w województwie, poprawę stanu i efektywności wykorzystania infrastruktury energetycznej.	70% - Schemat A, B i C 85% - Pozostałe schematy 85% - projekty wymienione w Indykatywnym Planie Inwestycyjnym Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**Działanie 2.1 Infrastruktura komunikacyjna** **Działanie 2.2 Infrastruktura energetyczna**

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
podlaskie	4	Społeczeństwo informacyjne	Celem Osi priorytetowej jest upowszechnienie stosowania technik systemu telekomunikacyjnego oraz zwiększenie dostępu do usług elektronicznych poprzez rozbudowę regionalnej infrastruktury teleinformatycznej.	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	
pomorskie	2	Społeczeństwo wiedzy	Tworzenie warunków sprzyjających budowaniu społeczeństwa wiedzy.	Maksymalny poziom współfinansowania ze środków unijnych wynosi 75%. Minimalna wartość projektu - równowartość w PLN kwoty 500 000 EUR lub 250000 EURO (2.2.1)	**Działanie 2.1 Infrastruktura edukacyjna i naukowo-dydaktyczna** **Działanie 2.2 Infrastruktura i usługi tworzące podstawy społeczeństwa informacyjnego**
śląskie	2	Społeczeństwo informacyjne	Stworzenie warunków do rozwoju społeczeństwa informacyjnego w regionie	Maksymalny poziom dofinansowania środkami Europejskiego Funduszu Rozwoju Regionalnego wynosi 85% wydatków kwalifikowalnych projektu	**Działanie 2.1 Infrastruktura społeczeństwa informacyjnego** **Działanie 2.2. Rozwój elektronicznych usług publicznych**
świętokrzyskie	2	Wsparcie innowacyjności, budowa społeczeństwa informacyjnego oraz wzrost potencjału inwestycyjnego regionu	Poprawa powiązań pomiędzy podmiotami działającymi na rzecz innowacyjności i gospodarką. Tworzenie i rozbudowa sieci teleinformatycznych oraz rozwój systemów usług elektronicznych, w tym dla podmiotów gospodarczych. Wzrost dostępności kompleksowo wyposażonych terenów inwestycyjnych. Poprawa wizerunku regionu, jego potencjału gospodarczego i turystycznego.	Maksymalna wysokość dotacji ze środków UE wynosić będzie od 50% do 85% kosztów kwalifikowanych inwestycji i wynikać będzie z przepisów dotyczących pomocy publicznej, oraz mapy pomocy określającej poziom dofinansowania. Maksymalna wartość projektu dotyczącego infrastruktury B+R wynosi 4 000 000 PLN dla projektów realizowanych przez wyższe uczelnie lub inne jednostki naukowe, oraz 200 000 PLN dla projektu realizowanego przez przedsiębiorców. Maksymalna wysokość dotacji ze środków UE wynosić będzie od 50% do 85% kosztów kwalifikowanych inwestycji i wynikać będzie z przepisów dotyczących pomocy publicznej, oraz mapy pomocy określającej poziom dofinansowania.	**Działanie 2.1 Rozwój innowacji oraz wspieranie działalności dydaktycznej i badawczej szkół wyższych oraz placówek sektora „Badania i Rozwój"** **Działanie 2.2 Budowa infrastruktury społeczeństwa informacyjnego** **Działanie 2.3 Promocja gospodarcza i turystyczna regionu** **Działanie 2.4 Tworzenie kompleksowych terenów inwestycyjnych**

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
warmińsko-mazurskie	7	Infrastruktura społeczeństwa informacyjnego	**Zwiększenie dostępu do sieci i wykorzystania technik informatycznych w gospodarce i sferze społecznej.**	Dotacja do 85 proc. kosztów kwalifikowanych projektu (dla projektów nie objętych pomocą publiczną). Dla projektów podlegających zasadom udzielania pomocy publicznej maksymalny poziom dofinansowania projektów ze środków publicznych (UE + budżet państwa) - zgodnie z zasadami określonymi w rozporządzeniach dotyczących udzielania pomocy publicznej w wysokości max. 50 proc. (w tym 85 proc. Europejski Fundusz Rozwoju Regionalnego i 15 proc. budżet państwa).	**Działanie: 7.1 Tworzenie infrastruktury społeczeństwa informacyjnego**
wielkopolskie	2	Infrastruktura komunikacyjna	**Zwiększenie wymiany gospodarczej z otoczeniem na rzecz wzrostu zatrudnienia.**	Dofinansowanie: max 85% kosztów kwalifikowanych	**2.1 Wzmocnienie regionalnego układu powiązań drogowych (drogi wojewódzkie, z wyłączeniem dróg wojewódzkich w miastach na prawach powiatu)** **2.2 Poprawa dostępności do regionalnego i ponadregionalnego układu drogowego (drogi wojewódzkie w miastach na prawach powiatu, powiatowe i gminne)** **2.3 Modernizacja regionalnego układu kolejowego** **2.4 Tabor kolejowy dla regionalnych przewozów pasażerskich** **2.5 Rozwój miejskiego transportu zbiorowego** **2.6 Rozwój regionalnej infrastruktury lotniczej** **2.7 Infrastruktura społeczeństwa informacyjnego**

Województwo	Numer osi priorytetowej	Tytuł osi priorytetowej	Cel priorytetu	Wnioskodawca może ubiegać się maksymalnie o wsparcie w wysokości:	Działania w ramach priorytetu
zachodniopomorskie	3	Rozwój społeczeństwa informacyjnego	**Wsparcie rozwoju regionu poprzez rozbudowę regionalnej i lokalnej infrastruktury społeczeństwa informacyjnego.**	75% całkowitych wydatków kwalifikowalnych, 85% całkowitych wydatków kwalifikowalnych w przypadku projektów zlokalizowanych wyłącznie na terenie gmin o niekorzystnej sytuacji społeczno-gospodarczej zgodnie z załącznikiem 6 do RPO WZ (nie dotyczy projektów objętych pomocą publiczną, dla których wysokość dofinansowania określona jest w odrębnych przepisach)	**Działanie 3.1 Infrastruktura społeczeństwa informacyjnego** **Działanie 3.2 rozwój systemów informatycznych i e-usług**

Tabela 1. Zestawienie osi priorytetowych w RPO według województw nastawionych na informatyzację administracji publicznej
Źródło: opracowanie własne na podstawie danych zawartych w Szczegółowych Opisach Priorytetów Regionalnego Programu Operacyjnego

regionalnym oraz lokalnym, tworzenie Systemów Informacji Przestrzennej, informatyzację instytucji publicznych. Ponadto w ramach tych samych programów regionalnych istnieje możliwość ubiegania się przez jednostki samorządu terytorialnego o dofinansowanie rozwoju e-usługi dla obywateli.

Wysokość pomocy w ramach dotacji unijnej nie jest jednakowa we wszystkich regionach. Każde województwo ma odrębne wytyczne kształtujące warunki pomocy. Intensywność pomocy dla projektów nieobjętych pomocą publiczną – maks. 85 proc., tam gdzie pomoc występuje – zgodnie z zasadami pomocy publicznej. Nabór wniosków prowadzony jest w formie konkursów z określonymi ramami czasowymi. Więcej szczegółów należy szukać na stronach internetowych instytucji odpowiedzialnej za wdrażanie regionalnego programu operacyjnego województwa, w którym ma być realizowany projekt.

Dokonując analizy źródeł finansowania procesu informatyzacji administracji publicznej warto przybliżyć działanie 8.3 Programu Operacyjnego Innowacyjna Gospodarka **Przeciwdziałanie wykluczeniu cyfrowemu e-Inclusion**, mającego na celu zapewnienie dostępu do Internetu dla osób zagrożonych wykluczeniem cyfrowym z powodu trudnej sytuacji materialnej lub niepełnosprawności. Wsparcie operacji najczęściej dotyczy: tworzenia usług elektronicznych, tworzenia elektronicznej komunikacji między przedsiębiorstwami, przeciwdziałania wykluczeniu cyfrowemu. Katalog Beneficjentów obejmuje następujące podmioty: jednostki samorządu terytorialnego, grupy jednostek samorządu terytorialnego – konsorcja, związki, stowarzyszenia i porozumienia, konsorcja jednostek samorządu terytorialnego lub w/w grup jednostek samorządu terytorialnego z organizacjami pozarządowymi. Maksymalny udział środków UE w kwocie dofinansowania (w %) wynosi 85%.

Wielka naprawa e-administracji

Intensyfikacja działań w obszarze informatyzacji państwa nie przekłada się na liczbę wdrożonych i sprawnie funkcjonujących e-usług publicznych. „Poziom zaawansowania rozwoju usług publicznych w 2004 roku wynosił w Polsce 35%, podczas gdy średnia dla krajów EU – 25 osiągnęła 68%. Poziom pełnej interaktywności usług publicznych *on-line* w EU-25 kształtował się na poziomie 40%, a w Polsce – 9%[3]". Informatyzacja administracji publicznej w Polsce przypomina bardziej bieg na 60 metrów niż maraton. Rzadko wdrażanie technologii informatyczno – komunikacyjnych przybiera postać zaplanowanego procesu z uporządkowanymi działaniami mającymi przynieść wymierne wskaźniki produktu i rezultatu. W konsekwencji środki na realizację projektów informatycznych e-administracji zostały zamrożone. Przyczynami tego stanu rzeczy były opóźnienia w płatnościach, błędy w przeprowadzaniu procedur zamówień publicznych, źle skoordynowane prace zespołów projektowych, brak znajomości metodologii service design.

W zaprezentowanym przez Ministerstwo Administracji i Cyfryzacji raporcie „Państwo 2.0" omówiono stan informatyzacji administracji publicznej oraz przedstawiano kierunek działań naprawczych skoncentrowanych wokół idei Informatyzacji Zintegrowanej, której naczelne zasady to: podporządkowanie informatyzacji obiegowi informacji, mówienie o procesach w administracji publicznej i usługach, a nie o projektach informatycznych, optymalizacja nakładów w stosunku do planowanych wyników, nieograniczony dostęp obywatela do usług z dowolnego urządzenia, systemu operacyjnego.

Źródła:

Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565; ost.zm., Dz.U. z 2008 r. nr 127, poz. 817)

Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204; ost.zm. Dz.U. z 2008 r. nr 216, poz. 1371)

Dąbrowska A., Janoś – Kresło M., Wódkowski A., *E-usługi a społeczeństwo informacyjne*, Wyd. Difin Sp. z o.o., Warszawa 2009

Społeczeństwo informacyjne w liczbach, Departament Społeczeństwa Informacyjnego Ministerstwa Administracji i Cyfryzacji, Warszawa 2012,

PAŃSTWO 2.0. Nowy start dla e-administracji, https://mac.gov.pl/wp-content/uploads/2012/04/MAC-Panstwo-2-0-Nowy-start-dla-e-administracji-4-2012_raport_web.pdf

http://iw.org.pl/pl/baza-wiedzy/finansowanie-projektow/1308

http://prawo.vagla.pl/node/9928

http://di.com.pl/news/44880,0,MAC_i_Panstwo_20_Czy_e-administracja_teraz_wystartuje.html

http://di.com.pl/news/46537,0,Odzyskamy_unijne_pieniadze_na_informatyzacje_ale_czy_e-administracja_ruszy.html#

http://www.fundusze-europejskie.pl/administracja-publiczna/0,0,a,3853,ile-kasy-w-2013-na-informatyzacje.html

3 A. Dąbrowska, M. Janoś – Kresło, A. Wódkowski, *E-usługi a społeczeństwo informacyjne*, Wyd. Difin Sp. z o.o., Warszawa 2009, s. 48.

http://forsal.pl/artykuly/575283,e_administracja_slony_rachunek_za_12_informatycznych_prac_rzadu.html

http://www.portalsamorzadowy.pl/prawo-i-finanse/ile-w-2013r-na-informatyzacje-ile-na-unijne-dotacje,37891_0.html

http://rpo.dolnyslask.pl

http://fundusze.kujawsko-pomorskie.pl

http://www.rpo.lubelskie.pl

http://www.lrpo.lubuskie.pl

http://www.rpo.lodzkie.pl

http://www.fundusze.malopolska.pl

http://rpo.mazowia.eu

http://rpo.opolskie.pl

http://www.wrota.podkarpackie.pl

http://www.rpowp.wrotapodlasia.pl

http://www.dpr.woj-pomorskie.pl

http://rpo.silesia-region.pl

http://www.rpo-swietokrzyskie.pl

http://www.rpo.warmia.mazury.pl

http://www.wrpo.wielkopolskie.pl

http://www.rpo.wzp.pl

http://www.poig.gov.pl/Dokumenty/ZmianyWDokumentach/Documents/SZOP_POIG_ver_17_27062013.pdf

Ewa Modzelewska - doktorantka na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego (kierunek Nauki o polityce). Specjalista w Pionie Badań i Rozwoju Instytutu Wzornictwa Przemysłowego sp. z o.o.

Zapraszamy do udziału

SEMINARIUM

XIX edycja seminarium w cyklu ZARZĄDZANIE KRYZYSOWE I RATOWNICTWO - INFORMATYCZNE SYSTEMY OSTRZEGAWCZE W ZARZĄDZANIU KRYZYSOWYM

19 września 2013r. | Warszawa

W PROGRAMIE

- System zarządzania kryzysowego w Polsce ? stan obecny i potrzeby rozwoju
  Płk. dr hab. Grzegorz Sobolewski (Akademia Obrony Narodowej)
- Wybrane systemy radiokomunikacyjne dla potrzeb bezpieczeństwa publicznego
  prof. dr hab. inż. Ryszard Katulski (Wydział Elektroniki, Telekomunikacji i Informatyki Politechnika Gdańska)
- Rozwój usług i sieci telekomunikacyjnych oraz kryteria wyboru dla potrzeb zarządzania kryzysowego
  Jerzy Paczocha (Instytut Łączności PIB)
- Zarządzanie kryzysowe a możliwości smart TV i telewizji hybrydowej HbbTV
  Zaproszenie skierowano do: Paweł Tutka, ekspert
- Lotniczy skaning laserowy w projekcie ISOK - możliwość zastosowań w ochronie przed zagrożeniami (powodzie, pożary, etc)
  Zaproszenie skierowano do: Piotr Woźniak, GUGiK, kierownik projektu ISOK
- Co nowego w technologiach satelitarnych w zakresie ochrony przed zagrożeniami kryzysowymi
  dr Bożena Łapeta (IMGW - PIB)
- Monitor IMGW-PIB - system informatyczny dla potrzeb zarządzania kryzysowego
  Grzegorz Słota (IMGW - PIB)

Więcej informacji: **www.cpi.com.pl**

Chmura zaufania

Michał Tabor

Wstęp

Mechanizmy podpisu elektronicznego są zdefiniowane od kilkunastu lat w systemie prawnym, znormalizowane przez krajowe i międzynarodowe instytucje standaryzacyjne, a także zaimplementowane przez wielu dostawców kart, certyfikatów i aplikacji. Najlepiej opisanym i dostępnym dla wszelkich zastosowań jest bezpieczny podpis elektroniczny weryfikowany kwalifikowanym certyfikatem[1,2]. Podpis kwalifikowany nie jest w stanie konkurować z podpisem odręcznym i w praktyce jest wykorzystywany w niewielkim stopniu, głównie tam gdzie przepisy prawne wymusiły jego stosowanie[3].

W tym samym czasie banki stworzyły własne mechanizmy zapewniające bezpieczeństwo dowodowe transakcji, mechanizmy te są oparte o funkcje kart płatniczych, procedury i kody jednorazowe. Ostatnie lata pokazują, że nie tylko banki, ale także inni uczestnicy rynku oraz sama administracja zaczynają stosować mechanizmy prostsze niż podpis kwalifikowany, dostosowane do potrzeb i ryzyka uczestników transakcji. Szczególnymi przykładami tych mechanizmów zaimplementowanych na potrzeby administracji, jest podpis deklaracji podatkowych [4], profil ZUS [5] i uwierzytelnianie pozwów do eSądu [6]. Podstawową ich wadą jest to, że każdy realizuje mechanizmy podpisu we własny sposób, nie dając możliwości ich użycia poza systemem, w którym powstały. Konieczność uproszczenia procedur uwierzytelniania została zauważona w znowelizowanej ustawie o informatyzacji [7] oraz zaimplementowana jako Profil Zaufany ePUAP [8,9], dostarczając narzędzie do podpisywania dokumentów kierowanych przez obywateli i przedsiębiorców do administracji publicznej.

Potrzeby rynku komercyjnego w zakresie elektronizacji są znacznie większe niż opisane w prawie narzędzia, wykraczają znacząco poza samą funkcję podpisania dokumentu elektronicznego. Rozwój ekonomiczny wymusza realizację procesów biznesowych łatwiej i szybciej z wykorzystaniem Internetu. Podpis elektroniczny jako sposób zabezpieczenia tylko wynikowego dokumentu elektronicznego, a nie całości usługi elektronicznej, nie może sprostać nowym wymaganiom rynku. Nowo implementowany podpis elektroniczny musi dostarczyć mechanizmy bezpieczeństwa dla całych procesów biznesowych. Niniejsze opracowanie stanowi ogólne omówienie Chmury Zaufania – stanowiącej ramy bezpieczeństwa i interoperacyjności dla usług oferujących zabezpieczenia dla transakcji elektronicznych.

Usługi zaufania

Jedną z głównych zmian na rynku IT ostatnich lat, które widać zarówno na rynku Europejskim jak i poza nim jest dostarczanie przez usługodawców internetowych usług elektronicznych umożliwiających realizację celów biznesowych, zamiast oferowania tylko narzędzi w postaci aplikacji i komputerów. Coraz więcej oprogramowania jest oferowanego jako usługa, powstają specjalizowane ośrodki i usługi realizujące przetwarzanie danych i realizację całych procesów biznesowych w chmurze. Tak jak usługi pocztowe umożliwiły w przeszłości realizacje umów, składanie dokumentów i doręczanie produktów bez konieczności osobistego stawienia się w miejscu transakcji, tak usługi

obsługi procesów biznesowych w Internecie umożliwiają realizację biznesu na odległość, gdzie koniecznością staje się zapewnienie mechanizmów zaufania pomiędzy uczestnikami tych usług.

Tworząc nowe rozwiązania dla podpisu elektronicznego należy wykorzystać potencjał dotychczasowych rozwiązań, korzystając z ich najlepszych cech i eliminując dotychczasowe wady. Należy zauważyć, że powstało i funkcjonuje wiele produktów umożliwiających utworzenie i weryfikację podpisu elektronicznego, jest także szereg usługodawców wydających certyfikaty i świadczących usługi bazujące na podpisie X.509, jednocześnie przepisy prawne Unii Europejskiej i wewnętrzne Polskie stworzyły ramy do funkcjonowania podpisu elektronicznego, które dają przestrzeń dla stosowania różnych rozwiązań i nie ograniczają się jedynie do PKI.

Analiza problemów

Aby na nowo podejść do podpisu elektronicznego należy także zrozumieć, gdzie aktualnie dostępne formy podpisu elektronicznego są niewystarczające i co stanowi problem ich zastosowania w szerokim spektrum usług dla zastosowań komercyjnych.

Pierwszym z nich jest to, że podpis elektroniczny dla większości użytkowników jest niezrozumiały. Użytkownik nie wie co podpisuje, jak podpisuje, czy to co widzi zostało podpisane zgodnie z jego intencjami. Polityki certyfikacji nakazują podpisującemu pełną kontrolę nad stacją służącą do złożenia podpisu, a jednocześnie takiej kontroli podpisujący nie jest w stanie zapewnić, co może stanowić ryzyko zarówno dla podpisującego jak i dla ufającego.

Dotychczasowy sposób dystrybucji narzędzi do podpisywania, w którym koszt posiadania karty i certyfikatu został przeniesiony na podpisującego nie sprawdził się, ponieważ w większości procesów biznesowych nie podpisujący ma interes prawny w podpisaniu dokumentu, a ten, który ma jemu zaufać. Toteż model, w którym za posiadanie narzędzia do podpisywania musi zapłacić podpisujący i wcześniej dokonać rejestracji nie ma szansy dalszego rozwoju.

Dużym wyzwaniem jest interoperacyjność podpisu, w funkcjonujących obecnie rozwiązaniach przyjęto założenie, że zarówno podpisujący jak i weryfikujący dysponują komplementarnymi urządzeniami do podpisu i weryfikacji, a jakakolwiek niezgodność ich uniemożliwia prawidłową weryfikację podpisu. Znormalizowanie formatów podpisu dało tylko częściowo rozwiązanie, ponieważ liczba określonych normami formatów i profili podpisu jest bardzo duża.

Potrzeby podpisywania są wielorakie, wiąże się z nimi różne ryzyko zależne od podejmowanych przez uczestników zobowiązań. Dostarczenie rozwiązania podpisu elektronicznego, które ma jeden model zabezpieczeń (np. karta + PIN) nie jest adekwatne dla wszystkich potrzeb i powoduje to, że narzędzie stosowane zarówno do zobowiązań o niskim ryzyku i o bardzo wysokim musi stanowić uśrednienie wymagań bezpieczeństwa i użyteczności. Ochrona wymaga różnego rodzaju narzędzi, o różnej gradacji bezpieczeństwa dla różnych rozwiązań i możliwości redukcji ryzyka nie tylko w warstwie technicznej, ale także w warstwie organizacyjnej (proceduralnej) lub przeniesienia ryzyka na inny podmiot.

Usługi dla biznesu, administracji i obywatela

Dostarczenie usług skrojonych na potrzeby swoich użytkowników wymaga elastyczności, zarówno co do oferowanych poziomów zaufania i stosowanych zabezpieczeń, ale przede wszystkim użyteczności. Użyteczność oznacza:

- zrozumiały i przyjazny interfejs użytkownika, w którym użytkownik jest prowadzony i wie jakie jest znaczenie czynności przez niego wykonywanych;
- możliwość komunikowania się w powszechnie wykorzystywanych formatach danych, które będą czytelne dla wszystkich uczestników komunikacji;
- możliwość stosowania różnego rodzaju rozwiązań stacjonarnych i mobilnych, tak aby rozwiązanie dopasowane było do sposobu pracy uczestników procesów;
- możliwość zastosowania usług zaufania różnych dostawców, gdzie powiązania i przepływ ryzyka jest realizowany w tle procesu;
- możliwość współpracy z wieloma dostawcami usług biznesowych, tak aby usługi zaufania stanowiły element usług biznesowych, a nie osobny system.

W ramach budowania dotychczasowego modelu podpisu elektronicznego opartego o PKI stworzono szereg norm i narzędzi, wykorzystywanych w funkcjonujących rozwiązaniach. Budując nowe usługi należy wykorzystać potencjał dotychczasowych usług PKI, stosując zabezpieczenia, formaty, schematy postępowania i urządzenia zdefiniowane na potrzeby PKI. Usługi certyfikacyjne polegające na wydawaniu certyfikatów, możliwości ich unieważnienia oraz dostarczające informacji o ich aktualnym statusie nie dają przestrzeni do budowania usług elastycznych – ponieważ dane służące do składania podpisu elektronicznego chronione są w jeden ustalony sposób, a dane potrzebne do weryfikacji podpisu umieszczone w certyfikacie są niezmienne w czasie jego ważności. Podejście i sposób świadczenia usług certyfikacyjnych musi umożliwić oferowanie usług o różnym poziomie bezpieczeństwa i elastycznym wpleceniu go w procesy biznesowe, dlatego też konieczne jest przedefiniowanie modelu PKI w zakresie sposobu budowania zaufania i roli certyfikatu.

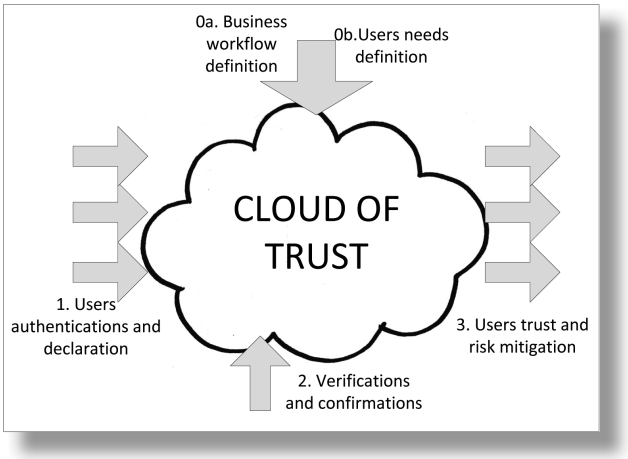
Zmiana modelu zaufania PKI (podpisów statycznych realizowanych za pomocą podpisu na karcie i weryfikowanych certyfikatem) do Chmury Zaufania - czyli usług związanych z zabezpieczeniem transakcji biznesowych wymaga rozszerzenia wachlarza zabezpieczeń oferowanych przez ten model. Będą to zabezpieczenia oparte na dotychczasowych mechanizmach uwierzytelnienia, dowodach z przebiegu procesu biznesowego, potwierdzenia czasu i miejsca, potwierdzania nadania i doręczenia, zabezpieczenia integralności kolejnych wersji dokumentów i zapisy rejestrów zdarzeń. Ważną cechą wyróżniającą to podejście jest fakt, że całość schematu rozszerza zbiór zabezpieczeń opartych o posiadaną wiedzę, biometrię i urządzenia, o nowe zabezpieczenia oparte o proces biznesowy i zespół cech dostosowanych do ryzyka danego procesu biznesowego.

Chmura Zaufania

Chmura Zaufania (Cloud of Trust) stanowi kompleksowy zbiór usług zabezpieczenia transakcji biznesowych, dostarcza mechanizmy podpisu elektronicznego i zaufanie do wszystkich usług składowych. Chmura stanowiąc zwarty model zaufania wobec poszczególnych usług w niej zawartych daje możliwość elastycznego ich dostosowania do potrzeb procesów biznesowych i indywidualnych potrzeb uczestników tych procesów.

Przykładem procesu biznesowego dla którego ma zastosowanie modelu Chmury Zaufania jest podpisywanie umowy o pracę, przy następujących założeniach:

- proces związany z podpisaniem umowy określony jest przepisami prawa i praktyką dostarczającego go podmiotu – np. biura pośrednictwa pracy;
- jednym z uczestników takiego procesu jest przyszły pracodawca, który potrzebuje umowy o pracę aby mieć podstawę do określenia wymagań wobec pracownika;



Rysunek. 1 - *Chmura Zaufania (Cloud of Trust)*

- drugim z uczestników jest pracownik, który potrzebuje mieć pewność otrzymania wynagrodzenia za realizowaną pracę;
- ostatnim uczestnikiem jest biuro pośrednictwa pracy, którego celem jest otrzymanie wynagrodzenie za doprowadzanie do podpisania takiej umowy.

Zadaniem Chmury Zaufania (rys. 1) tym zmniejszenie poziomu ryzyka i wymagań prawa dla wszystkich uczestników obsługiwanych przez nią procesów biznesowych. Chmura Zaufania działa w oparciu o określony proces biznesowy (0a) i określone wymagania uczestników tego procesu (0b). W ramach realizowanego przez chmurę procesu następuje zebranie wymaganych poświadczeń i zobowiązań (1), ich weryfikacja (2) i dostarczenie potwierdzeń wiarygodności (3).

Usługi w Chmurze Zaufania

Podstawą budowy chmury zaufania jest usługa zaufania (Trust Service), będąca brokerem usług zaufania, dostarczająca dwóch rodzajów usług:

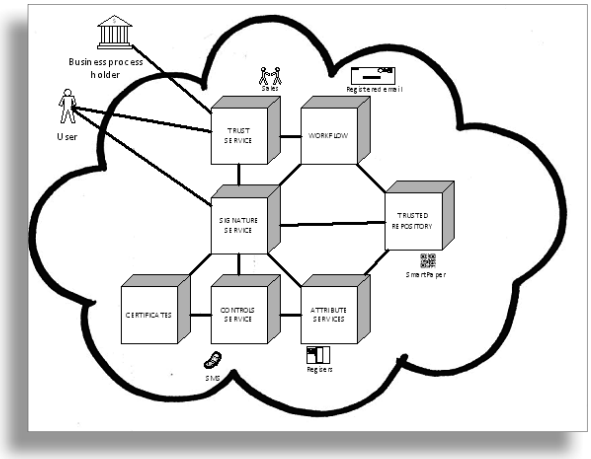
- Usług podpisywania - dostarczenia zabezpieczeń dla powstających dokumentów
- Usług realizacji procesu biznesowego – dostarczająca dowodów z przeprowadzonej procedury

Rolą Trust Service jest agregowanie w jednym miejscu różnych usług podpisywania i obsługi procesów biznesowych, oraz wymiana zaufania z innymi usługami Trust Service.

Poza usługami podstawowymi wymienionymi powyżej chmura zaufania składa się z:

- Usług certyfikacyjnych (Certificate Services) – obejmujących dostarczenie certyfikatów, zarządzanie ich cyklem życia.
- Usług zabezpieczeń (Controls Services) – zapewniających różnego rodzaju potwierdzenia i zabezpieczenia głównie dla usług podpisywania.
- Usług poświadczeń (Attribute Services) – dostarczających do procesów biznesowych poświadczeń wymaganych dla realizacji tych procesów.
- Usług zaufanych repozytoriów (Trusted Repository) – przechowujących i udostępniających dowody ze zrealizowanych procesów biznesowych.

Wszystkie usługi stanowiące chmurę zaufania łączą się miedzy sobą, dostarczając w realizowanych procesach materiał dowodowy oczekiwany do spełnienia celu biznesowego poszczególnych uczestników.



Rysunek. 2 *Usługi w Chmurze Zaufania*

Zestawienie usług zaufania w ramach pojedynczej chmury zaufania wraz z najważniejszymi powiązaniami zaprezentowano na rysunku 2. W ramach pojedynczej chmury zaufania może wchodzić wiele usług zaufania dostarczających różnego rodzaju dowodów i zabezpieczeń dla realizowanych przez chmurę procesów biznesowych, natomiast w ramach pojedynczej chmury powiązane ze sobą usługi zaufania uznają wzajemnie swoja wiarygodność i mają ustalone wzajemne relacje odpowiedzialności rzetelności tych usług. Gwarantem zaufania wobec poszczególnych komponentów wchodzących w skład pojedynczej Chmury Zaufania jest Trusted Service – będące interfejsem i głównym miejscem zaufania dla odbiorców.

Usługa podpisu

Usługa podpisu dostarcza zabezpieczenia i poświadczenia dla dokumentów elektronicznych. W każdym procesie biznesowym powstają dokumenty stanowiące materiał dowodowy związany z danym procesem biznesowym. Dokumenty te w zależności od ryzyka uczestników procesu muszą mieć odpowiednie zabezpieczenia i dostarczać oczekiwane przez użytkowników informacje. Aby zrozumieć znaczenie dokumentów z procesu biznesowego należy patrzeć na nie w kontekście ewentualnego sporu sądowego, w którym strony będą próbowały wyprzeć się swoich zobowiązań, lub wskazać, że przekazane im informacje były niepełne lub niezgodne ze stanem faktycznym.

Zadaniem usługi podpisu jest dostarczenie narzędzi umożliwiających złożenie oświadczenia woli przez uczestnika procesu biznesowego i przedstawienie w nim oczekiwanych przez drugą stronę poświadczeń związanych z tym oświadczeniem woli. Dla przykładu jeżeli dla realizacji oświadczenia woli wymagane jest potwierdzenie danych osobowych to zadaniem usługi podpisu jest zebranie tych danych, tak aby podpisywane oświadczenie zawierało dane niezbędne dla jego wiarygodności. Usługa podpisu dla realizacji potwierdzeń wykorzystuje usługi poświadczeń (Attribute Services) opisane w dalszej części opracowania.

Składanie oświadczenia woli i potwierdzanie dokumentów jest czynnością generującą ryzyko dla podpisującego, dlatego też konieczne jest dostarczenie odpowiednich zabezpieczeń dla realizacji tego procesu. Zabezpieczenia te powinny być dostosowane do rodzaju zobowiązania, wartości transakcji i ryzyka związanego z dochodzeniem zobowiązań. Ze względu na fakt, że podpisujący składa różnego rodzaju oświadczenia woli, ale także podpisuje

dokumenty o znacznie mniejszym znaczeniu, zabezpieczenia każdego rodzaju powinny umożliwiać elastyczne dostosowanie do potrzeb. Przykładem zabezpieczenia może być zastosowanie hasła jednorazowego dostarczanego kanałem SMS w procesie podpisywania. Za dostarczenie różnego rodzaju zabezpieczeń na potrzeby Usługi Podpisu odpowiedzialne są Usługi Zabezpieczeń (Controls Services).

Model usług podpisu, usług zabezpieczeń i usług potwierdzeń został opisany w pracach [10,11].

Zadaniem usługi podpisu jest zapewnienie bezpiecznego procesu podpisywania dokumentu, w ramach którego do podpisu włączone zostają niezbędne poświadczenia oraz zastosowane wymagane zabezpieczenia. Zaufana usługa podpisu zmniejsza ryzyko:

- po stronie podpisującego – poprzez dostarczenie narzędzi, których zabezpieczenia uniemożliwiają złożenie oświadczenia w sposób niekontrolowany i zapewniając że stronie ufającej zostaną udostępnione tylko te dane, poświadczenia i zobowiązania, które świadomie podpisujący potwierdzi,
- po stronie ufającego – poprzez dostarczenie mu wymaganych procesem biznesowym poświadczeń, powstałych w procesie podpisywania i weryfikację istotnych elementów związanych z danym poświadczeniem.

Usługi podpisu mogą wykorzystywać dotychczasowe mechanizmy podpisu oparte o certyfikat X.509 [12] wraz z Podpisem Kwalifikowanym, usługi podpisu serwerowego lub pieczęci serwerowej [13,14], a także usługi PKI 2.0 Lightweight Certificate Signature[10,11].

Usługa workflow

Celem usług dostarczanych w ramach Chmury Zaufania jest taka obsługa procesów biznesowych, aby zapewnić wszystkim uczestnikom tych procesów realizację ich oczekiwań w zakresie bezpieczeństwa dowodowego przeprowadzonego procesu (Safety Target) i minimalizacje związanego nim ryzyka (Risk Mitigation).

Ilustracją zaufanych usług obsługi procesów (workflow) jest proces podpisywania kontraktu między dwoma podmiotami. W procesie podpisywania kontraktu wymieniane są dokumenty pomiędzy stronami tego kontraktu, treść tych umów podlega wzajemnej weryfikacji, a potwierdzenia z ich przekazywania i doręczenia stanowią równorzędny materiał dowodowy co same podpisy pod kontraktem. Najczęstszym powodem spraw sądowych nie jest zaprzeczenie wobec kontraktu, a rozumienie jego poszczególnych zapisów rozumiane jako intencje stron, które podlegały ustaleniom w procesie negocjacji kontraktu. Zaufane usługi obsługi procesu biznesowego (Trusted Workflow Services) mają za zadanie obsłużyć cały proces biznesowy, zebrać dowody z tego procesu, tak aby stanowiły one zabezpieczenie dla wszystkich stron i mogły służyć w ewentualnym procesie sądowym.

Jednym z najważniejszych elementów procesu biznesowego jest wymiana dokumentów pomiędzy jego uczestnikami. Zadaniem zaufanej usługi jest zapewnienie wysłania, przekazania, doręczenia i odebrania dokumentów, z zapewnieniem ich autentyczności i integralności, a także zapewnienie uwierzytelnienia stron procesu. W przypadku procesów biznesowych, w których zbieranych jest wiele dokumentów usługi workflow odpowiedzialne są za ich skompletowanie, a w przypadku gdy proces biznesowy wymaga synchronizacji działań usługi workflow kontrolują czas i nadzorują właściwą kolejność doręczeń i weryfikacji. Szczególnym przypadkiem zaufanych usług obsługi procesów biznesowych są usługi Registred Email [15] zapewniające obsługę procesu nadawania i doręczania korespondencji.

Repozytorium dokumentów

Usługi zaufania wymagają w procesie dokumentów, których autentyczność i integralność jest zapewniona, a także wytwarzają dokumenty, które będą stanowiły wynik cząstkowy lub całościowy przeprowadzonego procesu biznesowego. Zadaniem repozytoriów dokumentów jest zapewnienie przechowywania i udostępniania dokumentów zebranych i powstałych w procesach dowodowych, tak aby zapewnić ich wartość dowodową w zakładanym czasie, a w szczególnych przypadkach wieczyście. Chmura zaufania może korzystać z jednej lub wielu usług repozytoriów dokumentów realizujących różne zadania,

- Zapewnienie bezpieczeństwa repozytorium należy rozumieć jako:
- Zapewnienie dostępności znajdujących się w nim dokumentów – tak aby uprawnieni uczestnicy procesów mieli dostęp do dokumentów w nich zawartych.
- Zapewnienie poufności dokumentów, tak aby osoby, które nie są uprawnione do dostępu do dokumentów, nie miały możliwości ich użycia.
- Zapewnienia integralności i autentyczności dokumentów, tak aby każdy dokument mógł posłużyć jako materiał dowodowy i stanowił podstawę zaufania stron. W szczególności bardzo ważnym elementem jest zapewnienie mechanizmów gwarantujących, że umieszczony w nich materiał dowodowy nie utraci mocy dowodowej z powodów technicznych, np. w sytuacji gdy metody kryptograficzne i certyfikaty tracą swoje właściwości dowodowe.

Formaty dokumentów i ich zabezpieczenia są różne w zależności od potrzeb i systemów teleinformatycznych będących zarówno ich producentami jak i odbiorcami. Zadaniem repozytorium jest udostępnianie dokumentów w formatach i z zabezpieczeniami wymaganymi przez ich odbiorców, z jednoczesnym zachowaniem dowodów i zabezpieczeń z którymi zostały utworzone. Szczególną formą udostępniania dokumentów elektronicznych może być ich postać drukowalna [16], gdzie zawarty na wydruku identyfikator dokumentu w repozytorium umożliwia pobranie dokumentu źródłowego.

Repozytoria dokumentów stanowią także ważny element dostępności wyników usług Chmury Zaufania dla odbiorców zewnętrznych, ponieważ umożliwiają otrzymanie rezultatu przeprowadzonego procesu biznesowego przez odbiorców zewnętrznych – np. adresatów zobowiązań, w tym sądy i administrację publiczną. Dokumenty takie udostępniane są bez konieczności dodatkowego uwierzytelnienia na podstawie unikalnego i poufnego identyfikatora, a warunki dostępności mogą wyłączać możliwość nawet uprawnionego usunięcia takiego dokumentu z repozytorium.

Usługi poświadczeń i zabezpieczeń

Elastyczność mechanizmów zabezpieczeń i gradacji ryzyka w ramach chmury zaufania realizowana jest przez usługi poświadczeń (Attribute services) i zabezpieczeń (Controls Services). Usługi poświadczeń dostarczają do procesów biznesowych i podpisywanych dokumentów wymaganych przez nie informacji. W szczególności poświadczenia mogą zawierać następujące informacje dotyczące podpisującego lub uczestnika procesu biznesowego:

- potwierdzenia tożsamości płynące z różnych źródeł:
  - urzędowo potwierdzona tożsamość (np. profil zaufany),
  - potwierdzona przez bank,
  - potwierdzona przez pracodawcę,
- potwierdzenia kanału komunikacyjnego (email, telefon, adres korespondencyjny),
- potwierdzenia miejsca,
- potwierdzenia zastosowania szczególnych zabezpieczeń w procesie podpisywania,
- potwierdzenia wykupienia szczególnej usługi (ubezpieczenia),
- potwierdzenia dotyczące specjalnego zobowiązania np. gwarantowanej kwoty transakcji,

- potwierdzenia realizacji procedury lub procesu (np. zgodnie z ustalonym pełnomocnictwem w korporacji),
- potwierdzenia pochodzące z systemów zewnętrznych (banki, rejestry),
- potwierdzenia atrybutów podpisu elektronicznego (np. niezaprzeczalność, autentyczność).

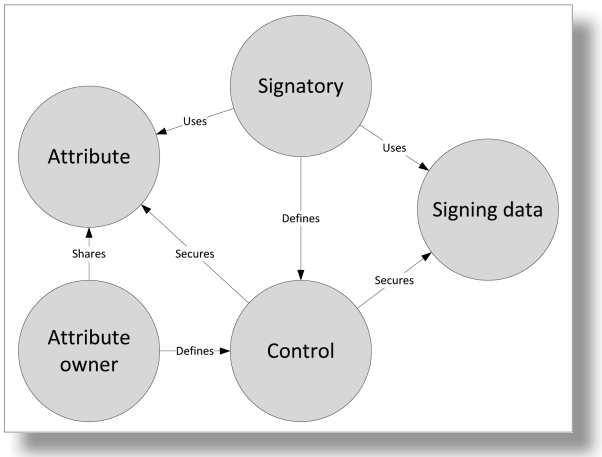
Użycie poszczególnych poświadczeń wymaga ustanowienia dla każdego z nich ustalonych zabezpieczeń, tak aby posłużenie się poszczególnymi poświadczeniami i kluczami było zależne od spełnienia wymagań zdefiniowanych w każdym zabezpieczeniu. Katalog zabezpieczeń jest otwarty poniżej pokazano kilka przykładów z nich:

- mechanizmy uwierzytelnienia (hasło, karta),
- mechanizmy haseł jednorazowych,
- mechanizmy autoryzacyjne od dostawców poświadczeń (np. z banku),
- mechanizmy synchronizacji,
- mechanizmy ograniczeń zdefiniowanych przez użytkownika (czas, miejsce, zakres),
- mechanizmy zależne od realizacji procesu biznesowego (autoryzacja dynamiczna).

Usługi podpisu

Usługi zabezpieczeń i usługi poświadczeń dostarczają bezpośrednio mechanizmów wspierających tworzenie podpisu elektronicznego. Usługi podpisu umożliwiają utworzenie podpisu spełniającego oczekiwane kryteria zaufania (np. zawartość potwierdzonych danych). Jeżeli podpis jest realizowany technikami asymetrycznymi usługi podpisu mogą kontrolować użycie danych służących do składania podpisu realizując go w oparciu o systemy zarządzania kluczami, systemy zarządzania kartami [17] lub podpis z mediatorem [18]. Użycie zarówno kluczy jak i wykorzystanie poświadczeń jest zależne od zabezpieczeń zdefiniowanych przez podpisującego lub przez dostawców i właścicieli poświadczeń. Szczególnym przypadkiem dostarczyciela poświadczeń jest sam podpisujący, który definiuje szczegółowe rodzaje zobowiązań oraz zasady ich zabezpieczania. Przykładem tego rodzaju poświadczeń mogą być graniczne kwoty zobowiązań dopuszczone przez podpisującego i wymagane dla tych kwot zabezpieczenia.

Poniższy rysunek prezentuje wzajemne zależności poświadczeń, zabezpieczeń, danych służących do podpisywania w realizacji usług podpisu elektronicznego.



Rysunek. 3 *Wzajemne zależności elementów usługi podpisu elektronicznego*

Podsumowanie

Chmura Zaufania jest opisem mechanizmów podpisu elektronicznego zorientowanego na usługi świadczone w Internecie, z uwzględnieniem potrzeb poszczególnych procesów biznesowych. Warunki bezpieczeństwa usług realizowanych w oparciu o chmurę są definiowalne i zależne od ryzyka, a zaufanie może być realizowane na poziomie zaufania do całej chmury lub poszczególnych jej usług. Niniejsze opracowanie nie definiuje mechanizmów technologicznych dotyczących realizacji Chmury Zaufania, ale wskazane w bibliografii opracowania pozwalają na jej zbudowanie.

Prezentowane w projekcie rozporządzenia UE [19] wzmocnienie różnorodnych usług zaufania daje przestrzeń do realizacji ww. rozwiązania nie tylko w warstwie technicznej, ale także w warstwie formalnej opisanej przepisami Unii Europejskiej.

Bibliografia

1. Dyrektywa 1999/93/EC Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie Wspólnotowej struktury dla elektronicznych podpisów.
2. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym Dz.U. 01.130.1450
3. Michał Tabor, P o s z u k i w a n y ! ! ! Użytkownik podpisu elektronicznego, Czas informacji 4(12) 2012
4. Strona projektu eDeklaracje, http://e-deklaracje.gov.pl
5. Strona platformy usług elektronicznych Zakładu Ubezpieczeń Społecznych http://pue.zus.pl
6. Strona Elektroniczne Postępowanie Upominawcze - http://www.e-sad.gov.pl
7. Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, Dz.U.2010.40.230
8. Michał Tabor, Daniel Wachnik, Dokumentacja modelu Zaufanego Profilu ePUAP, Trusted Information Consulting 2009
9. Strona portalu ePUAP – http://epuap.gov.pl
10. PKI 2.0 Lżejszy certyfikat podpisu elektronicznego, Polskie Karty, Almanach 2011, http://www.pki2.eu/
11. P.Kubiak, L.Krzywiecki, M.Kutylowski, M.Tabor, D.Wachnik, Lightweight Certifcates- Towards a Practical Model for PKI (BIS) 2012 , LNBIP 117, (Springer Verlag 2012),
12. RFC5820, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
13. Asokan, N., Tsudik, G., Waidner, M.: Server-supported signatures. J. Computer Security (1996)
14. Perrin, T., Burns, L., Moreh, J., Olkin, T.: Delegated cryptography, online trusted parties, and PKI
15. ETSI TR 102 605 V1.1.1 (2007-09) Technical Report Electronic Signatures and Infrastructures (ESI); Registered E-Mail
16. Michał Tabor, Jak inteligentnie wykorzystać papier do informatyzacji procesów, Czas informacji 1(13), 2013
17. e-Gov 2.0 - Towards a sustainable society, http://www.gemalto.com
18. P.Kubiak, M.Kutylowski, A.Lauks-Dutka, M.Tabor, Mediated Signatures - Towards Undeniability of Digital Data in Technical and Legal Framework, LNBIP 57, (Springer Verlag 2010),
19. Projekt Rozporządzenia Parlamentu Europejskiego I Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, COM(2012) 238

Abstract

The needs of the commercial market in the field of digital processing, are much larger than those provided by most tools. Economic growth enforces business processes to be easier and faster with the use of the Internet. The electronic signature as a way to secure

only the document and not the whole digital service will not meet the demands of the market. The newly implemented electronic signature must provide security mechanisms for all business processes. This paper provides a general overview of Cloud of Trust - a framework for providing security services for a variety of electronic transactions.

Michał Tabor - ekspert w dziedzinie podpisu elektronicznego i zarządzania bezpieczeństwem informacji, autor rozwiązania składania deklaracji PIT bez podpisu, autor koncepcji profilu zaufanego ePUAP. Dyrektor ds. operacyjnych Trusted Information Consulting sp. z o.o.

Zapraszamy do udziału

SEMINARIUM

XXII edycja seminarium w cyklu GIS W PRAKTYCE - MAPY CYFROWE W ADMINISTRACJI. REALIZACJA INSPIRE W POLSCE

3 września 2013r. | Warszawa

Zapraszamy Państwa do udziału w seminarium w cyklu GIS W PRAKTYCE, którego tematem przewodnim będą mapy cyfrowe w administracji. Podczas tego wydarzenia zaproszeni specjaliści omówią między innymi takie zagadnienia, jak możliwości wykorzystania map cyfrowych w planowaniu przestrzennym, ochronie środowiska oraz w działalności służb komunalnych. Przybliżą prawne aspekty standaryzacji danych przestrzennych, a także omówią zagadnienia dotyczące wdrażania dyrektywy INSPIRE w Polsce.
Prowadzenie obrad: Janusz Dygaszewicz

W PROGRAMIE

- Realizacja unijnej dyrektywy INSPIRE w Polsce. Wykorzystanie GIS w urzędach państwowych i samorządowych.
  Maciej Rossa (Dyrektor Departamentu Generalna Dyrekcja Ochrony Środowiska)
- Możliwości wykorzystania map cyfrowych w planowaniu przestrzennym, ochronie środowiska, działalności służb komunalnych
  dr inż. Waldemar Izdebski (Politechnika Warszawska)
- **Łączenie danych statystycznych z informacją geograficzną a gospodarowanie przestrzenią w administracji publicznej**
  Janusz Dygaszewicz (Główny Urząd Statystyczny)
- Wdrażanie dyrektywy INSPIRE w administracji publicznej a jakość usług i efektywność działania
  Agnieszka Nowakowska (Główny Urząd Statystyczny)
- Prawne aspekty standaryzacji danych przestrzennych
  dr Anna Fogel (Instytut Gospodarki Przestrzennej i Mieszkalnictwa w Warszawie)
- Infrastruktura INSPIRE w zakresie WEB-GIS i WEB-Mapping
  dr hab. Janusz Michalak (Uniwersytet Warszawski, Wydział Geologii)

Więcej informacji: **www.cpi.com.pl**

(Nie tylko) dziura w jezdni, czyli o „inteligencji" rzeczy martwych

Mieczysław T. Starkowski

Jest potrzeba – teleinformatyka powinna proponować rozwiązanie. I tak się dzieje coraz częściej. Od tego nie ma odwrotu. W ten sposób dążymy do realizacji idei smarter cities. Choć naturalnie trzeba przy tym pokonać na ogół poważne bariery psychologiczne.

W ostatnich latach zapanowała moda na smart (*inteligencję* przedmiotów). Wszystko dookoła nas ma być smart: komputery, telefony, a od pewnego czasu całe miasta. Naturalnie każdy z nas chciałby żyć w takim inteligentnym mieście, czyli korzystać z takich rozwiązań dla administracji publicznej, żeby było wygodnie, a więc praktycznie – żeby żyło nam się lepiej. Jak się zatem przejawia inteligencja takiego miasta?

- Przykładów mamy już sporo – mówi Marzena Fuksa-Łazarska z IBM Polska, odpowiedzialna za rozwój strategii smarter cities w małopolsce. Choćby monitory na przystankach wyświetlające informacje, o której godzinie przyjedzie tramwaj czy autobus. Zakładając czujniki w określonych miejscach możemy lokalizować taki pojazd i wiemy, za ile minut będzie na danym przystanku. To jest jeden z prostych etapów tworzenia inteligentnego miasta. Ale przecież z takich prostych rzeczy składa się nasza codzienność.

Niestety, w naszym kraju mamy jeszcze sporo do zrobienia. W Warszawie od wielu lat jest taki projekt, ale ciągle nie jest dopracowany i nie działa precyzyjnie.

- W Warszawie i Krakowie nie są to projekty IBM – podkreśla Marzena Fuksa-Łazarska. – Więcej wdrożeń naszych systemów mamy na świecie, przede wszystkim w Stanach Zjednoczonych, Chinach i Indiach. Tam te produkty są już bardzo rozwinięte.

Jeżeli chodzi o funkcjonowanie miasta, do najlepiej znanych i popularnych już rozwiązań należą te związane z bezpieczeństwem. Przede wszystkim kamery, czyli miejski monitoring wizyjny. Oprogramowanie IBM daje władzom miast pomocne narzędzie w tym zakresie.

Kamery mogą między innymi obserwować ruch ludzi i pojazdów. Oczywiście wszyscy zdają sobie sprawę, jak duże budzi to kontrowersje. Ale przecież naruszenie prywatności następuje w imię naszego bezpieczeństwa, argumentują zwolennicy takich rozwiązań.

Wyobraźmy sobie taką sytuację. Człowiek z teczką wchodzi do metra, siada na ławce, kładzie teczkę na podłodze, po czym wstaje i odjeżdża (już bez teczki). Naturalnie w mieście (w tym również w metrze) jest system monitoringu, czyli na stacjach jest mnóstwo kamer, a więc i monitorów w centrum dowodzenia. Ale może się zdarzyć, że osoby obserwujące tego nie zauważą. Natomiast wychwyci to oprogramowanie. Zwróci uwagę właśnie na to, że człowiek wszedł z teczką, a odjechał bez niej. Jest bowiem zaprojektowane na wychwytywanie takich różnic. Dlatego samo zagląda do nagrań wstecz, śledzi obraz z wielu kamer aż do miejsca, gdzie została pozostawiona teczka. Po czym,

jeżeli ją zlokalizuje, daje sygnał alarmowy do służb, że w tym miejscu jest potencjalnie niebezpieczny przedmiot, którym trzeba się zająć.

Monitoring może wiązać się też z bezpieczeństwem ruchu drogowego w mieście. W tym przypadku system *rozpoznaje* wypadek i alarmuje. Człowiek nie musi dzwonić, następuje automatyczne powiadomienie, gdy pojawia się niebezpieczeństwo.

Istnieje również aplikacja IBM informująca o zalecanych objazdach. Na przykład jeśli zdarzy się wypadek i droga jest zablokowana, to na tablicach umieszczonych na pobliskich skrzyżowaniach pojawia się informacja, że w tym miejscu jest korek i trzeba dalej udać się alternatywną drogą.

Oczywiście nie są to produkty z pudełka. Przeciwnie, chodzi o zaawansowane indywidualne rozwiązania, które dostosowuje do konkretnych potrzeb danego miasta. Zdaniem Marzeny Fuksa-Łazarskiej bardzo dobrym przykładem takiego dostosowania rozwiązań jest Kraków.

Nikogo nie trzeba przekonywać, jak denerwująca jest dla mieszkańców dziura w jezdni i długi czas jej naprawy. Typowa sytuacja: pojawiają się ubytki, brakuje informacji, nie wiadomo, kto ma je lokalizować, czy ma jeździć jakaś inspekcja po drogach i tak dalej. Jest to oczywiście związane z kosztami zatrudnienia pracowników.

Dla krakowskiego Zakładu Infrastruktury Komunalnej i Transportu wymyślono zatem sposób nietypowy, ale bardzo prosty. Chodzi o wykorzystanie zaangażowania najbardziej zainteresowanych, czyli mieszkańców. To przecież oni cały czas poruszają się po tych drogach i im najbardziej zależy, by nie niszczyć swoich samochodów, by jeździło się szybko i sprawnie.

Powstało zatem oprogramowanie pozwalające na zgłoszenia powstałych ubytków, ich lokalizowanie, a tym samym usprawnienie procesu naprawy. Po zgłoszeniu do systemu, że w jezdni zrobiła się dziura, informacja o niej jest od razu przesyłana w odpowiednie miejsce i następuje zlecenie naprawy. Na pierwszy rzut oka wydaje się to oczywiste, a jednak nie wszędzie funkcjonuje to tak dobrze i w niewielu miastach – w systemie elektronicznym.

Dziurę w jezdni w Krakowie można zgłosić na kilka sposobów. Najłatwiejsza metoda to zrobienie zdjęcia telefonem komórkowym i za jego pośrednictwem wysłanie go do systemu. Oprogramowanie samo lokalizuje ubytek, bo system określa i przekazuje współrzędne geograficzne. Rozwiązanie to ma dodatkową zaletę: jeżeli kilka osób prześle zdjęcie tego samego miejsca, oprogramowanie zidentyfikuje je i prześle dalej do systemu tylko jedno zgłoszenie, a nie kilka.

Zdjęcie może być wysłane *anonimowo* (z niezidentyfikowanego numeru). Jeżeli natomiast zgłaszający chce się ujawnić (udostępniając swój numer telefonu lub adres mailowy, po naprawie tego ubytku dostaje informację zwrotną. Daje to poczucie sensu takiego działania.

To drobna aplikacja, ale ważna. Myślę, że tych zgłoszeń będzie coraz więcej. To jest jeden z dowodów na to, że nasze oprogramowanie jest używane do stworzenia aplikacji, która pomaga miastu i mieszkańcom, uważa Marzena Fuksa-Łazarska.

Ta aplikacja powstała dla Krakowa. Później weszła ona do portfolio IBM. Obecnie sprzedaje się ją na całym świecie. Oczywiście nie jest ona zawsze identyczna, ale dopasowana do potrzeb danego miasta.

Kraków docenia takie rozwiązania, dążąc stopniowo do tworzenia smarter city. Urząd Miasta rozpoznaje nowe potrzeby i odpowiada na nie. W ubiegłym roku powstało kilka propozycji.

- W jednostkach podległych Urzędowi Miasta odbyły się „burze mózgów" i narodziło się wiele ciekawych pomysłów – podkreśla Marzena Fuksa-Łazarska. – Urząd wybrał sześć spośród nich i wysłał do potencjalnych dostawców zapytanie o możliwość stworzenia odpowiednich programów oraz koszt ich wykonania.

Wybrano do realizacji kilka z nich, obecnie czekamy na ich wdrożenia.

Wiele ciekawych rozwiązań powstało na całym świecie. Na przykład w Nowym Jorku osoba niepełnosprawna lub osoba z wózkiem może wejść na dedykowaną stronę internetową, gdy potrzebuje dojechać z określonego punktu do innego, o konkretnej godzinie. Serwis ten pokazuje najkrótsze lub najszybsze połączenia. Oprogramowanie odnajduje miejsca sprzyjające podróży wózkiem inwalidzkim albo wózkiem dziecięcym. Pokazuje, gdzie jest dobry zjazd z danej drogi z krawężnika i o której godzinie jedzie autobus niskopodłogowy. Program łączy te wszystkie informacje i pokazuje, w jaki sposób można dotrzeć z punktu A do B, między innymi rysując na mapie, którą stroną chodnika trzeba jechać.

Oczywiście wiąże się to z wieloma uwarunkowaniami. Przede wszystkim potrzebne są precyzyjne dane o rozkładzie jazdy oraz typie taboru. Niezbędne są informacje o topografii chodników przyjaznych osobom podróżującym na wózkach oraz z wózkami. W naszym kraju trudno to sobie ciągle wyobrazić. Zaczęło się już coś dziać z myślą o rowerzystach, ale na razie nie ma chyba jeszcze map z zaznaczonymi zjazdami z chodników.

Wiąże się z tym kolejna możliwość wykorzystania kamer systemu monitoringu wizyjnego. Stosując oprogramowanie IBM, można ich użyć do liczenia przechodniów, rowerzystów, samochodów, a więc operator systemu jest w stanie powiedzieć, jakie są potrzeby drogowe, w tym co do tworzenia ścieżek rowerowych. Tę tendencję widać już w wielu miastach. Kładzie się duży nacisk, by zlikwidować korki, zachęcając kierowców, by przesiadali się na rowery. W tym celu trzeba budować ścieżki rowerowe, ponieważ wiele osób ma obawy przed poruszaniem się jezdniami.

Jednym ze wspomniamych kilku projektów zatwierdzonych do realizacji w Krakowie jest oprogramowanie obsługujące proces zamiany mieszkań komunalnych. Pojawia się pytanie: ile jest mieszkań komunalnych do zamiany? Okazuje się, że sporo, program całkiem dobrze funkcjonuje, a Kraków dużo na tym zaoszczędził.

Załóżmy, że rodzina ma duże mieszkanie komunalne, a nie radzi sobie z opłatami za nie. Może zatem zarejestrować się w takim portalu i poszukać sobie mniejszego mieszkania – również komunalnego i zamienić na mniejsze, z niższym czynszem. Z drugiej strony rodzina, która ma mniejsze mieszkanie komunalne, a większe potrzeby metrażowe, może przejąć to większe mieszkanie, spłacając dług poprzednich lokatorów. Dochodzi do wymiany mieszkań, obie rodziny są zadowolone, a miasto dostaje zwrot zadłużenia.

Niesłychanie istotną rzeczą w dużych miastach jest bezpieczeństwo na stadionach. Bardzo ważne jest więc monitorowanie tego bezpieczeństwa, czyli między innymi kontrolowanie liczby kibiców. Jeżeli konkretne wejście jest bardzo zatłoczone, można pozwolić na otwarcie innego wejścia czy po prostu zmienić strumień napływających osób. Jeśli występuje wzrost zagrożenia w jednym z obszarów, system sygnalizuje to dyspozytorom.

Kamery potrafią rozpoznawać twarze. Niezwykle pomocny jest przy tym system dostępowy (pisaliśmy o nim w jednym z poprzednich numerów CI). Widzowie posługują się kartami kibica. Gdy ktoś okaże taki dokument przy wejściu, to wiadomo, że wchodzi na stadion i jego twarz jest rejestrowana przez kamerę. Jeśli zatem coś dzieje się później na widowni, kamery nagrywają tę osobę i system od razu jest w stanie podać personalia tej osoby. Nie trzeba czekać tygodni, aż ktoś znajdzie tę osobę po pracowitym przeszukaniu baz papierowych. To jest rzeczywiście system rozpoznawania twarzy, prawdziwej identyfikacji. Łącznie z tym, że system sam podaje personalia poszukiwanych osób.

A jakże istotne w dzisiejszych burzliwych czasach jest monitorowanie wałów przeciwpowodziowych. Czujniki instaluje się w wałach i w ten sposób stale monitorowany jest poziom wody. Jeżeli w danym miejscu wał zostaje osłabiony, system od razu daje znać i można szybko – na bieżąco – reagować, a nie wtedy, gdy gołym okiem już widać, że woda się przelewa. Ten system jest już wykorzystywany w Stanach Zjednoczonych i kilku innych krajach.

Podobny program służy monitorowaniu rowów melioracyjnych. Jeżeli gdzieś występuje blokada, bo na przykład spadło drzewo, to system jest w stanie wychwycić to i przekazać informację odpowiednim służbom. Wiele gmin na świecie wprowadziło takie rozwiązanie. Ono funkcjonuje i jest bardzo opłacalne. Taki system oznacza nie tylko wydatek, ale przede wszystkim oszczędności, podkreśla Marzena F. Łazarska. Wysłanie ekipy w konkretne zagrożone miejsce jest dużo tańsze niż ciągłe kontole podległego obszaru.

Powstała też aplikacja do zarządzania wodą, a konkretnie nawadnianiem parków. W tym przypadku również było sporo wątpliwości, po co takie oprogramowanie. Dominuje powszechna opinia, że *wystarczy* nawadniać. A jednak zastosowanie w jednym z dużych parków amerykańskich pozwoliło na określenie, że monitorowanie zużycia wody daje oszczędności rzędu setek tysięcy dolarów rocznie.

Znamy już w naszym kraju numer 112. System ten może być znacznie rozszerzony (tak jest na przykład w Stanach Zjednoczonych). Dyspozytor wprowadza do systemu dane zdarzenia, a system sam generuje powiadomienia do odpowiednich służb wraz z detalami takimi jak na przykład położenie hydrantu - tak, aby kierowca wozu gaśniczego wiedział, gdzie ma zaparkować.

Ciekawe rozwiązania wdrażane są w placówkach ochrony zdrowia. Rejestrując się w szpitalu pacjent dostaje specjalną opaskę na rękę. Dzięki niej jest lokalizowany, czyli obsługa zawsze wie, gdzie on się znajduje. Podobne opaski ma także personel, ale również urządzenia. Dlatego zawsze można łatwo znaleźć każdego lekarza czy pielęgniarkę oraz sprzęt, który akurat jest potrzebny.

Posiadająca opaskę pielęgniarka wchodząc do sali aktywuje wyświetlenie na monitorze informacji, któremu pacjentowi jaki lek podać. Nie musi mieć przy sobie żadnych dokumentów. Nie zdarza się, że ktoś o tych lekach

zapomni albo komuś pomyli się kolejność. W systemie jest zapisane, któremu pacjentowi o której godzinie co się należy i przypomina o tym sygnał świetlny lub dźwiękowy. W warunkach naszej polskiej publicznej służby zdrowia brzmi to jeszcze pozornie abstrakcyjnie (chodzi oczywiście przede wszystkim o koszty). Ale jeśli policzyć wszystko dokładnie, widać też ogromne korzyści. Dlatego są już wdrożenia w szpitalach prywatnych. Takie rozwiązania są opłacalne ze względów organizacyjnych. Ale nie tylko – po pewnym czasie dają też zwrot nakładów.

Niestety bywają ciągle kłopoty z wprowadzaniem idei smarter cities. Według nieoficjalnych informacji w Katowicach rozmowy na temat różnych rozwiązań trwają już ponad dwa lata (choć podobno ich zakończenie jest coraz bliższe). W rozmowach z władzami miast bardzo często problem polega na ich niechęci do podejmowania ryzyka. Niejednokrotnie prezentują postawę zachowawczą.

Nie wystarcza przekonywanie, że aplikacja odpowiada potrzebom i rozwiąże wiele kłopotów. Niemal zawsze pada sakramentalne pytanie: a kto to już ma w Polsce? Mało kto chce być pionierem. Gdy któraś gmina zrobi już ten pierwszy krok, później jest znacznie prościej rozmawiać z innymi.

Dotychczas łatwiej jest wprowadzać nowatorskie rozwiązania smarter cities w innych krajach, ale będą się one rozpowszechniać na całym świecie, w tym również w Polsce. Od tego nie ma odwrotu – przekonuje Marzena Fuksa-Łazarska.

Niektóre rozwiązania smarter cities

http://www-03.ibm.com/press/us/en/pressrelease/35945.wss

http://www-03.ibm.com/press/us/en/pressrelease/37973.wss

http://www-03.ibm.com/press/us/en/pressrelease/38152.wss

http://www-03.ibm.com/press/us/en/pressrelease/38153.wss

http://www-03.ibm.com/press/us/en/pressrelease/36952.wss

http://www-03.ibm.com/press/us/en/pressrelease/36883.wss

Mieczysław T. Starkowski - jest dziennikarzem. Od wielu lat zajmuje się między innymi szeroko pojętą teleinformatyką.

Zapraszamy do udziału

WARSZTATY

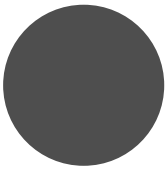
ŚRODOWISKO PRAWNE PROWADZENIA DZIAŁALNOŚCI TELEKOMUNIKACYJNEJ

Warszawa, 28.08.2013

Centrum Promocji Informatyki i Kancelaria Dentons zapraszają na warsztaty poświęcone przyszłości rynku telekomunikacyjnego. Podczas spotkania chcielibyśmy omówić najważniejsze zmiany, które weszły w życie na mocy nowelizacji prawa telekomunikacyjnego. Przedmiotem wykładu będzie zarówno analiza prawna zmian treści prawa, jak i praktyka jego stosowania. Warsztaty będą również doskonałą okazją do wzajemnej wymiany poglądów praktyków rynku telekomunikacyjnego

Więcej informacji: **www.cpi.com.pl**

Informatyzacja mniej lub bardziej zintegrowana



Tomasz Kulisiewicz

Środowisko informatyczne od początku zastosowań komputerów w **naszej administracji publicznej apeluje o stosowanie ich w taki sposób, by** ułatwiać **życie obywatelom i przedsiębiorcom, a przy tym zwiększa**ć **sprawność administracji.**

Warto pamiętać o tej kolejności – zwłaszcza w świetle syndromów obserwowanych od początku informatyzacji administracji publicznej. Trzy najtrudniejsze do zwalczenia zjawiska to:

1. niealgorytmizowalność prawa, polegająca na tym, że przepisy nie odzwierciedlają żadnych logicznych ścieżek procesowych i węzłów decyzyjnych;
2. stosowanie informatyki do XVIII-wiecznego weberowskiego modelu administracji, w której nośnik danych był tożsamy z informacją;
3. budowanie systemów informacyjnych i informatycznych według zasady „bo tak to musi być w komputerze".

Źródeł pierwszego z powyższych zjawisk trzeba szukać bardzo głęboko – w realiach procesu legislacyjnego, niestety nie realizującego modelu **racjonalnego prawodawcy**. Racjonalny prawodawca:

- zanim uchwali ustawę czy przygotuje i podpisze rozporządzenie, najpierw zastanowi się nad tym:
  - czy zjawisko czy problem, który chce regulować przepisem, jest rzeczywiście problemem realnym?
  - czy przypadkiem kwestii nie reguluje już od dawna inny przepis – tyle, że nieprzestrzegany (i dlaczego)?
  - czy koniecznie trzeba wprowadzać przepis? A może sprawę da się rozwiązać dzięki samoregulacji (np. kodeksów dobrych praktyk)?
- jeśli już zdecyduje, że należy przygotować regulację legislacyjną, to:
  - dokona oceny skutków regulacji, przeprowadzając analizę kosztów i korzyści (bo może okaże się, że w bilansie korzyści społecznych wprowadzenie przepisu będzie wszystkich zainteresowanych kosztować dużo więcej, niż przyniesie korzyści), a w jej ramach określi, czy dana regulacja zmniejszy czy zwiększy obciążenia administracyjne (i o ile):
    - przedsiębiorców i obywateli
    - samej administracji
  - określi termin, w którym obowiązkowo dokona oceny skutków wprowadzenia przepisu – nie oczekując, że skutki te przejawią się w 2 dni czy w 2 tygodnie, ale nakreślając racjonalny horyzont czasowy, np. trzyletni, jaki najczęściej widzimy w unijnych dyrektywach, natomiast zakładając, że po takiej ocenie podjęta zostanie decyzja, czy wprowadzony przepis:
    - pozostawić bez zmian, bo się sprawdził,
    - zmodyfikować, bo okazał się nie dość skuteczny lub wywoływał niepożądane skutki uboczne.
    - anulować, bo spełnił swoją rolę albo po pewnym czasie okazał się niepotrzebny (choćby dlatego, że przez ten czas problem sam zniknął, bo zmieniły się warunki, otoczenie gospodarcze lub społeczne).

Jakoś tak się dziwnie składa, że przepisy niealgorytmizowalne powstają wtedy, kiedy pisane są na kolanie, gdyż prawodawca

nieracjonalny działa pod naciskiem tzw. woli politycznej lub „syndromu ugryzionego dziecka". To drugie ironiczne określenie warto wyjaśnić. Z syndromem ugryzionego dziecka mamy do czynienia wtedy, gdy zdaniem prawodawcy natychmiast trzeba uchwalić ustawę, która wykluczy możliwość zaistnienia jakiegoś zdarzenia, o którym dniem i nocą (ale maksymalnie przez 72 godziny) mówią wszyscy politycy biegający z jednego studia telewizyjnego do drugiego, a po drodze wpadający do radia i wypowiadający się dla prasy drukowanej.

Na temat zjawiska nr 2 z powyższej listy, czyli stawiania komputerów zamiast szaf i segregatorów – ale w ich roli – opublikowano m.in. w *Czasie informacji* już wiele artykułów i analiz, więc w tym miejscu tylko przypomnę, że pomieszanie kamiennych tablic, glinianych tabliczek, zwojów papirusu czy kartek formatu A4 wpiętych w segregatory z dostępem do informacji potrzebnej do podejmowania decyzji w procesach zachodzących w administracji publicznej jest jednym z głównych źródeł porażek e-administracji.

Powiązane jest z nim zjawiska nr 3, czyli stosowanie zasady „bo tak musi być w komputerze". Ma ono swoje źródło w nieprawidłowym określeniu potrzeb i przebiegów informacji w procesach potrzebnych do podejmowania i wydawania decyzji administracyjnych. Na samym końcu skrupia się to na interesancie, który musi pracowicie wypełniać formularze z kratkami, w które nic się nie mieści (bo nigdy nie próbował ich wypełnić ten, który je zaprojektował), podając tam informacje, które w danym postępowaniu są albo całkowicie zbędne, albo urząd je już dawno ma u siebie (a najczęściej i jedno, i drugie).

Powyższe zjawiska usiłujemy zwalczać (lub choćby minimalizować ich oddziaływania) na różne sposoby. Jednym z takich sposobów jest planowanie strategii i kierunków informatyzacji administracji – co z lekką emfazą zostało nazwane w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[1] Planem Informatyzacji Państwa. Ustawa wprowadziła porządek koncepcyjny w tworzeniu centralnej strategii informatyzacji administracji – choć odrębną kwestią jest to, jak skutecznie udawało się dotąd wdrażać strategie, wytyczne i ustawowe regulacje. Doświadczenia z dotychczasowymi Planami Informatyzacji Państwa nie były najlepsze – głównie z powodu rozmijania się racjonalności (czy nieracjonalności) prawodawcy ze szczerymi chęciami oraz możliwościami realizacyjnymi jakimi dysponowali autorzy i realizatorzy PIP.

Plan Informatyzacji Państwa

Plan Informatyzacji Państwa miał służyć do realizacji Strategii rozwoju społeczeństwa informacyjnego i według Art. 5. ustawy o informatyzacji był „instrumentem planowania i koordynowania informatyzacji działalności podmiotów publicznych". PIP miał nie tylko określać priorytety rozwoju systemów, koordynować projekty informatyczne realizowane przez więcej niż jeden podmiot publiczny, określać zadania i systemy urzeczywistniające cele Strategii, ale także zawierać oszacowania kosztów projektów i wskazywać źródła ich finansowania. Jednak zakres PIP sięgał też dość głęboko w zagadnienia techniczne, jako że celem PIP miała być też „*modernizacja oraz łączenie systemów teleinformatycznych"* a także zapewnienie warunków bezpieczeństwa i interoperacyjności systemów. W nowelizacjach m.in. „odszczegółowiono" procedury przygotowywania i międzyministerialnego uzgadniania projektów

1 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565)

informatycznych, dodano regulacje dotyczące ePUAP. Rangę PIP miał podnosić fakt, że plan ustanawiany był w drodze rozporządzenia Rady Ministrów. Rangę tę zyskały PIP na rok 2006 a później PIP na lata 2007-2010. Pierwszy PIP można właściwie traktować jako wprawkę – zwarte (13-stronicowe) opracowanie zawierające cele i priorytety ustanowione zostało rozporządzeniem RM z 1 sierpnia 2006 r., które ukazało się dopiero 18 sierpnia, a weszło w życie 2 września. W rezultacie ten pilotowy plan obowiązywał tylko przez 4 miesiące. PIP na lata 2007-2010 też był sformułowany krótko i treściwie: 4 lata zmieściły się na 33 stronach Dziennika Ustaw. Jednak kilka kluczowych przedsięwzięć nakreślonych w tym PIP miało już dużo mniej szczęścia w realizacji – by wspomnieć plany takich projektów jak STAP czyli Sieć Teleinformatyczną Administracji Publicznej, pl.ID czy platformy wspierające ochronę zdrowia. W sejmowym Internetowym Systemie Aktów Prawnych *Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010* ma status „uznany za uchylony" z dniem 17 czerwca 2010 r. co „delikatnie sugeruje", że PIP 2007-2010 z różnych powodów się rozpłynął.

Ministerstwa, komitety, rady, organizacje i inne ciała napracowały się w 2011 r. nad projektem PIP 2011-2015. We wrześniu 2011 r. mogło się wydawać, że obszerny (ponad 90 stron) dokument *(Projekt rozporządzenia Rady Ministrów z 2011 r. w sprawie Planu Informatyzacji Państwa na lata 2011-2015*) jest już bliski oficjalnego zatwierdzenia, jednak lista zastrzeżeń i uwag była bardzo długa. Znamienne, że trzy główne teleinformatyczne organizacje zawodowe, Polska Izba Informatyki i Telekomunikacji, Polskie Towarzystwo Informatyczne oraz Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, mocno skrytykowały projekt PIP zalecając jego odrzucenie w ujęciu proponowanym przez rząd. Wspomniane organizacje miały różne zastrzeżenia do różnych elementów projektu, ale w jednym były całkowicie zgodne – wszystkie trzy zdecydowanie oprotestowały przedstawiony w projekcie pomysł powołania odrębnej agencji rządowej pod nazwą Międzyresortowego Operatora Sieci Teleinformatycznej (MOST). Można odnieść wrażenie, iż strona rządowa wykorzystała reorganizację MSWiA jako resortu zajmującego się od 2005 r. informatyzacją i przejęcie w listopadzie 2011 r. zadań informatyzacji administracji przez Ministerstwo Administracji i Cyfryzacji, jako okazję do wycofania się z krytykowanego projektu i na tym skończyły się Plany Informatyzacji Państwa w ich ustawowej roli i formie.

Nowe gospodarz, nowe podejście

Nowy gospodarz informatyzacyjnego podwórka, Ministerstwo Administracji i Cyfryzacji, próbuje innego podejścia, kontynuując w tej sferze podejście i sposób działania Zespół Doradców Strategicznych Prezesa Rady Ministrów z czasów strategicznych opracowań z lat 2010-2011 i raportu Polska 2030. Podejście takie widoczne jest w przedstawionym w marcu 2013 r. projekcie Programu Zintegrowanej Informatyzacji Państwa (PZIP). Na pierwszy rzut oka widać leksykalną różnicę między „planem" a „programem". Według deklaracji autorów PZIP koncentruje się na budowie mechanizmów mających służyć tworzeniu modelu działania administracji, którego bardzo do tej pory brakowało, a który nazwany został w strategicznych opracowaniach MAiC państwem Optimum 2.0. Deklarowanym celom PZIP można tylko przyklasnąć, bowiem celem programu informatyzacji ma być *„zapewnienie obywatelom i przedsiębiorcom, ale również samej administracji, dostępu do narzędzi użytecznych, bezpiecznych, prostych w stosowaniu, powszechnie dostępnych i neutralnych technologicznie."* Wiele rządów na świecie uczy się obecnie (przeważnie na własnych błędach), że model władcy oświeconego,

który lepiej wie, co potrzebne jest maluczkim, działa coraz gorzej – zresztą dobrze działał chyba tylko w legendach tworzonych przez dworskich bajarzy. Zwykle bowiem władca wpada w samouwielbienie i skutecznie izolując się od rzeczywistości zaczyna popełniać coraz więcej błędów, jako coraz mniej racjonalny prawodawca. Do czasu, kiedy ma zasoby, by maluczkim „zapchać gęby" różnymi dobrami, jeszcze to jakoś działa, ale w dzisiejszym świecie albo zaczyna brakować zasobów do realizacji powszechnej szczęśliwości, albo globalna komunikacja elektroniczna demaskuje wyobrażenia o powszechnej szczęśliwości. Ostatnio nawet demokracja przedstawicielska też coraz słabiej daje sobie radę z wyzwaniami, trzeba więc próbować modelu rozszerzonej partycypacji społeczeństwa. Jak słusznie zauważają autorzy PZIP, w realizacji takiego modelu należy wykorzystywać *„nowe możliwości, jakie pojawiają się w związku z dynamicznym rozwojem technologii cyfrowych oraz rozbudową cyfrowych zasobów i treści"*.

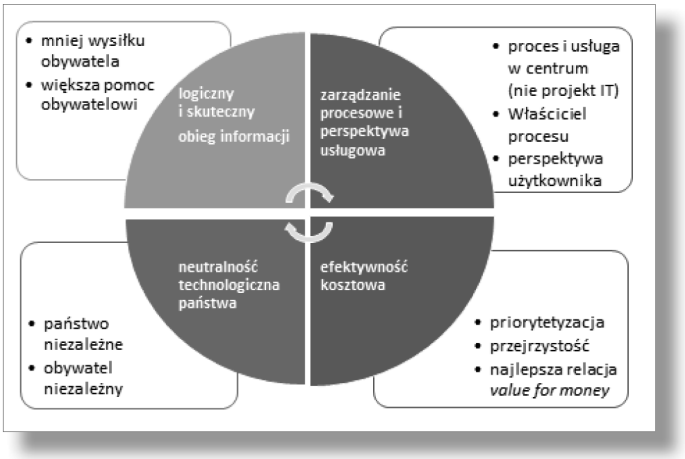
Wydaje się jednak, że w PZIP za bardzo skoncentrowano się na kuszeniu obywateli wygodą załatwiania spraw urzędowych, w tym zupełnie techniczno-administracyjnych, jak np. wspomniane w programie poszukiwanie pracy, czy regulowanie należności. Oczywiście jako były informatyk jestem i zawsze będę chętny do korzystania z usług elektronicznych, dzięki którym będę mógł załatwiać sprawy urzędowe „*niezależnie od miejsca pobytu" (*a zwłaszcza niezależnie od „ulubionego" przeze mnie osobiście miejsca zameldowania). Mniej się entuzjazmuję deklaracjami, że sposób działania elektronicznej administracji powinien być niezależny od „*rodzaju stosowanej technologii służącej do korzystania z sieci"* – bo widziałem już w życiu kilka rewolucyjnych zmian technologii i architektur systemów informacyjnych i wiem, że nie można się zanadto przywiązywać do żadnej z nich, bo zaraz przyjdzie następna.

W PZIP powtórzono za raportem *„Państwo 2.0. Nowy start dla e-administracji"* iż zintegrowana informatyzacja powinna się oprzeć na czterech filarach – logicznym i skutecznym obiegu informacji, koncentracji na procesach administracyjnych a nie na projektach informatycznych, przejrzystości i efektywności wydatkowania środków publicznych oraz neutralności technologicznej (Rys. 1).

Moim zdaniem dwa pierwsze filary są na tyle wyższe od dwóch pozostałych, że podpieranie nimi całej platformy państwa powoduje, iż platforma ta nie będzie stała równo. Dwa pierwsze filary są bowiem powiązane z prawidłową konstrukcją architektury informacyjnej państwa – jak to wskazuje w swoich licznych opracowaniach prof. Andrzej Sobczak[2]. W takim ujęciu w PZIP brakuje zdefiniowania pryncypiów i wizji architektury zintegrowanego systemu informacyjnego państwa. Dopóki brak jest takiej wizji, to nadal będziemy mieli do czynienia z „mało racjonalnym prawodawcą" nie potrafiącym wyzwolić się z pułapki trzech syndromów, które przedstawiłem na początku niniejszego artykułu.

W PZIP przytoczono bardzo ważne sformułowanie dotyczące celów istnienia i działania państwa jako struktury organizacyjnej: *„Państwo optimum powinno dbać o powszechny dostęp do tego, co definiujemy jako sprzyjające rozwojowi dobra publicznego. Dotyczy to takich usług publicznych jak: edukacja, prawo do zabezpieczenia na starość, pomoc na rynku pracy, dostępność (...) powszechnego systemu ochrony*

2 http://architekturakorporacyjna.pl/architektura-korporacyjna-panstwa-vs-modernizacja-panstwa/1384/



Rysunek. 1. *Cztery filary zintegrowanej informatyzacji*
(źródło: Program Zintegrowanej Informatyzacji Państwa – MAiC, marzec 2013, s. 6)

zdrowia". Pytanie, czy nowej wizji państwa szukać trzeba w programie informatyzacji (choćby jak najbardziej zintegrowanej), czy raczej w dokumentach strategicznych mogących spowodować prawdziwą „racjonalizację prawodawcy".

Ironiczne powiedzonko znanego w środowisku informatycznym specjalisty od audytu systemów brzmi: „systemy informatyczne dzielą się na zintegrowane oraz te działające." Jako obywatele trzymajmy kciuki, by dotyczyło to tylko oprogramowania…

Tomasz Kulisiewicz – absolwent informatyki Politechniki Budapeszteńskiej, analityk rynku komunikacji elektronicznej. Kierował panelami badawczymi w Narodowym Programie Foresight Polska 2020, badaniach Foresight Kadr Nowoczesnej Gospodarki i Foresight Akademickie Mazowsze 2030. Współzałożyciel inicjatywy Internet Obywatelski (2001), Stowarzyszenia Komputer w Firmie (2003) oraz Ośrodka Studiów nad Cyfrowym Państwem (2012).

Zapraszamy do udziału

WARSZTATY
NOWELIZACJA PRAWA ZAMÓWIEŃ PUBLICZNYCH
Warszawa, 11.09.2013

Kolejna nowelizacja prawa zamówień publicznych wprowadziła szereg istotnych zmian. Zupełnie nowe zasady udzielania zamówień związanych obronnością i bezpieczeństwem, nowe zasady uczestnictwa w przetargach grup kapitałowych i zaostrzenie przepisów w zakresie wykluczania wykonawców z postępowań o udzielenie zamówienia publicznego, to tylko niektóre z ważnych zagadnień. Warsztat „nowelizacja prawa zamówień publicznych" ma na celu zapoznanie uczestników ze zmienionymi przepisami oraz możliwymi praktycznymi konsekwencjami wprowadzonych zmian.

Więcej informacji: **www.cpi.com.pl**

Trzy oblicza e-administracji w Polsce

Danuta Descours

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[1] nałożyła na jednostki administracji publicznej w Polsce zadanie polegające na umożliwieniu obywatelowi składania dokumentów do urzędów za pośrednictwem internetu, stworzyła podstawę prawną do funkcjonowania elektronicznej administracji (e-administracji). Obowiązek ten zgodnie z ustawą realizowany jest poprzez Elektroniczną Skrzynkę Podawczą (ESP), czyli dostępnego publicznie środka komunikacji elektronicznej służącego do przekazywania informacji w postaci elektronicznej do podmiotu publicznego przy wykorzystaniu powszechnie dostępnej sieci teleinformatycznej. Aby móc skorzystać z tej formy kontaktu obywatela z administracją publiczną, zainteresowana osoba zgodnie z ww. Ustawą musi posiadać bezpieczny podpis elektroniczny (płatny) lub profil zaufany ePUAP, który z kolei jest bezpłatny. Profil zaufany ePUAP funkcjonuje w Polsce od niedawna, bo od 9 czerwca 2011 r., szczegółowe wytyczne dotyczące jego funkcjonowania zostały wprowadzone długo wyczekiwanym Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji[2].

Temat wykorzystania przez użytkowników możliwości jakie daje elektroniczna administracja w Polsce po wejściu w życie wymienionego wyżej Rozporządzenia jest tematem „na czasie". Możliwości jakie daje e-administracji w Polsce oraz sposób jej wykorzystania przez obywateli, pozwalają podzielić wszystkich potencjalnych użytkowników na trzy grupy. Pierwsza grupa to oblicze wyznające następującą zasadę w kontakcie z urzędem „tylko i wyłącznie papier jest dokumentem", druga grupa - „dokument może być złożony elektronicznie, ale odpowiedź muszę mieć papierową, bo tylko taka z podpisami, pieczątkami jest oryginalna", trzecia grupa - „wszystko elektronicznie, szybko i bez konieczności wizyty w urzędzie". Dla potrzeb wykonania obiektywnej analizy zysków oraz strat wynikających z korzystania z elektronicznej administracji, w każdej grupie zostało wykonane to samo zadanie polegające na złożeniu kompletnego wniosku o wydanie zezwolenia na wycięcie drzew lub krzewów.

W celu sprawdzenia ile czasu i energii będzie potrzebne do załatwienia zadanej sprawy w postaci papierowej, wcielam się w rolę reprezentanta grupy pierwszej. Udaję się więc do właściwego co do mojego miejsca zamieszkania urzędu, wychodzę z pracy o godzinie 13:00, aby zdążyć przed jego zamknięciem (będę to później musiała odpracować). Po dotarciu do odpowiedniego budynku, przejściu przez labirynt korytarzy, odsyłana z pokoju do pokoju docieram w końcu do właściwego wydziału i biura. Uzyskuje w nim informację

1 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. 2005 Nr 64, poz. 565 z późn. zm.

2 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej Dz. U. 2011, nr 93, poz. 547.

o sposobie załatwienia sprawy, opłacie jaką należy uiścić oraz pobieram odpowiedni wniosek. Na korytarzu wypełniam wniosek, niestety chcąc go oddać dowiaduję się, że potrzebny jest jeszcze podpis współwłaściciela działki, więc zabieram wniosek do domu. Po zebraniu wszystkich niezbędnych podpisów, znów wychodzę wcześniej z pracy (tym razem o godzinie 14:00), zawożę wniosek do urzędu, po drodze wstępuję jeszcze na pocztę, aby uiścić opłatę skarbową i dołączyć dowód wpłaty do wniosku. No i już wniosek złożony, na kopii wniosku w okienku podawczym otrzymuję pieczątkę wpływu. Teraz wystarczy tylko dzwonić, dopytywać czy jest już decyzja. Podsumowanie: trzy godziny do odrobienia w pracy, dwie wizyty w urzędzie, zmarnowany czas na poszukiwanie odpowiedniego wydziału, miejsca parkingowego, miejsca do wypełnienia wniosku, niepotrzebne nerwy, kolejka na poczcie. Ale po dwóch dniach kompletny wniosek został przyjęty.

W drugiej oraz trzeciej grupie zakładam, iż przed przystąpieniem do złożenia wniosku o wydanie zezwolenia na wycięcie drzew lub krzewów posiadam już skrzynkę kontaktową na platformie regionalnej oraz potwierdzony profil zaufany. Jednakże, aby obiektywnie dokonać analizy korzyści i mankamentów e-usług poniżej opisuję czynności jakie jednorazowo musiałam wykonać wcześniej.

Założenie skrzynki kontaktowej polega na wypełnieniu elektronicznego formularza rejestrującego, konieczności zapoznania się regulaminem platformy, a po założeniu potwierdzenia linka otrzymanego na maila. Wszystkie czynności związane z rejestracją zajęły mi 15 minut. Aby móc podpisywać wnioski od razy założyłam wniosek o profil zaufany. Aby to uczynić w pierwszej kolejności musiałam założyć konto na platformie centralnej www.epuap.gov.pl wypełniając standardowy elektroniczny formularz zgłoszeniowy. Następnie z poziomu założonego konta wysłałam elektroniczny wniosek o profil zaufany. Powyższe czynności zajęły mi kolejne 20 minut. Po złożeniu wniosku w terminie 14 dni, potwierdziłam swój profil (potwierdzenie tożsamości, podpisanie umowy), udając się do najbliższego co do miejsca zamieszkania Urzędu Skarbowego. Ważną z punktu widzenia użytkownika zakładającego profil zaufany jest informacja, iż jest to jedyna wizyta w urzędzie w związku z potwierdzeniem profilu i można samemu wybrać punkt w którym chcemy potwierdzić dane (nie musi to być urząd właściwy, co do miejsca zamieszkania). Oczywiście wcześniej wykonana operacja zakładania konta jest również operacją jednorazową. Po dokonaniu tych formalności mogę już w pełni korzystać z dostępnych e-usług oferowanych na platformie ePUAP (platforma centralna), bądź na platformach regionalnych, które pozwalają na identyfikację użytkownika poprzez profil zaufany (np. Platforma SEKAP w województwie śląskim, Cyfrowy Urząd w województwie warmińsko-mazurskim).

Będąc przedstawicielem grupy drugiej swoje zadanie rozpoczynam od wyszukania w wyszukiwarce internetowej adresu www właściwego urzędu. Na stronie odnajduję link do platformy obsługującej elektroniczne formularze. Wyszukuję rodzaj sprawy, którą chcę załatwić, zapoznaję się z kartą informacyjną sprawy, uzyskując takie informacje jak sposób załatwienia, wymagane dokumenty, opłaty, wydział, numer telefonu, biura. Po zapoznaniu się z kartą dotyczącą załatwianej sprawy loguję się do platformy, wypełniam wcześniej wyszukany elektroniczny wniosek danymi, jednym kliknięciem sprawdzam jego poprawność, opatruję podpisem lub podpisuję profilem zaufanym, wysyłam. Jako formę odbioru dokumentów zaznaczam opcję „pocztą tradycyjną". Po wysłaniu otrzymuję od urzędu do którego wysłałam tak zwane UPO czyli Urzędowe Poświadczenie Odbioru – elektroniczną pieczątkę

wpływu do urzędu. Opłatę uiściłam przy wykorzystaniu bankowości internetowej, wygenerowany dowód wpłaty dołączyłam w formacie .pdf do wysyłanego wniosku, jako formę odbioru zaznaczam „wysyłka poprzez pocztę tradycyjną". Podsumowanie: wszystkie te czynności zajęły mi około 30 minut, nie licząc czasu poświęconego na założenie konta oraz potwierdzenia profilu zaufanego, ponieważ tą czynność wykonuje się jednorazowo. Co najważniejsze wszystkie czynności związane ze złożeniem wniosku wykonałam w dogodnym dla mnie czasie oraz miejscu, bez konieczności zwalniania się z pracy i wizyt w urzędzie. Teraz pozostaje tylko oczekiwanie na odpowiedź i wizyta na poczcie, ponieważ przesyłki polecone listonosz roznosi do godziny 15:30, ja pracuję do 16:00, ale jest to jedyna niedogodność.

Jako przedstawiciel trzeciej grupy, postępuję jak reprezentant grupy drugiej do momentu wypełnienia pola forma odbioru dokumentów, w której zaznaczam opcję elektroniczna odpowiedź na skrzynkę kontaktową. Opłatę skarbową opłacam korzystając z bankowości internetowej, bądź obsługi płatności internetowych dostępnej w danym portalu (np. PaybyNet). Podsumowanie: pół godziny na wysłanie wniosku i dokonanie opłaty. Odpowiedź wpłynie na moją elektroniczną skrzynkę kontaktową, wcześniej na mój telefon komórkowy otrzymam powiadomienie o tym, iż odpowiedź wpłynęła. Po otrzymaniu takiej informacji loguję się do skrzynki, potwierdzam odebranie (Urzędowe Poświadczenie Doręczenia) i odbieram odpowiedź – to wszystko. Oszczędność czasu, nerwów, pieniędzy.

Wyniki mojej analizy przedstawiają się następująco. W każdym z omawianych przypadków postępowanie zakończyło się otrzymaniem decyzji (spodziewanym efektem). Sposób złożenia przeze mnie dokumentów nie wpłynął na termin załatwienia danej sprawy, natomiast różny był czas jaki poświęciłam na czynności związane z załatwieniem sprawy. Różne również były koszty pośrednie, które wiązały się z zadaniem (opłata parkingowa, koszt dojazdu, itd.). Bez wątpienia najszybszą formą złożenia wniosku do urzędu jest komunikacja elektroniczna, pomimo konieczności wcześniejszego założenia skrzynki oraz potwierdzenia profilu. Kolejną zaletą wynikającą ze składania wniosku elektronicznego jest brak ograniczenia czasowego, ponieważ nie jestem ograniczona godzinami pracy urzędu. Miejsce, z którego wysyłam wniosek w drugim oraz trzecim przypadku również nie gra roli, jedynym ograniczeniem jest dostęp do internetu, ale czy zostanie to wysłane z Polsce, czy z innego kraju nie ma znaczenia. Jeżeli tak jak w trzecim wypadku zaznaczę opcję elektronicznej formy odpowiedzi, to tą odpowiedź również w innym mieście, bądź kraju odbiorę.

Ja jako klient usług administracji dokonujący tej analizy bez wątpienia wybieram oblicze numer trzy. Zdaję sobie jednak sprawę, iż należę do nielicznej grupy, potwierdzeniem tego faktu mogą być wyniki najnowszego Raportu[3] wykonanego na zlecenie MSWiA z którego wynika, iż prawie 75% urzędów posiadających elektroniczną skrzynkę podawczą nie otrzymało tą drogą żadnych dokumentów w ciągu pierwszych 5 miesięcy roku 2011.

Chcę więc zwrócić uwagę, iż według mnie ruch należy teraz do pracowników jednostek administracji publicznej, a ruch ten powinien polegać na

3 Raport z badania ilościowego zrealizowanego na zlecenie Ministerstwa Spraw Wewnętrznych i Administracji „Badanie wpływu informatyzacji na działanie urzędów administracji publicznej w Polsce w 2011 roku", sierpień 2011 r.

promowaniu e-usług. Ustawodawca powołał odpowiednie przepisy prawne, pracownicy administracji, informatycy wdrożyli projekty informatyczne takie jak ePUAP czy na szczeblu lokalnym SEKAP. Teraz główną siłę należy skierować na zachęcenie mieszkańców, przedsiębiorców do korzystania z dobrodziejstw jakie daje e-administracja. Trafioną i sprawdzającą się formą promocji są spotkania/warsztaty na których użytkownik może założyć skrzynkę kontaktową, złożyć wniosek o profil zaufany pod okiem urzędnika.

Bibliografia:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. 2005 Nr 64, poz. 565 z późn. zm.
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej Dz. U. 2011, nr 93, poz. 547.
3. Raport z badania ilościowego zrealizowanego na zlecenie Ministerstwa Spraw Wewnętrznych i Administracji „Badanie wpływu informatyzacji na działanie urzędów administracji publicznej w Polsce w 2011 roku", sierpień 2011 r.

Danuta Descours - Obecnie doktorantka w Katedrze Inżynierii Wiedzy Uniwersytetu Ekonomicznego w Katowicach. Od początku swojej pracy zawodowej zajmuje się zagadnieniem rozwoju społeczeństwa informacyjnego, w szczególności wdrażaniem systemów informatycznych w jednostkach administracji publicznej

Zapraszamy do udziału

SEMINARIUM

VIII edycja seminarium w cyklu BADANIA NAUKOWE - ZASADY REDAGOWANIA I PREZENTOWANIA PRAC NAUKOWYCH

Warszawa, 03.09.2013

PROGRAM

- Bibliometryczny pomiar aktywności badawczej - raport Ernst&Young „Produktywność naukowa wyższych szkół publicznych w Polsce"
  dr Aleksandra Parteka (Politechnika Gdańska)
- Jak pisać (redagować) prace naukowe:
  Ewa Rozkosz (Specjalista ds. dokumentacji i informacji naukowej Dolnośląska Szkoła Wyższa)
- Przygotowanie pracy naukowej, podnoszenie prestiżu w sferze zawodowej - podstawowe wymagania formalne i tryb przeprowadzania czynności w pracach naukowych
- *dr Agnieszka Mikos-Sitek (UKSW)*
- Jak napisać wniosek o grant
  Maja Richards (Punkt Kontaktowy Europejskich Programów Badawczych w SGH)
- Od pomysłu do projektu naukowego na przykładzie wniosków NCN:
  dr Konrad Juszczyk (Studenckie Koło Językoznawcze REMAT)

Więcej informacji: **www.cpi.com.pl**

Prawne aspekty Cloud Computing

Anna-Maria Dzięgiel

Cloud Computing *sensu stricte* oznacza - „chmurę obliczeniową". Jest to typ „rozprzestrzeniania" narzędzi informatycznych polegający na udostępnianiu użytkownikom oprogramowania, infrastruktury lub platform rozwoju aplikacji zainstalowanych w serwerach utrzymywanych przez dostawcę owych rozwiązań bądź też podwykonawców[1].

Termin „chmura obliczeniowa" stanowi pewnego rodzaju przenośnię - odnosząca się do budowy oferowanych na tej zasadzie usług. Obliczenia nie odbywają się na komputerze użytkownika, lecz są obsługiwane przez wiele serwerów „umiejscowionych" w serwerowni dostawcy usługi czyli providera. Ponadto na nich zainstalowane jest oprogramowanie. Użytkownik widzi jedynie jego interfejs[2]. Kompleksowe usługi, które może eksploatować użytkownik - składają się z różnych serwisów dostarczanych przez jedną lub inne wykwalifikowane do tego podmioty[3]. Aktualnie znaczna liczba innowacyjności usytuowana jest w modelach chmur obliczeniowych[4].

W mechanizmie Cloud Computing użytkownik nie jest zobowiązany instalować całkowitego systemu informatycznego – do utworzenia łączą z środowiskiem chmury wystarczy co do zasady standardowa przeglądarka internetowa bądź prosty program interfejsu[5].

Cloud Computing stanowi mechanizm umożliwiający wszechobecny, komfortowy oraz dostępny na żądanie dostęp za pośrednictwem sieci do dzielonych zasobów obliczeniowych (tj. sieć, serwery, pamięć masowa, aplikacje i usługi)[6].

Chmura obliczeniowa niejednokrotnie porównywana jest do standardowych modeli outsourcingowych, od których odznacza się jednak znacznie z uwagi na strukturę, jak także aspekt prawny[7].

---

1 Informatyczny słownik angielsko - polski dostępny na stronie www.idg.pl definiuje komputery typu mainframe za Networld.pl, Ronald L. Krutz, Russel Dean Vines, Cloud Security. A comprehensive Guide to Secure Cloud Computing, Wiley Publishing INC, 2010, s. 7.

2 Renzo Marchini, A practical Introduction to the Legal Issues, British Standards Institution 2010, s. 4.i nast.

3 „Internet jest chmurą". „CHIP". 03/2009, s. 38. Warszawa: Burda Communications sp. z o.o.. .

4 Dominik Trojnar: Wirtualizacja jako przyszłość sieci teleinformatycznych. W: SECON 2010 – Materiały konferencyjne. Warszawa: WAT, 2010.

5 Informatyczny słownik angielsko - polski dostępny na stronie www.idg.pl definiuje komputery typu mainframe za Networld.pl, Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly Media, 2009r. , wyd. I., str. 2., Anthony Velte, Toby Velte, Robert Elsenpeter, Cloud Computing. A Practical Approach, wyd. MCGraw-Hill, Companies, 2010, s.6-7.Peter Mell, Thimoty Grance, The NIST definition of Cloud Computing, US. Department of Commerce, wrzesień 2011 r.,

6 Renzo Marchini, A practical Introduction to the Legal Issues, British Standards Institution 2010, s. 4.i nast.

7 Open Cloud Manifesto został sygnowany przez kilkadziesiąt firm świadczących usługi Cloud Computing w 2009 r. min. IBM, Hewlett Packard, Hitachi. Manifest dostępny jest na stronie internetowej:http://opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf, odczyt 27 marca 2012 oraz Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly Media, 2009r. , wyd.I., str. 2.i nast., Arthur Mateos , Jothy Rosenberg, Chmura obliczeniowa. Rozwiązania dla biznesu, Helion S.A, 2011r., s.3o i nast., Anthony Velte, Toby Velte, Robert Elsenpeter, Cloud Computing. A Practical Approach, wyd. MCGraw-Hill Companies, 2010, s.6-7.

Standardowo pojmowany model outsourcingowy jest zdecydowanie mniej przemienny niż chmura, która umożliwia użytkownikom typowe, aktualne dopasowanie portfolio eksploatowanych produktów w zależności od konkretnego zapotrzebowania[8]. Powyższy mechanizm umożliwia np.: efektywniejszą optymalizację kosztów utrzymania infrastruktury IT[9].

Kategorie dostarczania usług w chmurze klasyfikuje się za zasadnicze kategorie:

SaaS (Software as a Service), tak zwane oprogramowanie usytuowane w środowisku chmury; IaaS (Infrastructure as a Service), innymi słowy infrastruktura umiejscowione w środowisku chmury[10]; PaaS (Platform as a Service),określane jako zdalnie udostępniana platforma do rozwoju aplikacji zamieszczona w chmurze[11].

Kwestia ochrony danych osobowych stanowi jedno z fundamentalnych aspektów zagadnień prawnych integralnie związanych z chmurą obliczeniową[12]. Dane osobowy stanowią w dzisiejszych czasach doniosłe znaczenie i posiadają swoja wartość. Z uwagi na powyższe powinna być im zagwarantowana właściwa ochrona[13].

Na terenie Unii Europejskiej model ochrony danych osobowych, sformułowany jest w dwojaki sposób. Otóż w wymienionym powyżej rejonie obowiązuje prawo wspólnotowe - generalnie - Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu ponadto , powyższy zakres obejmuje, także ustawodawstwo konkretnych państw[14]. Na terenie Rzeczpospolitej Polskiej w tymże zakresie obowiązuje ustawa o ochronie danych osobowych z 29 sierpnia

8 Arthur Mateos, Jothy Rosenberg, Chmura obliczeniowa. Rozwiązania dla biznesu, Helion S.A, 2011r, Anthony Velte, Toby Velte, Robert Elsenpeter, Cloud Computing. A Practical Approach, wyd. MCGraw-Hill Companies, 2010, s.6 i nast., Renzo Marchini, A practical Introduction to the Legal Issues, British Standards Institution 2010,

9 Peter Mell, Thimoty Grance, The NIST definition of Cloud Computing, US. Department of Commerce-,wrzesień 2011 r, Ronald L. Krutz, Russel Dean Vines, Cloud Security. A comprehensive Guide to Secure Cloud Computing, Wiley Publishing INC, 2010, s. 7., Ronald L. Krutz, Russel Dean Vines, Cloud Security. A comprehensive Guide to Secure Cloud Computing, Wiley Publishing INC, 2010

10 Jeff Caruso, Iaas vs. PaaS vs. SaaS, 2.11.2011 r., http://www.networkworld.com/news/2011/102511-techargument- iaas-paas-saas-252357.html

11 Arthur Mateos, Jothy Rosenberg, Chmura obliczeniowa. Rozwiązania dla biznesu, Helion S.A, 2011r, str. 29 i nast., Arthur Mateos, Jothy Rosenberg, Chmura obliczeniowa. Rozwiązania dla biznesu, Helion S.A, 2011r., s.37., Anthony Velte, Toby Velte, Robert Elsenpeter, Cloud Computing. A Practical Approach, wyd. MCGraw-Hill, Companies, 2010., Ronald L. Krutz, Russel Dean Vines, Cloud Security. A comprehensive Guide to Secure Cloud Computing, Wiley Publishing INC, 2010., Jeff Caruso, Iaas vs. PaaS vs. SaaS, 2.11.2011 r., http://www.networkworld.com/news/2011/102511-techargument-iaas-paas-saas-252357.html

12 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex, 2011, nr.8531, rozdział II części I dotyczący prawa polskiego., Andrzej Drozd, Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy, Wyd. Prawnicze, Lexis Nexis, Warszawa 2004, s. 48 i nast. ponadto bardzo ciekawa publikacja: Rafał Surowiec, Dane osobowe w chmurach, Rzeczpospolita, 21 lipca 2011 r.

13 Lothar Determann, Data Privacy in the Cloud: Dozen Myths and Facts, The Computer& Internet Lawyer, tom 28, nr 11, listopad 2011 r.

14 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex, 2011, nr.8531, rozdział II części I dotyczący prawa polskiego., Andrzej Drozd, Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy, Wyd. Prawnicze, Lexis Nexis, Warszawa 2004., s. 48 i nast. ponadto bardzo ciekawa publikacja: Rafał Surowiec, Dane osobowe w chmurach, Rzeczpospolita, 21 lipca 2011 r.

1997 r. (u.o.o.d.o) oraz min. ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[15].

Integralnie związanym czynnikiem z eksploatowaniem usług w modelach Cloud Computing, niejednokrotnie łączony jest: „vendor lock"- innym słowy – jest to uzależnienie się od dostawcy. W sytuacji gdy, dostawca SaaS dostarcza gotową aplikację, dostawca PaaS - platformę do tworzenia aplikacji, a provider IaaS całkowitą infrastrukturę[16].

W powyższej sytuacji możliwe jest wystąpienie zdarzania, iż wynik pracy poczynionej w efekcie zastosowania dostarczonych narzędzi nie będzie harmonizował z warunkami innego dostawcy. Ponadto uniemożliwione będzie wyprowadzenie oraz transportowanie owych danych[17]. Na mocy przesłania Dyrektywy 95/46/WE wprowadza w art. 12 ogólną normę prawną, iż każdy może mieć dostęp do własnych danych[18]. Usługobiorcy przysługuje prawo, a jednoczenie, rzec by można nałożony jest na niego obowiązekaby dołożył należytej staranności w kwestii ustanawiania postanowień umownych, które zezwolą mu na komfortowe uzyskanie dostępu oraz transferowanie danych do innego dostawcy[19].

Kontrowersje, także powoduje kwestia usuwania danych z baz dostawcy po rozwiązaniu umowy. Brak odpowiednich gwarancji prawnych w tejże materii ukazuje trudne niuanse. W systemie prawnym obowiązującym na terenie Rzeczpospolitej Polskiej - u.ś.u-.d.o. w art. zapisany jest ewidentny zakaz -19. ust 1. przetwarzania danych po zakończeniu korzystania z usługi[20].

W kontekście przetwarzania danych w chmurze, kluczowe stają się kwestie funkcjonowania "prawa do bycia zapomnianym", a także przenoszenie danych na wniosek osoby zainteresowanej[21]. Użytkownik wyposażony jest w prawo przekazania kopii swoich danych osobowych w takim formacie, aby przenieść je w całości do innego usługodawcy[22]. Ponadto przysługuje mu prawo całkowitego usunięcia danych, które przekazał, nawet jeżeli wcześniej wyraził zgodę na ich

15 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex , 2011, nr.8531, rozdział II części I dotyczący prawa polskiego.

16 Jeff Caruso, Iaas vs. PaaS vs. SaaS , 2.11.2011 r., http://www.networkworld.com/news/2011/102511-techargument-iaas-paas-saas-252357.html, Andrzej Drozd, Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy, Wyd. Prawnicze, Lexis Nexis, Warszawa 2004., s. 48 i nast. ponadto bardzo ciekawa publikacja: Rafał Surowiec, Dane osobowe w chmurach, Rzeczpospolita, 21 lipca 2011 r.

17 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex , 2011, nr.8531.

18 J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art. 32 u.o.o.d.o., J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art. 32 u.o.o.d.o.

19 Renzo Marchini, A practical Introduction to the Legal Issues, British Standards Institution 2010, s. 100.i nast.

20 Andrzej Drozd, Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy, Wyd. Prawnicze, Lexis Nexis, Warszawa 2004., s. 48 i nast. ponadto bardzo ciekawa publikacja: Rafał Surowiec, Dane osobowe w chmurach, Rzeczpospolita, 21 lipca 2011 r.

21 John W. Rittinghouse, James F. Ransome, Cloud Computing. Implementation, Management, Security, CRC Press Taylor&Francis Group 2010, s.140 i nast.

22 John W. Rittinghouse, James F. Ransome, Cloud Computing. Implementation, Management, Security, CRC, Press Taylor&Francis Group 2010, s.147 i nast., Piotr Drobek (op), ABC przekazywania danych osobowych do państw trzecich, Biuro Generalnego Inspektora Danych Osobowych, wyd. Sejmowe, Warszawa 2007 r.

przetwarzanie[23]. Realna jest także sytuacja, aby administrator danych był zobligowany podjąć w takiej sytuacji działania mające na celu usunięcie wszelkich kopii, odnośników cz też innych odesłań do danych umożliwiających publiczny dostęp do nich[24].

Tematyka prawnoautorska istnieje w Cloud Computing w kilku ujęciach. Doniosłą materię stanowią problemy integralnie łączone z umowami na eksploatowanie programów komputerowych udostępnianych przez dostawcę bądź transferowanych do chmury przez użytkownika. [25] W szeroko pojętej doktrynie istnieją teorie zakładające, iż: Cloud Computing może stanowić mechanizm zwalczający piractwo komputerowe. Z uwagi na okoliczność, iż udostępnianie aplikacji w chmurze oraz usuwanie materialnych nośników powoduje ograniczenia liczby kopii pozbawionych bytu prawego[26]. Ponadto zdaniem doktryny zagranicznej Cloud Computing w stanowczy sposób unowocześnia klasyczne podejście do licencjonowania[27]. Nie mniej jednak dostawcy usług w chmurze obliczeniowej używają aplikację, bądź także narzędzia rozwoju - umocowane na licencjach open source[28]. Co więcej Programy udostępniane w ramach modelu SaaS, a także platforma PaaS mogą być skonstruowane z elementów, co do których licencja wykazuje, iż wskazane jest aby one zostawały udostępniane łącznie z kodem źródłowym[29]. Ponadto w świetle przepisów prawa polskiego tematyka takiego zagadnienia jak copyleft[30] jest sporna z uwagi na fakt, iż jego zastosowanie będzie gwarantować więcej, niż wynika to z monopolu autorskiego[31]. Znaczna liczba oprogramowania Cloud Computing opiera się na licencjach open source, ponadto uprawniają do inkorporacji wniosku, iż użytkownik usługi w modelu SPI, a zwłaszcza odbiorca usług zakładających udostępnienie infrastruktury, jak także możliwość budowania własnych aplikacji[32].

23 H. Ward Classen, Marie Fogarty, Avoiding Turbulence in the Cloud: Licensing and Contractual Issues forLicensor, Cloud Provider and End User, The Computer & Internet Lawyer, tom. 19, nr 2, luty 2012., John W. Rittinghouse, James F. Ransome, Cloud Computing. Implementation, Management, Security, CRC, Press Taylor&Francis Group 2010, s.145 i nast.

24 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex , 2011, nr.8531.. Barta, R. Markiewicz, P. Fajgielski, Ibidem, rozdział pt. Przetwarzanie i ochrona danych osobowych w sieciach komputerowych.

25 Elęzbieta Traple, Umowy o eksploatację utworów w prawie polskim, wyd. Oficyna, Warszawa 2010, s. 290 i nast.

26 Pankai Lakhotia, Microsoft says Cloud computing can end software piracy, stockwatch.com, 6.03.2010 r., http://www.stockwatch.in/microsoft-says-cloud-computing-can-end-software-piracy-26613

27 H. Ward Classen, Marie Fogarty, Avoiding Turbulence in the Cloud: Licensing and Contractual Issues forLicensor, Cloud Provider and End User, The Computer & Internet Lawyer, tom. 19, nr 2, luty 2012.

28 Bradley J. Waltz, Open Source Software in the Cloud, Intellectual Property Litigation, tom 23, nr 1, Joanna Kulesza, Ius Internet. Między prawem a etyką, Wyd. Akademickie, Warszawa 2010.

29 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V, Lex, 2011, nr.8531, rozdział II części I dotyczący prawa polskiego.,Bradley J. Waltz, Open Source Software in the Cloud, Intellectual Property Litigation, tom 23, nr 1 Andrzej Drozd, Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy, Wyd. Prawnicze, Lexis Nexis, Warszawa 2004.

30 Copyleft – „rodzaj systemu licencjonowania praw autorskich, zezwalający na modyfikację pracy i jej dalszą redystrybucję na identycznych warunkach". Gregory Hill: Principia Discordia. San Francisco: POEE Head Temple, 1970., Bradley J. Waltz, Open Source Software in the Cloud, Intellectual Property Litigation, tom 23, nr 1

31 Bradley J. Waltz, Open Source Software in the Cloud, Intellectual Property Litigation, tom 23, nr 1

32 J. Barta, R. Markiewicz, Komentarz do art.2 pr.aut., Ibidem, Krzysztof Siewicz, Zakres klauzuli copyleft w prawie polskim, Prace Instytutu Prawa Własności intelektualnej, UJ, zeszyt 93, s.251.

Obecnie nie istnieją normy prawa prywatnego międzynarodowego, które rozwiązywały by powyższą sytuację[33].

Meritum Cloud Computing stanowi udostępnianie i wykonywanie świadczeń w Internecie, z których odbiorca może korzystać w swobodnym zakresie, czasie i miejscu[34]. Ustalanie miejsca świadczenia usługi, miejsca odbioru lub miejsca powstania szkody. Powoduje pewne utrudnienia. Wymiar sądowniczy zmaga się z tym problemem w różnych częściach naszego globu[35]. Zadnienie ustalenia sądu stosownego do orzekania w sprawach spornych posiada doniosłe znacznie w umowach Cloud Computing z uwagi na transgraniczny wymiar usług[36]. W sytuacji niezbędności ustalenia sądu właściwego, wewnętrzne ustawodawstwo prawne państw, ustępuje regułom wyznaczonym przez międzynarodowe akty normatywne[37]. Ponadto w powyższej kwestii wiele kontrowersji powoduje uregulowanie dotyczące miejsca wykonania usługi[38]. Zarówno w doktrynie pojmowanej *sensu largo* jak i orzecznictwie widoczne są mechanizmy dążące do konkretyzacji zdefiniowania terminu „miejsca zdarzenia wywołującego szkodę". W świetle praw obowiązującego na ternie Rzeczpospolitej Polskiej ustalono, iż: „będzie to zarówno miejsce, w którym wystąpiła szkoda, a także położenie, w którym nastąpiło zdarzenie ją powodujące". Za miejsce, w którym szkoda wystąpiła przyjmuje się to „płożenie", w którym nastąpiły ujemne skutki zdarzenia[39]. W świetle orzecznictwa Europejskiego Trybunału Sprawiedliwości w Luksemburgu na podstawie orzeczenia dotyczącego spraw C-509-09 i l61/10 Trybunał stwierdził, iż art. 5 ust.3: „Rozporządzenia Bruksela I należy interpretować w sposób następujący": w wypadku naruszenia dóbr osobistych za pośrednictwem treści opublikowanych w witrynie internetowej, osoba, która uważa się za poszkodowaną, może wytoczyć (…) bądź przed sądami państwa członkowskiego, w którym wydawca tych treści ma swoją siedzibę, bądź przed sądami państwa członkowskiego, w którym znajduje się centrum jej interesów życiowych. Osoba ta może również, zamiast powództwa dotyczącego odpowiedzialności za całość doznanych krzywd i poniesionych szkód, wytoczyć powództwo przed sądami każdego państwa członkowskiego, na którego terytorium treść umieszczona w sieci jest lub była dostępna. Sądy te są właściwe do rozpoznania jedynie krzywdy lub szkody spowodowanych na terytorium państwa członkowskiego sądu, przed którym takie powództwo

33 Kurt Wimmer, Eve Pogoriler, Stephen Sattarfield, International Jurisdiction and the Internet in th Age of Cloud Computing, The Bureau of National Affairs, Washington 2011, http://www.cov.com/files/Publication/

34 Maksymilian Pazdan, Prawo prywatne Międzynarodowe, Wyd. Lexis Nexis, wyd. XIII.

35 Paweł Grzegorczyk, Jurysdykcja krajowa w sprawach z zakresu prawa własności przemysłowej, wyd. Oficyna, Lex nr 65056, Barta Janusz (red.), Markiewicz Ryszard (red.), Czajkowska-Dąbrowska Monika,Ćwiąkalski Zbigniew, Felchner Krzysztof, Traple Elżbieta, Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V, LEX 2011, nr 8545, Velte Anthony, Velte Toby, Elsenpeter Robert, Cloud Computing. A Practical Approach, MCGraw-Hill Companies, 2010

36 Kurt Wimmer, Eve Pogoriler, Stephen Sattarfield, International Jurisdiction and the Internet in th Age ofCloud Computing, The Bureau of National Affairs, Washington 2011, http://www.cov.com/files/Publication

37 Maksymilian Pazdan, Prawo prywatne Międzynarodowe, Wyd. Lexis Nexis, wyd. XIII.

38 Kurt Wimmer, Eve Pogoriler, Stephen Sattarfield, International Jurisdiction and the Internet in th Age of Cloud Computing, The Bureau of National Affairs, Washington 2011, http://www.cov.com/files/Publication, Saslesforce Master Subscription Agreement Developer Service,http://www2.sfdcstatic.com/assets/pdf/misc/salesforce_Developer_MSA.pdf, Barta Janusz (red.), MarkiewiczRyszard (red.), Czajkowska-Dąbrowska Monika, Ćwiąkalski Zbigniew, Felchner Krzysztof, Traple Elżbieta, Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V, LEX 2011, nr 8545

39 Henryk Dolecki (red.), Kodeks postępowania cywilnego. Komentarz. Tom V, wyd. I, Lex 2012.

zostało wytoczone[40]. W systemie prawnym USA natomiast dominuje pogląd ugruntowany w orzecznictwie, iż właściwość sądu w sytuacji „nadużyć" internetowych jest uzależniona od „woli oraz działań jednostki, która dopuściła się naruszenia na określonym terenie"[41]. W prawie Stanów Zjednoczonych kluczowym terminem jest wyznaczenie podmiotu będącego adresatem owych „ uszczerbków" [42].

Doniosłym zagadnieniem jest także kwestia ograniczenia odpowiedzialności za szkodę wywołaną nieodpowiednim przetwarzaniem danych[42].

Ponadto ważną cechą chmury obliczeniowej jest wielodzierżawa. Jest to mechanizm powodujący uszczerbek. Z uwagi na powyższe dostawcy starają się „ekstremalnie" zmniejszać swoją odpowiedzialność[44]. W świetle uregulowań Dyrektywy 95/46/WE w art. 23 pkt. 2 - administrator uprawniony jest do uchylenia się z odpowiedzialności za takie zdarzenie w całości lub w części, jeśli udowodni, że nie jest odpowiedzialny za działanie lub zaniechanie, które spowodowało uszczerbek[45].

Cloud computing jest to bardzo szeroki wachlarz usług, stwarzający podstawy jak i możliwości do organizacji każdej wielkości i z różnym stopniem zaawansowania w zakresie infrastruktury IT[46]. Na popularność Cloud Computing wpływ wywarła mnogość rozlicznych innowacyjnych mechanizmów technologicznych[47].

Z uwagi na okoliczność, iż oferta usytuowana jest przez providera usługi w chmurze realne jest skalowanie posiadanych zasobów do aktualnego obarczania przez pewną liczbę użytkowników[48].

40 Orzeczenie TS UE z dnia 25.10.2011 r., w sprawie eDate Advertising GmBH przeciwko X. MGN Limited,http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:370:0009:0010:PL

41 Mateusz Kondrat, Ochrona znaków towarowych przed naruszeniami w Internecie, wyd. Oficyna, Lex nr.81492., J. Gołaczyński, Umowy elektroniczne w prawie prywatnym międzynarodowym, Rozdział VI, Oficyna , 2007, Barta Janusz (red.), Markiewicz Ryszard (red.), Czajkowska-Dąbrowska Monika, Ćwiąkalski Zbigniew, Felchner Krzysztof, Traple Elżbieta, Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V, LEX 2011, nr 8545

42 Mateusz Kondrat, Ochrona znaków towarowych przed naruszeniami w Internecie, wyd. Oficyna, Lex nr 81492., Katarzyna Grzybczyk, Prawo właściwe dla autorsko prawnej umowy licencyjnej, wyd. Oficyna, Warszawa 2010.

43 Renzo Marchini, A practical Introduction to the Legal Issues, British Standards Institution 2010, str. 40 i nast.

44 Paweł Grzegorczyk, Jurysdykcja krajowa w sprawach z zakresu prawa własności przemysłowej, wyd. Oficyna, Lex nr 65056, Barta Janusz (red.), Markiewicz Ryszard (red.), Czajkowska-Dąbrowska Monika,Ćwiąkalski Zbigniew, Felchner Krzysztof, Traple Elżbieta, Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V, LEX 2011, nr 8545, Velte Anthony, Velte Toby, Elsenpeter Robert, Cloud Computing. A Practical Approach, MCGraw-Hill Companies, 2010, Simon Bradshaw, Christopher Millard, Ian Walden, Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services, International Journal of Law and Information Technology, Queen Mary University of London, tom. 19, nr 3, 20 .07.2011 r.

45 J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do rozdziału Prawo polskie a prawo unijne.

46 Krutz Ronald L., Vines Russel Dean, Cloud Security. A comprehensive Guide to Secure Cloud Computing, Wiley Publishing INC, 2010.

47 Andrzej Maciejeski, Konsumeryzacja. Pracownicy będą rządzić firmowym IT, Computerworld.pl,6.03.2012, http://www.computerworld.pl/artykuly/380831/Konsumeryzacja.Pracownicy.beda.rzadzic.firmowym.IT.html

48 Rittinghouse John W., Ransome James F., Cloud Computing. Implementation, Management, Security, CRC Press Taylor&Francis Group 2010, Mather Tim, Kumaraswamy Subra, Latif Shahed, Cloud Security and Privacy. Anenterprise perspective on Risk and Compliance, O'Reilly, 2009,

Reasumując Cloud Computing jako jeden z sposobów wykonywania usług IT, stwarza użytkownikowi możliwość używania zasobów obliczeniowych w dowolnym miejscu i dowolnym czasie. Ów użytkownik posiada możliwość skorzystania z aplikacji bez wymogu ich instalacji, jak także infrastruktury, na której uczyni „przesłanie" programów[49]. Z uwagi na doniosłe znacznie danych osobowych hipotetyczny użytkownik mający zamiar przenieść dane do chmury, powinien dokładnie przeanalizować różnorakie działania podejmowane przez dostawcę nakierowane na stworzenie bezpieczeństwa infrastruktury[50].

Ideologia infrastruktury Cloud Computing, zgodnie z którą różnorakie informacje oraz aplikacje przechowywane są na serwerach w centrach przetwarzania, zmniejszają się koszty nabywania, jak także niższe są kwoty utrzymania wymaganego oprogramowania[51].

„Przetwarzanie w chmurze" umożliwia obniżenie wydatków, w związku z zakupem licencji na oprogramowanie – gdyż np. „aplikacje" umieszcza się na serwerach, gdyż łączy się to z wprowadzeniem bardziej wydajnego schematu licencjonowania[52].

Z uwagi na konsolidacje platformy działania IT przeprowadzanie są efektywniej sprawniej. Pomijając koszty z tytułu niezbędności wykonywania standardowych zadań administracyjnych[53]. Owe usługi są „upowszechnione" tym samym zmniejsza to koszty związane z usuwanie na problemów oraz zarządzaniem rozwiązaniami niestandardowymi, odbiegającymi od zasady[54].

Finalnie można stwierdzić, iż chmura obliczeniowa to zadanie jak i wyzwania tak dla świata prawa jak i świata nowych technologi.

Powyższe „zjawisko" to niezwykle nowoczesna wizja dla utworzenia indywidualnego środowiska informatycznego[55]. Stwarza

49 Srinivasan Sundra Rajan, The importance of community clouds, 24.04.2011r., www.cloudcomputing.sys-con.com, Salkever Alex, 5 ways to protect against vendor lock- in in the cloud, http://gigaom.com, Lakhotia Pankai, Microsoft says Cloud computing can end software piracy, www.stockwatch.com

50 Muszyński Józef, Grid Computing a problem zarządzania, 2.07.2002 r.,www.networld.pl.,

51 Austien Ian, A liabel case raises a tricky question of Jurisdiction, The New York Times, 14.03. 2005 r., http://www.nytimes.com/, Wittow Mark H., Buller Daniel J., Cloud Computing: Emerging legal issues for acces to data anywhere, anytime, Internet Law, vol.14, nr 1, lipiec 2010,

52 Wimmer Kurt, Pogoriler Eve, Sattarfield Stephen, International Jurisdiction and the Internet in th Age of Cloud Computing, The Bureau of National Affairs, Washington 2011, http://www.cov.com,Bradshaw Simon, Millard Christopher, Walden Ian, Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services, International Journal of Law and Information Technology, Queen Mary University of London, tom ,19, nr 3, 20 lipca 2011.

53 Determann Lothar, Data privacy in the Cloud: A dozen Myths and Facts, The Computer& Internet Lawyer, vol.28, nr 11, listopad 2011,

54 Classen H. Ward, Fogarty Marie, Avoiding Turbulence in the Cloud: Licensing and Contractual Issues for Licensor, Cloud Provider and End User, The Computer & Internet Lawyer, tom. 19, nr 2, luty 2012, Bradshaw Simon, Millard Christopher, Walden Ian, Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services, International Journal of Law and Information Technology, Queen Mary University of London, tom. 19, nr 3, 20 lipca 2011, Ward T. Burke, Sipior Janice C., The Internet Jurisdiction Risk of Cloud Computing, Taylor&Franciss Group

55 http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0, Classen H. Ward, Fogarty Marie, Avoiding Turbulence in the Cloud: Licensing and Contractual Issues for Licensor, Cloud Provider and End User, The Computer & Internet Lawyer, tom. 19, nr 2, luty 2012, Bradshaw Simon, Millard Christopher, Walden Ian, Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services, International Journal of Law and Information Technology, Queen Mary University of London, tom. 19, nr 3, 20 lipca 2011, Ward T. Burke, Sipior Janice C., The Internet Jurisdiction Risk of Cloud Computing, Taylor&Franciss Group

możliwości korzystania z rozwiązań o wysokim poziomie innowacyjności technologicznych, które można skutecznie przekształcić w zależności od konieczności[56]. Ponadto realne staje się skuteczne reagowanie na zmieniające się warunki na rynku jak także zaangażowanie obarczonych zasobów przedsiębiorstwa w podnoszenie jego wydajności[57].

Anna Maria Dzięgiel – Prawnik. Interesuje się międzynarodowym prawem własności intelektualnej, prawem nowych technologii, francuskim, amerykańskim, rosyjskim praz ukraińskim prawem autorskim. Ochroną danych osobowych w świetle najnowszych światowych regulacji prawnych. Zgłębiam zagadnienia odpowiedzialności przedsiębiorców z niezgodne z prawem wykorzystywanie danych osobowych.

56 http://www.infoworld.com/d/cloud-computing/download-the-cloud-security-deepdive66source=ifwelg_fssr,http://www.infoworld.com/d/cloud-computing/download-the-cloud-services-deep-dive-report-479?source=ifwelg_fssr, Determann Lothar, Data privacy in the Cloud: A dozen Myths and Facts, The Computer& Internet Lawyer, vol.28, nr 11, listopad 2011.

57 http://www.infoworld.com/d/cloud-computing/cloud-computing-in-2012-infoworld-special-report-187077?source=fssr, http://www.infoworld.com/d/cloud-computing/download-the-cloud-security-deep-dive-660?source=ifwelg_fssr, Determann Lothar, Data privacy in the Cloud: A dozen Myths and Facts, The Computer& Internet Lawyer, vol.28, nr 11, listopad 2011.

Zapraszamy do udziału

WARSZTATY

AKADEMIA UMÓW IT dla działów prawnych poziom I

- Prawne aspekty umów IT

Warszawa, 24.09.2013

Celem warsztatu jest przedstawienie praktycznych aspektów sporządzania oraz negocjacji umów na wdrożenie systemów informatycznych oraz umów będących podstawa korzystania z oprogramowania w przedsiębiorstwie (np. licencje). Warsztaty opierają się na praktycznej analizie przykładowych klauzul umownych, analizie studium przepydków (case studies) oraz **nauce samodzielnej weryfikacji klauzul umownych przez uczestników szkolenia**.

Kto powinien wziąć udział w warsztatach?

- radcy prawni oraz prawnicy przedsiębiorstw zamierzających wdrożyć system informatyczny, korzystać z usług utrzymania systemów IT
- radcy prawni oraz prawnicy przedsiębiorstw przygotowujących się do zawarcia umowy outsourcingu informatycznego,
- radcy prawni oraz prawnicy zatrudnieni w firmach prowadzących wdrożenia systemów informatycznych lub dystrybucję oprogramowania,
- radcy prawni oraz prawnicy zatrudnieni w firmach świadczących usługi outsourcingu informatycznego,
- kadra zarządzająca IT, dyrektorzy IT oraz managerowie w firmach planujących wdrożenie systemu informatycznego lub skorzystanie z usług outsourcingu IT - posiadającą przynajmniej podstawową wiedzę z zakresu prawa cywilnego oraz prawa autorskiego

Warsztaty przeznaczone są przede wszystkim dla prawników praktyków zajmujących się przygotowywaniem i negocjacjami umów IT.

PROGRAM

- - Podstawy prawa własności intelektualnej w IT
- - Umowa na wdrożenie systemu informatycznego
- - Umowa depozytu kodu źródłowego oprogramowania
- - Outsourcing IT
- - Umowa outsourcingu IT
- - Umowy utrzymaniowe (serwisowe) oraz umowy dotyczące rozwoju oprogramowania

Więcej Informacji: **www.cpi.com.pl**

Składanie oświadczeń woli w formie elektronicznej

dr Jacek Murzydło

Jedną z form składania oświadczeń woli przewidzianą przez Kodeks cywilny jest forma elektroniczna. Znajomość nawet elementarnych zasad jej zastosowania może okazać się niezbędne nie tylko dla przedsiębiorców, ale także dla osób fizycznych coraz powszechniej korzystających z dobrodziejstw Internetu.

W dzisiejszych czasach Internet stał się medium niemal powszechnym, nie tylko ułatwiającym codzienne życie, lecz także – jak się nam częstokroć wydaje – umożliwiającym normalne funkcjonowanie. Wysyłamy e-maile, pobieramy różnorakie programy, spotykamy się ze znajomymi na portalach społecznościowych, poszukujemy pożądanych informacji. Usługi elektroniczne wchodzą także coraz odważniej w dziedziny życia, z którymi jeszcze do niedawna wydawały się nie do połączenia. Wskazać można w tym miejscu chociażby wnoszenie podań w formie elektronicznej do organów administracji publicznej, uzyskiwanie elektronicznych decyzji administracyjnych, korzystanie z bankowości elektronicznej. Niejednokrotnie do złożenia oświadczenia woli, a nawet zawarcia umowy wystarczy chociażby wysłanie e-maila lub kliknięcie w odpowiednią ikonę na stronie Internetowej. Nie każdy zastanawia się z jakimi konsekwencjami wiąże się składanie oświadczeń woli w formie elektronicznej. Powoduje to narastanie różnych pomyłek i niejasności o czym świadczy chociażby znany z ostatnich czasów kazus serwisu Pobieraczek.pl. Nie wszystkie niestety można jednoznacznie rozstrzygnąć. Medium jakim jest Internet wciąż ewoluuje przez co prawodawca nie zawsze jest w stanie nadążyć z dostosowaniem przepisów do nowych okoliczności. Oczywiście o wiele lepszą opcją byłoby gdyby były one na tyle uniwersalne, aby znajdować zastosowanie niezależnie od rozwoju technologicznego. To jednak w praktyce często bywa trudne do osiągnięcia, tym bardziej, że przedmiotową kwestię reguluje wiele różnych aktów prawnych, a ich ilość sukcesywnie rośnie.

Formy oświadczeń woli

Przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93, z późn. zm., dalej jako „K.c.") dopuszczają szeroki zakres form w jakich może zostać złożone oświadczenie woli. Stanowi o tym art. 60 cyt. ustawy definiujący oświadczenie woli. Zgodnie z nim oświadczeniem woli jest każde zachowanie się tej osoby (poza wyjątkami wskazanymi w ustawie), które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej. Pomimo, iż ustawa o tym nie wspomina, na istotny element oświadczeń woli wskazuje doktryna. Jak bowiem podnosi np. P. Machnikowski oświadczeniem woli jest wyłącznie zachowanie zmierzające do wywołania skutku w postaci powstania, zmiany lub ustania stosunku prawnego, tj. takie zachowanie, które ma wpłynąć na istnienie i treść uprawnień i obowiązków cywilnoprawnych[1].

1 P. Machnikowski, Kodeks cywilny. Komentarz (red. E. Gniewek), Wydawnictwo C.H. Beck, 2006

Tym samym wyróżnić można chociażby tradycyjny podział oświadczeń woli na:
1. wyraźne lub dorozumiane[2]
2. przy użyciu języka lub za pomocą niewerbalnych przekazów informacji (znaków)
3. pisemne lub ustne[3].

Odnosząc się do ostatniego ze wskazanych punktów – on bowiem w kontekście niniejszego opracowania ma najistotniejsze znaczenie – wskazać można m.in. na następujące formy[4]:
1. forma ustna – najbardziej powszechna forma, spotykana w zwykłych czynnościach życia codziennego, takich jak chociażby codzienne drobne zakupy. W K.c. w odniesieniu do jednostronnych czynności prawnych uregulowana chociażby w odniesieniu do testamentu ustnego (art. 952 K.c.) oraz oświadczenia o przyjęciu lub o odrzuceniu spadku (art. 1018 K.c.);
2. zwykła forma pisemna – zgodnie z art. 78 § 1 K.c. do zachowania pisemnej formy czynności prawnej wystarcza złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli. Do zawarcia umowy wystarcza zaś wymiana dokumentów obejmujących treść oświadczeń woli, z których każdy jest podpisany przez jedną ze stron, lub dokumentów, z których każdy obejmuje treść oświadczenia woli jednej ze stron i jest przez nią podpisany. Do zachowania zwykłej formy pisemnej nie konieczne ani napisanie dokumentu własnoręcznie (z wyjątkiem testamentów), ani nawet sporządzenie dokumentu osobiście. Ważne, aby składający oświadczenie woli własnoręcznie je podpisał (co najmniej nazwiskiem);
3. forma pisemna z podpisami notarialnie poświadczonymi – przewidziana m.in. w art. 75 [1] K.c. dla zbycia lub wydzierżawienia przedsiębiorstwa albo ustanowienia na nim użytkowania;
4. akt notarialny – sporządzany przez notariusza powinien zawierać treść oświadczeń stron i zostać przez notariusza odczytany, a następnie podpisany zarówno przez niego, jak i biorących udział w akcie oraz osób obecnych przy sporządzaniu aktu (patrz Rozdział 3 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, Dz. U. z 2008 r. Nr 189, poz. 1158, z późn. zm.). Forma ta wymagana jest np. dla umów zobowiązujących do przeniesienia własności nieruchomości (art. 158 K.c.).

Chwila złożenia oświadczenia woli w formie elektronicznej

Zgodnie z generalną zasadą wyrażoną w art. 61 § 1 K.c. oświadczenie woli, które ma być złożone innej osobie, jest złożone z chwilą, gdy doszło do niej w taki sposób, że mogła zapoznać się z jego treścią. Nie wdając się w dywagacje na temat rozumienia powyższej reguły, skupić należałoby się raczej na regulacji zawartej w art. 61 § 2 cyt. ustawy. Ona bowiem odnosi się bezpośrednio do oświadczeni woli wyrażonego w postaci elektronicznej. Zgodnie ze wskazanym artykułem chwilą złożenia takiego oświadczenia jest chwila, gdy wprowadzono go do środka komunikacji elektronicznej w taki sposób, żeby jego adresat mógł zapoznać się z jego treścią. Wyjaśnienia wymaga w tym miejscu w szczególności termin „środek komunikacji elektronicznej" oraz kwestia określenia kiedy możliwe jest zapoznanie się z treścią elektronicznego oświadczenia woli.

2 Dorozumiane oświadczenie woli może przybrać nawet postać milczenia, tj. skutki prawne wywołać może np. milczące zaakceptowanie oświadczenia woli drugiej strony (wyrok SN z dnia 6 października 2010 r., II CSK 210/10, LEX 786938).

3 A. Janiak, Kodeks cywilny. Komentarz. Tom I. Część ogólna (red. A. Kidyba). Wolters Kluwer Polska, 2012.

4 Nie stanowią one katalogu zamkniętego.

Odnośnie pierwszego z zagadnień pożądana definicja zawarta została w art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.). Zgodnie z nim środki komunikacji elektronicznej stanowią rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną. Środkiem komunikacji elektronicznej może być więc chociażby poczta elektroniczna, strona WWW, IRC, a nawet SMS, nie może nim być natomiast chociażby nośnik informacji taki jak chociażby płyta CD lub pamięć USB. Nie oznacza to oczywiście, że oświadczenie woli w formie elektronicznej (oczywiście poza przypadkami kiedy forma oświadczenia woli została wyraźnie przez ustawodawcę zastrzeżona) nie może zostać złożone na dowolnym elektronicznym nośniku danych. Z tą jednak różnicą, że w takim przypadku w zakresie ustalania chwili złożenia oświadczenia woli zastosowanie znajdzie reguła wyrażona w art. 61 § 1 K.c. (a nie w art. 61 § 2 K.c.)[5].

Zadać można w tym miejscu jeszcze jedno pytanie – czy adresat oświadczenia woli musi wyrazić zgodę na taką formę jego składania? Kwestia ta jest dyskusyjna, można jednak wskazać, że przeważająca część doktryny uznaje, iż adresat oświadczenia woli powinien wyrazić zgodę na taką formę.

Problematyczne okazać się może w praktyce określenie chwili wprowadzenia oświadczenia woli do środka komunikacji elektronicznej w taki sposób, żeby adresat mógł się zapoznać z jego treścią. Tym bardziej, że wiele oświadczeń woli składanych jest nie w czasie rzeczywistym (np. za pośrednictwem IRC lub w trybie wideokonferencji), ale z wykorzystaniem narzędzi, które nie zawsze umożliwiają składającemu oświadczenie woli proste ustalenie kiedy dotarło ono do adresata w sposób umożliwiający zapoznanie się z jego treścią (np. w przypadku poczty elektronicznej). W związku z powyższym spotkać się można niekiedy z wskazywaniem podziału na składanie oświadczeń woli w trybie online i w trybie offline, przy czym jako przykład wykorzystania drugiego z trybów niejednokrotnie wskazywana jest właśnie często poczta elektroniczna. Niewątpliwie składanie oświadczeń woli w trybie offline z wykorzystaniem poczty elektronicznej jest możliwe, jednak nie powinno się obydwu tych elementów utożsamiać. Można założyć bowiem, iż w wielu przypadkach wykorzystywana jest ona w trybie online. Niezależnie od powyższych dywagacji terminologicznych przyznać trzeba, że zastosowanie trybu offline dodatkowo komplikuje kwestię ustalenia momentu złożenia oświadczenia woli w formie elektronicznej. Oczywistą kwestią jest to, że przedmiotowe oświadczenie woli niekoniecznie będzie odczytane tuż po jego wysłaniu przez nadawcę. Nie ma przy tym znaczenia, że najczęściej wpłynie ono na serwer poczty adresata tuż po jego wysłaniu. Nie zawsze można bowiem zakładać, że adresat oświadczenia woli regularnie sprawdza konto email lub też - jeżeli adresat dysponuje kilkoma adresami email - że skorzysta akurat z tego na który oświadczenie zostało wysłane.

Podkreślić należy, że terminu „mógł się zapoznać”nie można utożsamiać z terminem „zapoznał się”. Tym samym nie jest

5 Uznać należy także, że do oświadczeń woli składanych w formie elektronicznej art. 61 § 1 K.c. zastosowanie znajdzie także w zakresie ich odwołania. Będzie ono więc skuteczne jeżeli doszło jednocześnie z tym oświadczeniem lub wcześniej.

koniecznym, aby adresat elektronicznego oświadczenia woli faktycznie się z nim zapoznał. Wystarczy jedynie, aby w normalnym okolicznościach, zgodnie z oczekiwaniem opartym na zdroworozsądkowych przesłankach, mógł się z nim zapoznać. Sytuacja taka wystąpi niewątpliwie w przypadku przedsiębiorców, wskazujących swoje adresy poczty elektronicznej jako dostępne kanały komunikacji, w godzinach ich pracy. Wymagać to będzie jednak niewątpliwe każdorazowej oceny, opartej na konkretnej analizie zaistniałego przypadku. Jak stwierdził bowiem Sąd Najwyższy w wyroku z dnia 18 kwietnia 2012 r. (V CSK 215/11) „w rozumieniu przytoczonego przepisu możliwość zapoznania się z treścią oświadczenia przez adresata nie może, z jednej strony, być utożsamiana z rzeczywistym zapoznaniem się przez niego z tym oświadczeniem (faktem zapoznania się), co oznacza, że skuteczne złożeniu oświadczenia woli następuje także, w sytuacji, w której co prawda adresat oświadczenia woli nie zna jego treści, ale miał realną możliwość zapoznania się z nią, gdyż doszła ona do niego w taki sposób, że mógł się z nią zapoznać. Z drugiej jednak strony, realna możliwość zapoznania się z treścią oświadczenia woli nie może być pojmowana abstrakcyjnie, powinna być oceniana z uwzględnieniem okoliczności danego wypadku."

Przytoczyć warto ponadto dwa postanowienia Sądu Najwyższego zgodnie z którymi:

- „dniem uiszczenia opłaty sądowej dokonanej za pomocą elektronicznego środka komunikacji jest dzień, w którym polecenie przelewu - mające pokrycie na rachunku zleceniodawcy - wprowadzone zostało do urządzenia nadawczego w taki sposób, że bank mógł zapoznać się z jego treścią; możliwość taką bank uzyskuje z chwilą odebrania polecenia przez jego urządzenie odbiorcze" – postanowienie SN z dnia 26 września 2008 r., V CZ 56/08;
- „oświadczenie woli w postaci elektronicznej dokonywane online zostaje złożone z chwilą jego przejścia do systemu informatycznego prowadzonego i kontrolowanego przez odbiorcę, to jest w momencie przyjęcia oświadczenia przez serwer odbiorcy i zarejestrowania na nim odpowiednich danych" - postanowienie SN z dnia 10 grudnia 2003 r., V CZ 127/03.

Powyższe oczywiście nie odpowiadają na wszelkie potencjalne pytania. Zakładać bowiem można wystąpienie dodatkowych komplikacji takich jak chociażby usunięcie oświadczenia woli przez jego adresata, bez jego czytania, z uwagi na podejrzenie otrzymania tzw. spamu (w tym przypadku przyjąć można zaistnienie możliwości zapoznania się z oświadczeniem woli). Sytuacja taka wystąpić może zresztą także w przypadku zaliczenia przez stosowny program wiadomości do spamu (określenie „możliwości zapoznania się" będzie w tym momencie trudniejsze, choć w przeważającej części przypadków wydaje się, iż będzie należało ją wykluczyć). Inną sytuacją może być także przesłanie adresatowi oświadczenia woli zapisanego z formacie, którego nie jest w stanie odczytać lub zapisanego w zawirusowanym pliku, którego, po próbie naprawy, nie można odczytać. W takich przypadkach zakładać należy, że adresat oświadczenia woli nie miał możliwości zapoznania się z jego treścią.

Co istotne inne niż K.c. ustawy także zawierają przepisy określające chwilę złożenia oświadczenia woli w formie elektronicznej. Wskazać w tym miejscu można np. art. 2 ust. 1 ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz. U. z 2012 r., poz. 1225) przyznający konsumentowi, który zawarł umowę poza lokalem przedsiębiorstwa, prawo odstąpienia od niej bez podania przyczyn, poprzez złożenie stosownego

oświadczenia na piśmie[6] w terminie dziesięciu dni od zawarcia umowy. Cytowany przepis określa przy tym, że do zachowania tego terminu wystarczy wysłanie oświadczenia przed jego upływem. Chwilą złożenia oświadczenia woli nie jest więc chwila w której jego adresat mógł się zapoznać z jego treścią, lecz chwila jego wysłania (ważne jest więc jego wysłanie, a nie potencjalny odbiór).

Podpis zwykły czy kwalifikowany

Do złożenia oświadczenia woli w formie elektronicznej nie jest wymagane opatrzenie go bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. Wystarczy jedynie aby podpis, którym zostało opatrzone takie oświadczenie pozwalał na jednoznaczną identyfikację osoby składającej oświadczenie woli. W praktyce jednak trzeba przyznać, że największą gwarancję, że oświadczenie złożyła właśnie ta osoba, a nie ktoś inny, daje wskazany rodzaj podpisu. Z tej też przyczyny ustawodawca przypisał mu przepisami K.c. szczególne znaczenie polegające na tym, iż oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej (art. 78 § 2 K.c.). Nie wystarczy więc, aby podpis elektroniczny[7] był bezpieczny, tj. łącznie:

- przyporządkowany wyłącznie do osoby składającej ten podpis,
- sporządzony za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,

- powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna[8].

Musi być ponadto weryfikowany za pomocą ważnego certyfikatu wydanego przez kwalifikowany podmiot świadczący usługi certyfikacyjne i spełniającego wymogi określone w ustawie o podpisie elektronicznym.

Znajduje to także potwierdzenie w art. 6 ust. 1 cyt. ustawy określającym, iż podpis taki stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny. Czy można zatem odmówić mocy prawnej oświadczeniu woli złożonemu w formie elektronicznej, które nie zostało opatrzone takim podpisem, a na przykład samym imieniem i nazwiskiem? Zważywszy na treść cyt. już art. 60 K.c. uznać można, że nie. Wola osoby dokonującej czynności prawnej może być bowiem wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny. Istotna jest więc możliwość jednoznacznego określenia tożsamości osoby składającej oświadczenie woli, a nie rodzaj podpisu elektronicznego, którym się posłużyła. W przypadku podpisania elektronicznego oświadczenia woli imieniem i nazwiskiem sytuacja taka będzie tym bardziej jednoznaczna, jeżeli składający to oświadczenie

6 Przy czym nie zawsze taka forma wystąpi w przypadku elektronicznego oświadczenia woli, o czym będzie mowa w części dalszej.

7 Podpis elektroniczny czyli zgodnie z art. 3 pkt 1 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm., dalej jako „U.p.e.") „dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny".

8 Patrz art. 3 pkt 2 U.p.e.

posługuje się dodatkowymi elementami indywidualizującymi (jak na przykład stałym adresem email).

Powyższe znajduje zresztą potwierdzenie w treści art. 8 U.p.e. wskazującej, że nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego.

Należy przy tym co istotne zwrócić uwagę, że w niektórych sytuacjach użycie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu może być wymagane. W niektórych przypadkach ustawy zastrzegają bowiem dla danej czynności prawnej formę pisemną, która jak już zauważono, zostaje zachowana zgodnie z art. 78 K.c. przy zastosowaniu wskazanego podpisu. Użycie w takiej sytuacji innego podpisu elektronicznego nie będzie skutkowało nieważnością czynności prawnej, chyba, że rygor nieważności zostanie wyraźnie przez ustawę przewidziany lub jeżeli ustawa zastrzega dla czynności prawnej inną formę szczególną (patrz art. 73 K.c.)[9].

Co więcej w przypadku użycia zwykłego podpisu elektronicznego wykazanie, że oświadczenie woli zostało złożone przez daną osobę lub też, że jest ono ważne, może być utrudnione, co może niekiedy poważnie wpłynąć na zakres praw i obowiązków jego adresata[10]. Dla przykładu zgodnie z art. 12 K.c. nie mają zdolności do czynności prawnych osoby, które nie ukończyły lat trzynastu, oraz osoby ubezwłasnowolnione całkowicie. Ograniczoną zdolność do czynności prawnych mają zaś małoletni, którzy ukończyli lat trzynaście, oraz osoby ubezwłasnowolnione częściowo (art. 15 K.c.).

Pomimo wskazanych ograniczeń osoby te stanowią znaczne grono użytkowników Internetu, masowo – bardziej lub mniej świadomie – składając wiele oświadczeń woli w tym zawierając liczne umowy. Czynność prawna dokonana przez osobę, która nie ma zdolności do czynności prawnych, jest zaś nieważna (art. 14 § 1 K.c.), chociaż zastosowanie znaleźć może art. 14 § 2 K.c. wskazujący, że umowa powszechnie zawierana w drobnych bieżących sprawach życia codziennego zawarta przez osobę niezdolną do czynności prawnych staje się ważna z chwilą jej wykonania, chyba że pociąga za sobą rażące pokrzywdzenie osoby niezdolnej do czynności prawnych. Wskazać można ponadto na przepisy zakazujące dokonywania określonych czynności prawnych osobom poniżej 18 roku życia. Jako przykład wskazać można chociażby art. 15 ust. 1 pkt 2 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2012 r., poz. 1356, z późn. zm.) zabraniający sprzedaży napojów alkoholowych m.in. osobom do lat 18. Ma to o tyle znaczenie, że sklepy Internetowe sprzedające alkohol nie posiadają najczęściej żadnych skutecznych metod weryfikacji wieku klienta, ograniczając się najczęściej jedynie do otrzymania jego deklaracji o pełnoletniości (poprzez „kliknięcie" na ikonę potwierdzającą ukończenie 18 lat).

9 Na przykład zgodnie z art. 92 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037, z późn. zm.) pod rygorem nieważności powinna zostać zawarta na piśmie umowa spółki partnerskiej.

10 Zgodnie z art. 6 K.c. ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne.

Wskazać można w tym miejscu na jeszcze jeden element. Jak już wspomniano bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny. Pojawia się więc pytanie o zakres ochrony adresata oświadczenia woli złożonego bez wykorzystania takiego podpisu. Potencjalna sytuacja nieuprawnionego wykorzystania podpisu elektronicznego może odnosić się bowiem głównie do takiego przypadku. Rozsądne jak się wydaje rozwiązanie zaproponował P. Machnikowski[11]. Stwierdził on, że w szczególności w przypadku poczty elektronicznej uznać należy, iż dla przyjęcia dobrej wiary adresata oświadczenia woli powinien on podjąć właściwe dla danych okoliczności działania mające na celu potwierdzenie tożsamości składającego oświadczenie woli. Stanowić one będą niewątpliwie zabezpieczenie, pozwalające uniknąć w przyszłości potencjalnych kłopotów.

dr Jacek Murzydło - specjalista ds. prawnych w Okręgowym Urzędzie Górniczym w Poznaniu, doktor nauk humanistycznych, aplikant radcowski. Autor licznych (ponad 170) artykułów z dziedziny prawa.

11 P. Machnikowski, Kodeks cywilny. Komentarz (red. E. Gniewek), Wydawnictwo C.H. Beck, 2006.

Zapraszamy do udziału

WARSZTATY

AKADEMIA UMÓW IT dla działów prawnych poziom II - Nowatorskie konstrukcje prawne w zakresie projektów IT

Warszawa, 25.09.2013

Celem warsztatu jest zapoznanie uczestników z aspektami prawnymi nowych trendów na rynku IT.

W ramach warsztatów uczestnicy zapoznają się miedzy innymi z następującą problematyką:

- jakie są wymagania prawne oraz ryzyka prawne związane z świadczeniem i korzystaniem z usług informatycznych w modelu Cloud Computing?
- jakie są wymagania prawne dotyczące ochrony danych osobowych w modelu Cloud Computing?
- jakie nowe wyzwania prawne związane są z wdrożeniem architektury SOA, EDA, CEP,
- czy można korzystać z oprogramowania na podstawie innych umów niż licencja? Jakie są korzyści i ryzyka prawne związane z umowami dzierżawy oraz użytkowania majątkowych praw autorskich?
- czy istnieje coś takiego jak „leasing" oprogramowania?
- jak zgodnie z prawem odnosić korzyści podatkowe związane z „leasingiem" oprogramowania?
- co powinna zawierać umowa „leasingu" oprogramowania?
- czy można „przejmować" zawartość baz danych udostępnianych online?
- jak sporządzić umowę o udostępnienie zawartości baz danych?
- jak przygotować się do sporu sądowego dotyczącego projektów IT?
- o czym należy pamiętać w toku zawierania i wykonywania umowy IT, aby nie dać się zaskoczyć w przypadku ewentualnego sporu sądowego?

Więcej informacji: **www.cpi.com.pl**

Rejestr ryzyka czy „lista strachu" kierownika projektu?

Roman Bratek

W kompetencjach kierownika projektu w trakcie realizacji projektu można wskazać dwa główne obszary: zarządzanie tym, co zaplanowano do wykonania oraz zarządzanie tym, czego nie dało się zaplanować i znajduje się w obszarze niepewności projektu. Będzie to aktywność zarządcza, która obejmuje zarówno problemy związane z wykonywaniem bieżących prac i obsługę zmian, które są zgłaszane, jak też rozpoznawanie potencjalnych sytuacji, które, jeśli do nich dojdzie, będą miały znaczący wpływ na projekt. Przewidywanie i ocena ryzyka, czyli tego, co w projekcie może pójść nie tak, jak planowano lub oczekiwano, powinno stanowić istotną sferę aktywności operacyjnej kierownika projektu oraz uwagi komitetu sterującego (sponsora) przed podejmowaniem decyzji. Zarządzanie ryzykiem jest odpowiedzialnością kierownika projektu, wspomaganego zarówno przez członków zespołu projektowego jak też osoby z bezpośredniego otoczenia projektu (interesariuszy, czyli strony zainteresowane projektem: jego produktami lub korzyściami, które mają być osiągnięte).

Wszystkie organizacje deklaratywnie uznają wagę i znaczenie zarządzania ryzykiem dla powodzenia projektu. Praktyka pokazuje, że w przeważającej liczbie przypadków jakieś formy zarządzania ryzykiem są w projekcie prowadzone. Jednak rzadko mają one charakter systemowy, regularny, oparty o ustalone procedury. Dochodzi do sytuacji, gdy zarówno kierownik projektu jak i komitet sterujący minimalizują czas, przeznaczony na analizę i przeglądy ryzyka. W fazie przygotowania projektu przeprowadza się ocenę ryzyka, która nie jest później systematycznie powtarzana. W fazie realizacji przeważnie zastępuje ją wyłącznie pasywna reakcja na pojawiające się problemy. Projekty mierzą się zatem częściej ze skutkami zmaterializowanego ryzyka niż aktywnego zarządzania, zanim zagrożenie stanie się faktem, czyli zagadnieniem projektowym, które należy rozwiązać.

Jakość początkowych analiz ryzyka projektu zwykle pozostawia wiele do życzenia i obciążona jest istotnymi wadami. Wynikają one ze słabej znajomości natury projektu, braku informacji oraz narzędzi. Zdarza się, że analizy ryzyka prowadzone są przed planowaniem projektu, a jedynym wsparciem kierownika projektu i jego zespołu w identyfikacji zagrożeń jest intuicja oraz niezbyt dobrzej udokumentowane dane historyczne.

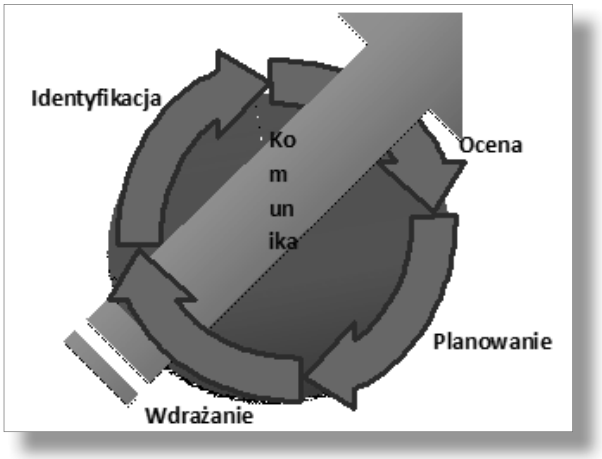
Najczęściej stwierdzanymi problemami, związanymi z przeprowadzaną we wstępnej fazie identyfikacją ryzyka projektu są:

1. Brak analizy kontekstu ryzyka, z którym zespół może zetknąć się w projekcie, słabe rozumienie priorytetów oraz akceptowalnych poziomów ryzyka u głównych interesariuszy projektu.
2. Identyfikowanie ogólnych (generycznych) czynników ryzyka, które przedstawiają typowe, a nie specyficzne dla tego projektu zagrożenia i ich źródła; wskazywanie jako ryzyka obszarów niepewności działań kierownika projektu lub jego obaw związanych z możliwościami realizacji powierzonej mu pracy.
3. Opisywanie ryzyka w postaci hasłowej, skróconej do równoważników zdania, które poprzez swoją niejednoznaczność lub możliwość interpretacji utrudniają komunikację i podejmowanie decyzji.
4. Ocena ryzyka przeprowadzana nieformalnie, w oparciu o intuicję i bez jasnych miar, pozwalających szacować ryzyko.
5. Brak wskazania dla zidentyfikowanych zagrożeń możliwych działań ograniczających ekspozycję na ryzyko, nieformalne lub domyślne akceptowanie ryzyka, nawet jeśli jest istotne dla projektu oraz brak dokumentowania działań, które postanowiono podjąć w celu mitygacji ryzyka.
6. Niejasne priorytety działań mitygujących , przez co zagrożenia, którymi się zarządza wynikają z obaw kierownika projektu (najczęściej dotyczących ryzyk związanych z realizacją) lub postrzegania hierarchii zagrożeń przez pryzmat ważności lub pozycji interesariuszy.

Powstająca w początkowej fazie projektu lista zagrożeń rzadko jest rozwijana do postaci pełnego rejestru ryzyka. Na poziomie decyzyjnym rozważane są ogólnikowo sformułowane potencjalne problemy, zaproponowane przez kierownika projektu, który kieruje się własnymi obawami lub „siłą głosu" poszczególnych interesariuszy. Zgromadzone informacje o ryzyku znacząco obniżają możliwość aktywnego i skutecznego przeciwdziałania zagrożeniom lub podejmowania efektywnych decyzji. Rejestr ryzyka nie staje się dla kierownika projektu oraz dla jego przełożonych wartościowym instrumentem wspomagającym decyzje. Ta pogłębia tendencję do pasywnego reagowania na problemy w trakcie realizacji projektu zamiast aktywnego rozpoznawania, a przede wszystkim przeciwdziałania zagrożeniom.

Na obronę kierownika projektu można powiedzieć, że zarzadzanie ryzykiem w projekcie jest pochodną całości zarządzania ryzykiem w organizacji. Jeśli firma nie ma odpowiednich narzędzi lub nie przykłada wagi do tego obszaru, to trudno oczekiwać, że w projekcie pojawi się inne podejście, skoro kierownik projektu jak i jego przełożeni, którzy tworzą komitet sterujący pochodzą z tej samej organizacji. Brak spójnego procesu zarzadzania ryzykiem, nieokreślone limity ryzyka, nieokreślone reguły decyzyjne i odpowiedzialności za zarządzanie ryzykiem nie wymuszają systematycznej analizy ryzyka w projekcie i nie działają motywująco na kierownika. Gdy uwzględni się wspomniane aspekty kulturowe np. indywidulaną niechęć do ryzyka, traktowanie wskazywania i raportowania zagrożeń, jako czarnowidztwo, postawę przełożonych, którą jakże trafnie opisuje powiedzenie: „wykonać, o trudnościach nie meldować…", to niska kultura i niekiedy bezradność kierownika projektu w zarządzaniu ryzykiem ukażą się w jeszcze szerszym świetle.

Tymczasem systematyczne stosowanie kilku metodycznych zasad pozwoliłoby uniknąć podstawowych problemów i błędów w tym obszarze. Punktem odniesienia będą tu koncepcje przedstawione w brytyjskiej metodyce zarządzania ryzykiem M_o_R®

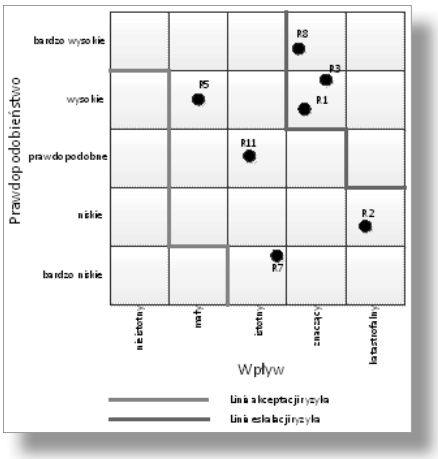


Rysunek 1. *Model procesów zarządzania ryzykiem zgodnie z M_o_R®*

(Management of Risk) należącej do Cabinet Office, reguły opisane w standardzie COSO oraz regulacje zawarte w normie ISO 31000.

Najczęściej przyjmowany model procesu zarzadzania ryzykiem prezentuje rysunek 1.

Osią modelu jest komunikacja, która ma kluczowe znaczenie dla całego procesu zarządzania ryzykiem, którego celem jest poprawienie skuteczności decyzji oraz obniżenie niepewności związanej z wytwarzanymi produktami lub zakładanymi rezultatami (korzyściami) projektu. Komunikacja jest niezbędna, aby pozyskać informacje potrzebne do identyfikacji zagrożeń, a także przekazać zespołowi lub organizacji decyzje, które zostały podjęte w związku z ryzykiem. Również pozostałe kroki procesu, czyli ocena ryzyka, planowanie, wdrażanie (oraz monitorowanie ryzyka i efektów działań) wymagają sprawnej komunikacji. Mechanizmy komunikacji, związane z zarządzaniem ryzykiem, określają następujące kwestie: od



Rysunek 2.

kogo pozyskać informacje o zagrożeniach, kogo i w jaki sposób poinformować o ich ocenie, jak raportować o zagrożeniach, do kogo i w jaki sposób eskalować informacje o zmianach i występować o decyzje.

Mechanizmy dotyczące komunikacji należy ustalić w momencie, gdy zespół projektowy przystępuje do przedsięwzięcia. W małych projektach wykorzystuje się zazwyczaj kanały i reguły codziennej komunikacji służbowej, powiązanej z zależnościami organizacyjnymi. W dużych, złożonych projektach mechanizmy komunikacji powinny być odrębnie przeanalizowane i uzgodnione z komitetem sterującym oraz głównymi interesariuszami projektu. Analiza kontekstu ma za zadanie dostarczyć wiedzy o potrzebach informacyjnych i regułach komunikacji. Powinna ona wskazać główne obszary i źródła zagrożeń, osoby, które mogą pomóc w ich identyfikacji, interesariuszy, którzy powinni być poinformowani o zagrożeniach. Ustala się częstotliwość gromadzenia oraz raportowania informacji o ryzyku. Konieczne jest określenie priorytetów mitygacji (istotność) poszczególnych rodzajów zagrożeń. Istotność zagrożeń związana jest z perspektywą, jaką członkowie komitetu sterującego oraz kluczowi interesariusze przyjmują w odniesieniu do poszczególnych celów projektu oraz z ich podejściem do ryzyka. Przykładowo, przedstawiciele kierownictwa mogą mieć niewielką skłonność do akceptowania zagrożeń istotnie wpływających na budżet projektu lub akceptować nawet duże zagrożenia dla przesuwania czasu realizacji lub oddziaływania na parametry techniczne/funkcjonalne produktów. Analizując kontekst ryzyka projektu, kierownik powinien ustalić z przełożonymi, jakie poziomy zagrożeń mogą być akceptowane, do jakiej wysokości ryzyka może nim zarządzać kierownik projektu, jaki poziom ekspozycji na ryzyko wymaga eskalacji decyzji do komitetu sterującego i uzyskania zatwierdzenia działań, podejmowanych przez kierownika projektu. Pomocnym narzędziem w tym zakresie może być mapa ryzyka. Pozwala ona wizualizować poziomy akceptacji oraz eskalacji zagrożeń i jednocześnie jest wygodną formą komunikacji i raportowania ryzyka. Przykład takiej mapy przedstawia rysunek 2. Poszczególne punkty na mapie to zagrożenia zapisane w rejestrze ryzyka, a ich położenie związane jest z prawdopodobieństwem wystąpienia oraz łącznym wpływem na projekt. Z uwagi na konieczność precyzyjnego wyznaczenia linii akceptacji i eskalacji, zazwyczaj stosuje się mapy o wymiarach 5x5 lub 6x6. Są one znacznie bardziej efektywne i przekazują więcej informacji niż mapy o wymiarze 3x3 (które z kolei są pomocne przy wstępnej selekcji wielu ryzyk).

Model procesu zarzadzania ryzykiem zbudowany wokół osi komunikacji dobrze oddaje cykliczny charakter działań podejmowanych w odniesieniu do zagrożeń. Ryzyko ma charakter dynamiczny stąd nie można poprzestać na jednokrotnym rozpoznaniu zagrożeń, powiązanych z decyzją o przygotowaniu projektu. Identyfikacja zagrożeń musi być przeprowadzana w różnych momentach cyklu życia projektu. Planowanie, wybór wykonawcy i podpisanie z nim umowy, uruchomienie prac specjalistycznych, wnioski o wprowadzenie zmian, zamykanie kolejnych etapów – każde z tych zdarzeń powinno wywoływać przegląd ryzyk już wcześniej zidentyfikowanych i opisanych.

Kierownik projektu i wspomagający go zespół projektowy sporządzają podczas początkowych prac (na etapie przygotowania) listę zagrożeń lub bardziej precyzyjnie – listę obszarów niepewności projektu. Często informacje o ryzyku mają postać zapisów, przedstawionych na poniższych przykładach:

a) „ryzyko opóźnienia dostawy produktu A”
b) „ryzyko niskich kompetencji zespołu wykonawczego w zakresie technologii X”

c) „ryzyko braku dostępu do zasobów z Departamentu Z podczas realizacji projektu"
d) „ryzyko opóźnienia projektu z powodu zmian w specyfikacji systemu"
e) „ryzyko opóźnień w przeprowadzeniu przetargu i wyborze wykonawcy"

Niekiedy do takiej listy zagrożeń, przeważnie używając skali trzystopniowej, zespół dopisuje ocenę, czy ryzyko jest małe, średnie lub duże. Dlaczego takie przedstawienie ryzyka projektu nie jest wystarczające? Przede wszystkim przytoczone w powyższych przykładach zapisy (podane w brzmieniu oryginalnym – pochodzą z rzeczywistych projektów) są ogólnikowe, nie wskazują przyczyn ryzyka, pomijają wpływ materializacji zdarzenia na projekt lub w zakresie wpływu odnoszą się wyłącznie do jednego parametru – czasu realizacji projektu. W takim ujęciu trudno określić, jak należy tym ryzykiem zarządzać, gdyż ogólnikowo przedstawione przyczyny lub potencjalne zdarzenia nie są wystarczającą podstawą do trafnych decyzji. Przykładowo, w odniesieniu do „ryzyka opóźnień w przeprowadzeniu przetargu i wyborze wykonawcy" nie wiadomo:

a) co jest przyczyną tego ryzyka,
b) czy skutek w postaci opóźnienia dotyczy całego projektu czy tylko konkretnego etapu, w którym dokonuje się wyboru wykonawcy,
c) czy opóźnienie wpłynie na budżet projektu,
d) czy ryzyko będzie miało wpływ na zakres/funkcjonalność lub jakość produktów.

Komunikacja na linii kierownik projektu – komitet sterujący lub kluczowi interesariusze może ulec dodatkowej komplikacji, gdy niejednoznaczne zapisy będą dawały adresatowi informacji możliwość interpretacji. W przykładzie b/, dotyczącym niskich kompetencji zespołu, trudno jest określić, czy autor zapisu traktuje niskie kompetencje jako domniemanie, czy też wie o niskich kompetencjach i ma na myśli skutki, do jakich może to doprowadzić. Ponadto, w takim zapisie niskie kompetencje można rozumieć jako **fakt**, a więc zapis ten kwalifikowałby się do rejestru zagadnień, a nie rejestru ryzyka. Kolejne pytania to: jakie są skutki niewielkich kompetencji zespołu wykonawczego w obszarze zastosowanej technologii– czy będą one związane z dużą liczba popełnianych błędów, problemami we wprowadzaniu zmian i poprawek, opóźnieniami w realizacji zaplanowanych prac? Kierownik projektu nie powinien zakładać, że jego przełożeni znają szczegóły projektu równie dobrze jak on sam – wielu pytań można uniknąć (i oszczędzić czas związany z wyjaśnieniami), dostarczając rzetelnego i użytecznego opisu ryzyka. Bardzo często również sam autor zapisu o ryzyku, przepytywany jakiś czas później przez swoich przełożonych o znaczenie zapisu, ma problem z wyjaśnieniem, co miał na myśli… Takie sytuacje podważają wiarygodność i zaufanie do kierownika projektu. Opisany powyżej problem problemów można zminimalizować stosując poniższy schemat opisu ryzyka:

„Przyczyna ryzyka" może spowodować „niepewne zdarzenie", które wywiera „skutek" na parametry projektu.

W tym schemacie:

- „przyczyna ryzyka" to opis faktów, przesłanek, czynników, które prowadzą do zagrożenia;
- „niepewne zdarzenie" to przedstawienie określonego potencjalnego zdarzenia;
- „skutek" przedstawia, jakie są ewentualne konsekwencje materializacji ryzyka dla projektu oraz jego celów.

Skorygowane opisy z podanych wcześniej przykładów mogłyby w rejestrze ryzyka zostać zapisane następująco:

1. Krótki czas przeznaczony na przygotowanie specyfikacji istotnych warunków zamówienia oraz braki w studium wykonalności mogą spowodować, że procedury przetargowe przeciągną się, a protesty i odwołania uczestników doprowadzą do opóźnień w wyłonieniu wykonawcy i przy niezmienionym czasie realizacji projektu, co wpłynie negatywnie na jakość wytwarzanego produktu [potencjalny wpływ na czas i jakość]
2. Niskie kompetencje zespołu wykonawczego w zakresie zastosowanej technologii mogą spowodować, że budowana aplikacja będzie miała dużo błędów krytycznych, których usuwanie i testowanie wydłuży przewidywany czas budowy rozwiązania o 3-4 miesiące i migracje danych o kolejny 1-2 miesiące, przez co nie uda się do końca bieżącego roku obsłużyć kluczowych klientów na nowej platformie internetowej. [wpływ na zakładane korzyści biznesowe].

W przypadku kilku powiązanych ze sobą przyczyn lub nakładających się zdarzeń, zespół powinien określić, które z nich ma największe oddziaływanie na cele projektu i wywoła najbardziej dolegliwe skutki. Dzięki tej informacji zarówno komitet sterujący, jak i kierownik projektu będą mogli ocenić, czy działania mitygujące mają skupić się na przyczynach ryzyka, ograniczyć ewentualny wpływ, czy są rozwiązania prowadzące do eliminacji ryzyka lub też czy ryzyko można przenieść na innych uczestników projektu. Warto przeanalizować, czy zidentyfikowane zagrożenie nie wzmacnia innych już znanych zagrożeń. W starym powiedzeniu: „nieszczęścia chodzą parami" jest sporo prawdy.

Ocena parametrów ryzyka następuje po identyfikacji zagrożenia. Polega ona na oszacowaniu prawdopodobieństwa materializacji, wpływu, czyli spodziewanych skutków materializacji ryzyka oraz bliskości. Wpływ rozumie się jako określenie przewidywanych skutków materializacji na czas/terminy realizacji przedsięwzięcia, budżet, zakres/jakość jego produktów, cele/korzyści przedsięwzięcia. Bliskość rozumiana jest jako przedział czasu, w którym może dość do materializacji ryzyka. Oceniając ryzyko należy określić, jaka jest jego istotność, czyli odnieść rozważane zagrożenie do innych już zidentyfikowanych zagrożeń oraz uzgodnionych limitów. Jeżeli ryzyko może zostać zaakceptowanie, należy to odnotować w rejestrze ryzyka oraz określić, kto i kiedy ma przeprowadzić ponowny przegląd tego zagrożenia. W przypadku, gdy ryzyko nie może zostać zaakceptowane, należy opracować odpowiednie plany działań mitygujących (plan reakcji na ryzyko). Mogą one prowadzić do eliminacji ryzyka, zmniejszenia prawdopodobieństwa lub skutków jego materializacji albo do przeniesienia ryzyka. W zależności od przyznanych uprawnień, kierownik projektu uruchamia realizację zaplanowanych działań lub zwraca się do przełożonych o autoryzację planów. Działania mogą być podejmowane niezwłocznie po ich zatwierdzeniu lub odłożone w czasie. W obydwu przypadkach kierownik projektu musi regularnie monitorować ryzyka i kontrolować skuteczność działań oraz status ryzyka. Służą do tego wskaźniki ryzyka, pozwalające badać, czy ekspozycja na konkretne ryzyko rośnie czy spada. Wskaźniki te są szczególnie pomocne, gdy uruchomiono już działania mitygujące. Posługując się nimi kierownik projektu ocenia, na ile efektywna jest przyjeta reakcja na ryzyko. Należy pamiętać, że mitygacja ryzyka pochłania koszty i absorbuje zasoby projektu. Jeśli nie jest skuteczna, czyli nie zmniejsza ryzyka, kierownik projektu ma obowiązek przeanalizować przyjętą linię postępowania. Oczekuje się, że zmieni sposób reakcji lub wprowadzi odpowiednie zmiany do planu działań mitygujących, aby osiągnąć zakładany cel, jakim jest zmniejszenie ekspozycji na ryzyko.

Opisywane w proponowany sposób ryzyko powinno zostać zanotowane w rejestrze ryzyka. Przechowuje on informacje

o zidentyfikowanych zagrożeniach, podjętych decyzjach i działaniach, będących reakcja na ryzyko. W kolejnych krokach procesu, uzyskane informacje są uzupełniane, zachowując historię zmian. Rejestr ryzyka jest więc dokumentem dynamicznym, pozwala śledzić działania zarządcze, oddaje stan wiedzy i zrozumienie wpływu każdego ze zidentyfikowanych zagrożeń na projekt. Rejestr wspomaga procesy decyzyjne zarówno na poziomie kierownika projektu jak i jego przełożonych. Wraz z mapą ryzyka oraz listami kontrolnymi, rejestr ryzyka pomaga zapanować na tym, co w projekcie nie mogło być zaplanowane i stanowiło obszar niepewności.

Organizacja cały czas uczy się zarzadzania ryzykiem, gromadzi doświadczenia, doskonali reakcje na ryzyko, zbiera informacje o wskaźnikach ryzyka. Jest to istotny aspekt związany z komunikacją, który realizuje się, wdrażając zaplanowaną reakcję na ryzyko.

Podsumowanie

Aby zarządzanie ryzykiem w projekcie było skuteczne i przynosiło spodziewane efekty należy:

1. Doprowadzić do wspólnego rozumienia zagrożeń projektu pomiędzy komitetem sterującym (sponsorem), głównymi interesariuszami, kierownikiem projektu i zespołem projektowym. Komunikacja jest kluczem do podejmowania trafnych decyzji, związanych z ryzykiem projektu. „Zamiatanie" zagrożeń pod dywan lub ich bagatelizowanie jest najbardziej ryzykownym sposobem postępowania.
2. Zagrożenia powinny być identyfikowane w sposób możliwie precyzyjny i jednoznaczny. Generyczne, ogólnikowe sformułowania nie wspomagają komunikacji i nie wspierają podejmowania decyzji. Nieprecyzyjne zapisy można skorygować w miarę postępów w zdobywaniu wiedzy o zagrożeniu natomiast informacje ogólnikowe zwykle pozostają niezmienione, a stojące za nimi zagrożenia nie są zarządzane.
3. Skuteczność w identyfikacji i ocenie ryzyka zależy nie tylko od umiejętności kierownika projektu i doświadczenia zespołu projektowego, ale również od wiedzy zgromadzonej po stronie organizacji. Taksonomie ryzyka, modele wspierające szacowanie, listy kontrolne ryzyka są nie tylko istotną pomocą, ale pozwalają również organizacji na gromadzenie doświadczeń, wprowadzanie ich do codziennej praktyki i przenoszenie jej pomiędzy projektami.
4. Ryzyko ma charakter dynamiczny i zmienia się w czasie. Ocena zagrożeń z jednorazowo przeprowadzonej analizy ryzyka na początku projektu, po zakończeniu pierwszego etapu realizacji może być w znaczącej części nieaktualna, zarówno w odniesieniu do samych zagrożeń jak i ich istotności. Przeglądy i ocena ryzyka powinny być realizowane regularnie i systematycznie.
5. Zarzadzanie ryzykiem w projekcie nie jest działaniem wymaganym wyłącznie przez metodyki lub dobre praktyki zarządcze, jako sztuka dla sztuki. Nawet najbardziej wnikliwa i rzetelna analiza, jeśli nie będzie przejrzana i wykorzystana przez decydentów, pozostanie wyłącznie kosztowną dodatkową działalnością zespołu projektowego. W efekcie, w krótkim czasie wartościowe informacje analityczne zostaną zastąpione ogólnikowym szumem informacyjnym, a oceny ekspozycji na ryzyko będą ujęte uniwersalnym słowem „średnie".

Roman Bratek - jest doświadczonym konsultantem i wieloletnim akredytowanym trenerem metodyk zarządzania projektami PRINCE2®i programami MSP®, które należą do brytyjskiego Cabinet Office. Jest pierwszym w Polsce akredytowanym trenerem metodyki zarządzania ryzykiem M_o_R®.

Metodyki zwinne a umowy wdrożeniowe – kilka uwag

Bohdan Widła

Zwinne metodyki – nie tylko w tworzeniu oprogramowania

Zwinne (*agile*) metodyki zarządzania projektami powstały jako nowa formuła tworzenia oprogramowania i remedium dla tradycyjnego podejścia, określanego jako kaskadowe (*waterfall*), w którym proces tworzenia oprogramowania przebiega w określonych etapach (od określenia wymagań, przez projekt i wykonanie, aż po testy, wdrożenie produkcyjne i utrzymanie). Podejście proponowane przez metodyki zwinne zakłada podział projektu na mniejsze iteracje, w ramach których oprogramowanie jest uzupełniane o kolejne elementy. Metodyki tego typu zdobywają coraz większą popularność, nie tylko przy realizacji projektów związanych z tworzeniem oprogramowania, ale także w projektach biznesowych. „Ideologiczne" podstawy zwinnych metodyk zostały zebrane w manifeście Agile, opublikowanym w 2001 r.[1] Manifest wyraża podstawowe założenia przyświecające tym metodykom w czterech tezach:

1. Ludzie i interakcje ponad procesy i narzędzia,
2. Działające oprogramowanie ponad obszerną dokumentację,
3. Współpracę z klientem ponad formalne ustalenia,
4. Reagowanie na zmiany ponad podążanie za planem[2].

Czytając manifest Agile, a zwłaszcza jego trzecią tezę, można odnieść wrażenie, że tworzenie i wdrażanie oprogramowania przy wykorzystaniu zwinnych metodyk nie tylko nie wymaga spisania umowy, ale wręcz się z nim kłóci. Takie ujęcie problemu byłoby jednak sporą przesadą. Manifest Agile powtarza tu raczej uniwersalną prawdę, dotyczącą wszystkich umów IT: to umowa ma służyć projektowi, a nie projekt umowie. Czy i w jaki sposób rosnąca popularność zwinnych metodyk może wpłynąć na praktykę pisania i negocjowania umów dotyczących wdrożeń systemów IT?

Czy coś się zmienia?

Na początku warto postawić pytanie, czy faktycznie można mówić tu o istotnych zmianach. Czy można wyobrazić sobie realizację wdrożenia, które z projektowego punktu

1 K. Beck i in., *Manifesto for Agile Software Development*, http://agilemanifesto.org

2 Cytat za polskim tłumaczeniem dostępnym na stronie http://agilemanifesto.org. Oryginalny tekst angielski wprost odwołuje się tu do negocjowania umów. Teza trzecia brzmi w nim: „Customer collaboration over contract negotiation".

widzenia będzie zarządzane zgodnie ze zwinną metodyką, w sytuacji gdy umowa napisana jest tak, jakby w projekcie funkcjonował tradycyjny, kaskadowy model? Oczywiście można, ale z dużym prawdopodobieństwem prowadziłoby to do klasycznego problemu rozbieżności pomiędzy treścią umowy a praktyką jej realizacji. Podstawowym założeniem zwinnych metodyk jest zapewnienie większej elastyczności w stosunku do tradycyjnych metodyk. Zderzenie „kaskadowej" umowy ze „zwinnym" projektem może łatwo doprowadzić do tego, że decyzje podejmowane przy zarządzaniu projektem nie będą zgodne z postanowieniami umowy, a jednocześnie z formalnego punktu widzenia nie będą stanowić jej zmiany. Przyczyną będzie zazwyczaj albo brak umocowania osób podejmujących decyzje, albo brak zachowania wymaganej formy (tu klasycznym przykładem jest podejmowanie decyzji o zmianach w formie e-mailowej, gdy umowa wymaga dla nich formy pisemnej pod rygorem nieważności).

Nawet jeśli stosunki między wykonawcą a zamawiającym są przyjazne, skutkiem mogą być problemy przy dokonaniu odbioru prac wykonawcy, skoro z prawnego punktu widzenia jest ona wykonana nienależycie (zamawiający otrzymał inne świadczenie, niż wynikało to z umowy). Wiele z nich może jednak albo nie wyjść na światło dzienne, albo dać się rozwiązać w nieskomplikowany sposób: poprzez odpowiednie porozumienie, albo potwierdzenie czynności „rzekomego pełnomocnika" zgodnie z art. 103 kodeksu cywilnego. Tego typu sytuacja może jednak łatwo doprowadzić do eskalacji wszelkich sporów realizacyjnych. Rozstrzygnięcie takiego sporu, zwłaszcza w sądzie, nie byłoby proste, a rezultaty nie byłyby łatwe do przewidzenia.

Jaki typ umowy?

Pojawiają się sugestie, że rozwój zwinnych metodyk pociąga za sobą rewolucję w świecie umów IT, polegającą na odejściu od ryczałtowej ceny, stałego harmonogramu i z góry określonych wymagań poprzez uelastycznienie przynajmniej jednego z tych czynników[3]. Na pierwszy rzut oka do filozofii zwinnych metodyk idealnie pasuje zatem umowa o świadczenie usług, które polegają na świadczeniu przez wykonawcę wsparcia w realizacji projektu wdrożenia systemu, realizowanego u zamawiającego[4]. Wszak zwinne metodyki kładą nacisk na współdziałanie wykonawcy z zamawiającym i elastyczne reagowanie na wyzwania pojawiające się w trakcie projektu, a nie na bezwzględne egzekwowanie wymagań i terminów. Na gruncie polskiego prawa byłaby to umowa o świadczenie usług, do której zgodnie z art. 750 kodeksu cywilnego stosuje się odpowiednio przepisy o zleceniu.

Taki model kontraktowania nie jest nowością na rynku IT, choć w ostatnich latach umowy tego typu nie należały do najpopularniejszych, a dominowały umowy oparte na modelu umowy o dzieło. Czy rosnąca popularność zwinnych metodyk może spowodować renesans umowy o świadczenie usług przy wdrażaniu systemów IT? Niektórzy entuzjaści zwinnych metodyk dochodzą wręcz do wniosku, że umowy o dzieło nie da się pogodzić ze zwinnymi metodykami[5]. Uważam tę ocenę za przesadzoną.

3 S. Atkinson, *Why the Traditional Contract for Software Development is Flawed*, Computer and Telecommunications Law Review 7/2010, s. 180.
4 Tamże.
5 S. Atkinson, *Why the Traditional Contract…..,* dz. cyt., s. 182.

W większości wypadków rezygnacja z umowy o dzieło na rzecz umowy o świadczenie usług oznacza większe ryzyko prawne po stronie zamawiającego i mniejsze ryzyko prawne po stronie wykonawcy, niż w przypadku zawarcia umowy o dzieło. Przepisy kodeksu cywilnego regulujące umowę o dzieło zdecydowanie faworyzują zamawiającego, co oczywiście wynika już z przyjętego dla niej modelu tzw. umowy rezultatu, a nie tzw. umowy starannego działania[6]. Dodatkowo, zamawiający ma do dyspozycji szereg silnych uprawnień. Bez szczegółowego omawiania można wymienić tu zwłaszcza prawo odstąpienia od umowy w razie opóźnienia w realizacji dzieła (art. 635 k.c.), prawo odstąpienia od umowy w razie wykonywania dzieła wadliwie lub sprzecznie z umową[7] (art. 636 k.c.), czy wreszcie rękojmię za wady dzieła, obejmującą uprawnienia do żądania naprawy wad, obniżenia wynagrodzenia lub odstąpienia od umowy (art. 637-638 k.c.).

Można spotkać się z poglądem, że odejście od „umów rezultatu" na rzecz umów usługowych nie powinno rodzić problemu, ponieważ w projekcie prowadzonym w oparciu o zwinne metodyki ryzyko spada wraz z postępem prac[8]. Jeśli to założenie okaże się prawdziwe, zawarcie umowy o świadczenie usług może faktycznie okazać się korzystniejsze m.in. z tego powodu, że w wynagrodzenie za realizację prac nie zostanie wliczona dodatkowa „premia za ryzyko". Trudno jednak akceptować takie uogólnienie bezkrytycznie.

Agile a umowa o dzieło

Rzeczywistość może okazać się daleka od modelu opisywanego w podręcznikach Agile. Po pierwsze, zwinne metodyki nie różnią się od pozostałych w tym sensie, że także z ich zasad w praktyce korzysta się wybiórczo. Po drugie, realizacja projektu w oparciu o zwinną metodykę z definicji zakłada większe współdziałanie ze strony zamawiającego, który z kolei nie zawsze będzie dysponował zasobami, aby takie współdziałanie zapewnić. Po trzecie, teza o zmniejszaniu się ryzyka wraz z postępami w pracach może oczywiście okazać się fałszywa. Wszystko to powoduje, że model, w którym dostawca jest jedynie „partnerem we wdrażaniu", a nie „wykonawcą systemu" nie musi sprawdzić się w praktyce. Wreszcie po czwarte, zamawiający może po prostu być zainteresowany utrzymaniem korzystniejszej pozycji, jaką daje umowa o dzieło.

Aby jednak zawarcie umowy o dzieło, której przedmiotem będzie realizacja wdrożenia zgodnie ze zwinnymi metodykami, nie przyniosło więcej szkód niż korzyści, trzeba dostosować ją do nowych realiów. Słowem-kluczem jest elastyczność. Konieczne wydaje się zwłaszcza wprowadzenie mechanizmu, który pozwoli korygować zakres prac w możliwie prosty sposób, na przykład w drodze porozumienia kierowników projektu, a nie sformalizowanego aneksu do umowy. Innymi słowy, umowa powinna być prawniczą

6 Choć pojęcia te nie mają umocowania ustawowego i funkcjonują jako swego rodzaju skróty myślowe, dobrze oddają fakt cechy obydwu umów: w przypadku umowy o dzieło przyjmujący zamówienie zobowiązuje się osiągnąć oznaczony efekt (umowa rezultatu), a w przypadku umowy o świadczenie usług usługodawca ma je świadczyć z należytą starannością, ale nie musi osiągnąć efektu (umowa starannego działania). Por. P. Machnikowski w: E. Gniewek, *Kodeks cywilny. Komentarz*, wyd. 2, Warszawa 2007, s. 1167.

7 Przepis ten przyznaje także prawo poprawienia lub dalsze wykonania dzieła innej osobie na koszt i niebezpieczeństwo przyjmującego zamówienie, jednak w praktyce umów IT uprawnienie to ma mniejsze znaczenie, głównie z uwagi na to, że skorzystanie z niego wymaga odpowiednio szerokich uprawnień do korzystania z oprogramowania.

8 Por. C. Larman, B. Vodde, *Practices for Scaling Lean & Agile Development: Large, Multisite, & Offshore Product Development with Large-Scale Scrum*, Boston 2010, s. 499 i nast.

implementacją tego, co i tak ma miejsce w trakcie realizacji projektu zgodnie z pryncypiami Agile. Celem jest doprowadzenie do stanu, w którym obowiązki wynikające z umowy odpowiadają aktualnym uzgodnieniom projektowym i treści poszczególnych wymagań (historii użytkownika, czyli *user stories*). Bardziej elastyczna struktura projektu, a zwłaszcza charakterystyczny dla zwinnych metodyk podział prac na iteracje (sprinty), ma wpływ także na kształt harmonogramu realizacji umowy. Zamiast rozbudowanego harmonogramu pojawia się wskazanie tylko kluczowych dat, z pozostawieniem decyzji co do szczegółowego podziału prac na sprinty w gestii zespołu projektowego. Oczywiście jeśli „uelastycznianie" umowy przekroczy rozsądne granice, może okazać się, że korzyści wynikające z przyjęcia modelu umowy o dzieło stają się iluzoryczne. Ryzykowne z punktu widzenia zamawiającego są zwłaszcza mechanizmy, które zmniejszają kontrolę nad kosztami, albo dają wykonawcy ostatnie słowo w kwestii zakresu prac.

Ważnym elementem jest także ustalenie zasad współdziałania zamawiającego w realizacji umowy. Zastosowanie zwinnej metodyki z założenia oznacza, że personel zamawiającego będzie bardziej aktywnie uczestniczył w pracach wdrożeniowych. Z punktu widzenia wykonawcy, konieczne jest zapewnienie sprawnego procesu podejmowania decyzji i udziału kompetentnych osób w zespole projektowym. Z kolei zamawiający powinni ostrożnie podchodzić do klauzul, z których wynikałoby, że prace realizowane są przez obie strony w równym stopniu. Po pierwsze, łatwo sformułować je w taki sposób, że odpowiedzialność za osiągnięcie rezultatu będzie rozmyta między zamawiającym a wykonawcą, a wówczas wykonanie dzieła może być przedmiotem umowy już tylko z nazwy[9]. Po drugie, takie sformułowanie postanowień umowy byłoby trudne do pogodzenia z przepisami o zasadach wykonywania zobowiązań. Współdziałanie w realizacji umowy nie jest długiem w rozumieniu art. 353 k.c.[10]. Nie można też utożsamiać współdziałania z wspólną realizacją tego samego świadczenia przez dłużnika i wierzyciela (w tym wypadku przez zamawiającego i wykonawcę).

Kolejne problemy pojawiają się w kontekście umów zawieranych w reżimie prawa zamówień publicznych[11]. W tym wypadku, postulat rezygnacji z odgórnego planowania na rzecz elastycznego reagowania zderza się z zupełnie innym podejściem wynikającym zwłaszcza z art. 144 ust. 1 pzp. Przepis ten dopuszcza istotne[12] zmiany umowy tylko w wypadkach, w których możliwość dokonania zmian oraz ich warunki zostały przewidziane w postanowieniach ogłoszenia o zamówieniu lub specyfikacji istotnych warunków zamówienia. Trudno także odstąpić od precyzyjnego opisania przedmiotu zamówienia, skoro wprost wymaga tego art. 29 ust. 1 pzp. Co więcej, choć jest to kontrowersyjny pogląd, zdaniem części doktryny każde rozszerzenie przedmiotu zamówienia wymaga wszczęcia nowego postępowania o udzielenie zamówienia publicznego[13]. Tym samym, nawet pomijając praktyczne problemy związane

9 Np. „Strony wdrożą system…" albo „Zespół projektowy wdroży system", gdzie zespół projektowy tworzą członkowie personelu zamawiającego i wykonawcy.

10 Por. F. Zoll w: A. Olejniczak, *System Prawa Prywatnego. Tom 6. Prawo zobowiązań – część ogólna. Suplement*, Warszawa 2010, s. 215-216.

11 Ustawa z 29 stycznia 2004 r. – Prawo zamówień publicznych; dalej jako pzp.

12 Na ten temat por. wyrok ETS z dnia 19 czerwca 2008 r. w sprawie C-454/06 (Pressetext. Nachrichtenagentur GmgH przeciwko Austrii).

13 Zob. G. Wicik, P. Wiśniewski, *Prawo zamówień publicznych, Komentarz*, Warszawa 2007, s. 687 oraz P. Granecki, *Prawo zamówień publicznych. Komentarz*, Warszawa 2007, s. 347.

ze stosowaniem zwinnej metodyki w instytucji publicznej, przepisy prawa zamówień publicznych mogą być bardzo istotną przeszkodą w zastosowaniu takiego podejścia do realizacji projektu.

Podsumowanie

Decyzja o realizacji projektu przy użyciu zwinnej metodyki nie oznacza, że wszystkie wypracowanej do tej pory standardy co do treści i struktury umów IT powinny trafić na śmietnik historii. Jednak bezrefleksyjne zastosowanie starych wzorców w projekcie realizowanym „zwinnie" raczej nie ułatwi pracy, a z dużym prawdopodobieństwem ją utrudni. Przygotowując umowę, której przedmiotem jest wdrożenie oprogramowania w modelu Agile, można zastosować szereg konstrukcji, a o ich wyborze za każdym razem powinny decydować uwarunkowania konkretnego projektu. Nie można też zapominać o regule, która jest aktualna nie tylko dla umów wdrożeniowych: ceną za elastyczność jest zwykle zwiększenie ryzyka prawnego. Powinno być to jednak skutkiem świadomej decyzji.

Metodyki zwinne a umowy wdrożeniowe – kilka uwag

Streszczenie:

Treść manifestu Agile, a zwłaszcza jego trzecia tezę, może sprawiać wrażenie, że tworzenie i wdrażanie oprogramowania przy wykorzystaniu zwinnych metodyk nie wymaga spisania umowy. Takie ujęcie problemu byłoby jednak sporą przesadą. Manifest Agile powtarza tu raczej uniwersalną prawdę, dotyczącą wszystkich umów IT: to umowa ma służyć projektowi, a nie projekt umowie. Celem artykułu jest próba oceny, czy i w jaki sposób rosnąca popularność zwinnych metodyk może wpłynąć na praktykę pisania i negocjowania umów dotyczących wdrożeń systemów IT?

A few remarks on agile methodologies and IT implementation contracts

Abstract:

The Agile manifesto, especially its third thesis, might suggest that developing and implementing software while using an agile methodology does not require writing down a contract. Such approach would be grossly exaggerated. The Agile manifesto reiterates a truth, which is rather universal for all IT contracts: the contract's purpose is to serve the project, not the other way around. The article aims to assess if and in what way will the growing popularity of agile methodologies change the practice of drafting and negotiation IT implementation contracts.

Bohdan Widła - absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnik w kancelarii Maruta i Wspólnicy sp. j., aplikant radcowski. Autor publikacji w czasopismach naukowych i branżowych z zakresu prawa własności intelektualnej i prawa zamówień publicznych.

Zapraszamy do udziału

KONFERENCJA

IX edycja konferencji w cyklu BADANIA NAUKOWE - NOWE PROCEDURY AWANSÓW NAUKOWYCH STAN PRAWNY OD 1 PAŹDZIERNIKA 2013 R.

Warszawa, 17.09.2013

Prowadzenie obrad: dr Emanuel Kulczycki

Więcej informacji: **www.cpi-sk.pl**

Czy definicja „administratora danych" wymaga zmian?

Damian Karwala

Obowiązująca aktualnie regulacja w zakresie ochrony danych osobowych – tak krajowa, jak i unijna – w aspekcie podmiotowym jej zastosowania wymienia administratora danych oraz podmiot przetwarzający dane na zlecenie/„w imieniu" administratora (ang. *data processor*). Rozróżnienie to oraz właściwa kwalifikacja podmiotów zaangażowanych w przetwarzanie danych osobowych ma daleko idące skutki. Decyduje bowiem o zakresie odpowiedzialności za przetwarzane dane (zasadniczą jej część nakładając na administratora danych), wyznacza prawo właściwe dla operacji przetwarzania danych, wpływa na sposób realizacji praw przysługujących osobom, których dane dotyczą, itd. Zgodnie z tym „klasycznym" podziałem pierwsza grupa podmiotów – administratorzy danych – decydują o przetwarzaniu danych osobowych, inicjują ich przetwarzanie, lub – jak stanowi art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] – decydują „o celach i środkach przetwarzania danych" (zob. również art. 2 lit. d) dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2]). Przy takim ujęciu podmioty zaliczane do drugiej grupy (przetwarzający dane) występują jako strony „pasywne", które nie powinny posiadać wpływu na sposób w jaki dane są przetwarzane.

Wydaje się jednak, iż założenie o biernej roli podmiotów przetwarzających dane (*processorów* danych) oraz oparcie się o tak zarysowany, stosunkowo prosty podział podmiotów uczestniczących w przetwarzaniu danych osobowych, nie jest już właściwe. Założenie to nie wytrzymuje „próby czasu", sam podział natomiast zamazuje się w świetle aktualnych praktyk gospodarczych i rozwijających się technologii[3]. Doskonałego przykładu dostarcza w tym zakresie fenomen przetwarzania danych „w chmurze" (chmura obliczeniowa, ang. *cloud computing*), w ramach której to technologii *processorzy* danych wywierają znaczący wpływ na to, w jaki sposób dane są przetwarzane. Podmioty przetwarzające (usługodawcy usług świadczonych „w chmurze") decydują o środkach

1 Tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.; dalej jako „u.o.d.o.".

2 Dz. U. UE L nr 281, s. 31 z 23.11.1995 r., dalej jako „Dyrektywa" lub „Dyrektywa 95/46/WE".

3 Por. Ch. Kuner, *European Data Protection Law. Corporate Compliance and Regulation*, Oxford University Press, 2007, s. 71-72; B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, *Social networks and web 2.0: are users also bound by data protection regulations?*, 2009, s. 68-69.

przetwarzania danych, a nawet w pewnym sensie określają (predefiniują) cele, dla jakich dane osobowe są przez klientów tego rodzaju usług (tzn. przez administratorów danych) przetwarzane. Ma to ścisły związek z określonym produktem oferowanym „w chmurze", np. w sytuacji gdy jest nim system do obsługi kadrowo-płacowej lub systemy klasy CRM (ang. *customer relationship management*)[4].

Nie dziwi zatem, że coraz częściej – nawet wśród największych podmiotów oraz samych organów ochrony danych – pojawiają się poważne problemy z właściwą oceną i kwalifikacją poszczególnych „aktorów" uczestniczących w procesie przetwarzania danych osobowych. Przykładowo, w głośnej przed kilku laty sprawie dotyczącej SWITF (Society for Worldwide Interbank Financial Telecommunication), sam zainteresowany (SWIFT) był przekonany, że występuje jako podmiot przetwarzający dane na zlecenie (*processor* danych). W efekcie natomiast przeprowadzonego postępowania podmiot ten został zakwalifikowany jako administrator danych, nie bez pewnych jednakże wątpliwości.[5] Podobnie Google, który w trakcie wykonywania zdjęć do projektu Street View zebrał również dane pochodzące z sieci bezprzewodowych (z ok. 3,6 miliona routerów Wi-Fi w samej tylko Holandii) argumentował, że nie powinien być uznawany za administratora danych, ponieważ nie było po jego stronie intencji przetwarzania tych danych. Odmienną kwalifikację przyjął organ holenderki, uznając Google za administratora danych, a w konsekwencji stwierdzając naruszenie przez spółkę przepisów o ochronie danych osobowych, m.in. w zakresie właściwych podstaw przetwarzania danych oraz realizacji obowiązku informacyjnego[6].

W celu „dopasowania" funkcjonujących obecnie definicji podmiotów zaangażowanych w operacje przetwarzania danych osobowych do zmienionych uwarunkowań, podejmowane są różnego rodzaju zabiegi interpretacyjne. W szczególności wskazuje się na konieczność przyjmowania szerokiego rozumienia pojęcia „środki przetwarzania danych" (art. 7 pkt 4 u.o.d.o.; oraz jego odpowiednik - „means" na gruncie wersji angielskojęzycznej Dyrektywy 95/46/WE). I tak, Grupa Robocza Art. 29 Dyrektywy – w podstawowej w tym zakresie opinii z 2010 r. – proponuje, aby nie odnosić go wyłącznie do technicznych aspektów przetwarzania danych osobowych, ale także do tego „jak" (w jaki sposób) odbywa się przetwarzanie, co obejmuje takie zagadnienia jak: „jakie dane się przetwarza", „jakie osoby trzecie mają dostęp do tych danych", „kiedy usuwa się dane", itd. Tym samym – jak wskazuje Grupa Robocza – określanie to powinno obejmować *„zarówno kwestie techniczne i organizacyjne, gdy podejmowanie decyzji można przekazać przetwarzającym (np. „z jakiego sprzętu komputerowego i oprogramowania korzystać?"), jak i zasadnicze elementy, które*

4 Grupa Robocza Art. 29 Dyrketywy, *Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej*, przyjęta 1 lipca 2012 r., WP 196, s. 9-10; zob. również F. Gilbert, *Cloud Service Providers as Joint-Data Controllers*, Journal of Internet Law, sierpień 2011.

5 Grupa Robocza Art. 29 Dyrketywy, *Opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Woldwide Interbank Financial Telecommunication, SWIFT)*, przyjęta 22 listopada 2006 r., WP 128, s. 12-14.

6 Holenderski organ ochrony danych (College beschermingpersoonsgegevens, CBP), *Final findings. Dutch Data Protection Authority investigation into the collection of Wifi data by Google using Street View cars*, 7.12.2010 r., dokument dostępny pod adresem: http://www.dutchdpa.nl/downloads_overig/en_pb_20110811_google_final_findings.pdf.

w tradycyjny i nieodłączny sposób określa administrator danych, takie jak „które dane się przetwarza?", „jak długo się je przetwarza?", „kto ma do nich dostęp?" itd.[7]*".*

Tym samym – o ile możliwość decydowania o „środkach" (ale wyłącznie w wąskim zakresie, tzn. w odniesieniu do kwestii technicznych i organizacyjnych, nie zaś w kontekście „zasadniczych elementów") nie jest odnoszona wyłącznie w stosunku do administratora danych, lecz odnosi się również do podmiotów przetwarzających – o tyle możliwość decydowania o „celach" przetwarzania pozostawiana jest wyłącznie po stronie administratora. Jak bowiem pokreśliła Grupa Robocza Art. 29, określenie „celu" przetwarzania jest zastrzeżone dla „administratora danych". Oznacza to, że *„administrator danych może przekazać określanie „sposobów" przetwarzania w odniesieniu do kwestii technicznych lub organizacyjnych. Zasadnicze* [natomiast] *kwestie dotyczące sedna zgodności przetwarzania danych z prawem należą do administratora danych*[8]*".*

Proponowane podejście prowadzić może w rezultacie do odczytania warunku zawartego w aktualnej definicji „administratora danych" – wbrew dosłownemu brzmieniu tej definicji – jako „decydowanie o celach lub środkach przetwarzania danych", nie zaś jako „decydowanie o celach i środkach przetwarzania danych". Decydowanie bowiem o środkach przetwarzania danych – bez względu na to, jakie znaczenie i zakres nadamy temu pojęciu – nie jest traktowane jako „zastrzeżone" dla administratora danych. Określony zaś podmiot, aby był uznany za administratora, nie musi decydować o środkach przetwarzania danych, może decydować jedynie o celach takiego przetwarzania.

Powyższe pokazuje również, że dokonanie jednoznacznego rozróżnienia pomiędzy administratorami danych a podmiotami przetwarzającymi (*processorami*) staje się obecnie coraz trudniejszym zadaniem. Dostrzega to zresztą również Grupa Robocza Art. 29 Dyrektywy 95/46/WE, zwracając uwagę na *„trudności w stosowaniu definicji użytych do celów dyrektywy w złożonych okolicznościach, w których można przewidzieć wiele scenariuszy samodzielnego lub wspólnego funkcjonowania administratorów danych i przetwarzających, przy różnym stopniu autonomii i odpowiedzialności"*. Grupa Robocza *„nie znalazła jednak powodów, aby przypuszczać, że obecne rozróżnienie między administratorami danych i przetwarzającymi nie będzie już w tej perspektywie odpowiednie i użyteczne*[9]*"*. Również Komisja Europejska nie dostrzegła konieczności odejścia od funkcjonującego w tym zakresie modelu. Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (tzw. ogólne rozporządzenie o ochronie danych)[10] zachowuje bowiem tradycyjny podział na administratorów oraz *processorów* danych. Zgodnie z art. 4 pkt 5 projektu rozporządzenia, „administrator" to *„podmiot, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych; w przypadkach, w których cele, warunki i sposoby*

7 Grupa Robocza Art. 29 Dyrketywy, *Opinia 1/2010 w sprawie pojęć « administrator danych » i « przetwarzający »*, przyjęta 16 lutego 2010 r., WP 169, s. 15.

8 Tamże, s. 16.

9 Tamże, s. 36.

10 *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final; opublikowany dnia 25 stycznia 2012 r.

ustalane są prawem Unii lub państwa członkowskiego, administrator lub szczególne kryteria jego wyznaczania mogą zostać określone w prawie Unii lub państwa członkowskiego"; natomiast „podmiot przetwarzający" oznacza *„osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, który przetwarza dane osobowe w imieniu administratora"* (art. 4 pkt 6).

O ile zgodzić należy się z zachowaniem tego „klasycznego" podziału na administratora danych oraz *processora* danych[11], o tyle zastrzeżenia budzi sam sposób zdefiniowania tych kluczowych dla całej regulacji konstrukcji prawnych. Projekt ogólnego rozporządzenia w art. 4 pkt 5 dodaje bowiem do definicji „administratora danych" wymóg decydowania również o „warunkach" (ang. *conditions*) przetwarzania danych osobowych. W tym kontekście w szczególności nie jest jasne, jak należy rozumieć termin „warunki", tzn. czy obejmował będzie on odpowiedzi na pytanie o to „jak" dane są przetwarzane, czy też należy nadawać mu inne (ale jakie?) znaczenie. Po drugie, na co należy zwrócić uwagę, a co może rodzić nawet większe trudności praktyczne, zaproponowana w projekcie rozporządzenia definicja „administratora" posługuje się nadal spójnikiem „i". Oznacza to, że kwalifikacja określonego podmiotu, jako administratora danych, wymagać będzie łącznego spełnienia wymogu decydowania o celach, środkach, jak również o warunkach przetwarzania danych osobowych. W tym zakresie pojawia się również pytanie, czy możliwe będzie „delegowanie" na podmiot przetwarzający dane prawa do decydowania nie tylko o „środkach" przetwarzania, lecz również o ich „warunkach". Nawet jednak jeśli dopuści się taką możliwość, zaproponowane brzmienie definicji nie pozwala na jednoznaczne wskazanie, jaka jest podstawa dla takiej „delegacji" oraz jej ewentualny zakres.

Zamiast powyższego, zaproponować można odmienne rozwiązanie, tj. ograniczenie czynników przesądzających o kwalifikacji danego podmiotu, jako administratora danych, wyłącznie do „celów" przetwarzania. Takie rozwiązanie oznaczałoby rezygnację z przesłanki „środków" (oraz zaproponowanej przez Komisję przesłanki „warunków"), jednak wydaje się, iż pozwoliłoby to uniknąć przynajmniej części z pojawiających się obecnie trudności. Wydaje się, że pozwoliłoby to również na lepsze odzwierciedlenie występujących praktyk biznesowych i aspektów technologicznych, czy organizacyjnych. Rezygnacja w ramach definicji „administratora danych" z przesłanki „środków" przetwarzania danych wydaje się tym bardziej wskazana, bowiem:

- istnieją obecnie zasadnicze wątpliwości, jak należy rozumieć przesłankę „środków", co utrudnia odkodowanie definicji „administratora danych" oraz wyznaczenie możliwie precyzyjnej granicy pomiędzy administratorem a podmiotem przetwarzającym dane;
- już na gruncie aktualnie obowiązującej regulacji nadaje się większe znaczenie przesłance „decydowania o celach" niż warunkowi „decydowania o środkach" przetwarzania danych osobowych; jak zauważa się w doktrynie europejskiej, *„spośród tych dwóch elementów, Grupa Robocza kładzie większy nacisk na decydowanie przez administratora o przeznaczeniu (celu), niż na decydowanie o środkach*[12]*"*;

11 Zuważyć jednak należy, że w doktrynie europejskiej zgłaszane są również propozycje odejścia od tego podziału ; por. W.K. Hon, Ch. Millard, I. Walden, *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011.

12 Zuważyć jednak należy, że w doktrynie europejskiej zgłaszane są również propozycje odejścia od tego podziału ; por. W.K. Hon, Ch. Millard, I. Walden, *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011.

- Grupa Robocza Art. 29 Dyrektywy dopuszcza nawet możliwość „delegowania" na *processora* danych kompetencji w zakresie decydowania o środkach (przynajmniej w wąskim znaczeniu tego pojęcia), tym samym potwierdzając mniejsze znaczenie tego czynnika, w kontekście definiowania instytucji „administratora danych",
- generalne znaczenie „celu" przetwarzania danych jest na gruncie regulacji dotyczącej ochrony danych osobowych o wiele większe (by nie powiedzieć – kluczowe), gdyż m.in. – jak zasadnie podnosi się w doktrynie – *„wpływa ono na określenie zakresu obowiązków administratora, jak również ma znaczenie przy całościowej ocenie zasadności i/lub proporcjonalności przetwarzania*[13]*"*.

W ramach trwających obecnie prac legislacyjnych nad ogólnym rozporządzeniem o ochronie danych, prowadzonych w Parlamencie Europejskim, proponuje się wprowadzenie w tym zakresie odpowiednich zmian. Rezygnację z przesłanki w postaci „środków" oraz „warunków" przetwarzania danych osobowych (i pozostawienie w definicji „administratora" jedynie wymogu decydowania o „celach" przetwarzania danych) zaproponowano m.in. w opinii Komisji Rynek Wewnętrzny i Ochrona Konsumentów (IMCO)[14] oraz w opinii zgłoszonej przez Komisję Prawo (JURI)[15]. Analogicznej zmiany nie przewiduje jednak – co ciekawe – tzw. „raport Albrechta". Na obecnym etapie nie sposób zatem przesądzić w jakim kierunku potoczą się prace nad zdefiniowaniem kluczowej dla całej regulacji konstrukcji administratora danych. W ocenie autora zmiany te są jednak konieczne, w kierunku proponowanym powyżej.

Damian Karwala - radca prawny przy Okręgowej Izbie Radców Prawnych w Krakowie, współpracujący z Kancelarią Prawną Traple Konarski Podrecki i Wspólnicy sp.j.

13 Tamże, s. 31, przypis dolny 55.

14 *Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)),* z 28 stycznia 2013 r. W opinii tej – jako uzasadnienie dla takiego rozwiązania – podano: *"With new technologies and services available such as cloud computing traditional division of entities involved in the processing of personal data may prove difficult, with the processor having in such cases significant influence over the way in which data are being processed. For this reason it seems reasonable to determine the controller as the entity, which decides over the purpose of processing personal data as determination of finality is the most important decision with the other factors serving as means to achieve* it" (s. 42).

15 *Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))*, z 25 marca 2013 r.

16 Committee on Civil Liberties, Justice and Home Affairs, sprawozdawca: Jan Philipp Albrecht, *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))*, wersja z 16 stycznia 2013 r., 2012/0011(COD).

6-7 listopada 2013 r., Poznań

www.konferencja-eab.pl

Organizatorzy:

Pod nazwą „**e-Administracja dla Biznesu"** 6-7 listopada w Poznaniu zostanie zorganizowana **konferencja, której celem jest stworzenie platformy wymiany informacji** o rządowych planach **rozwoju oraz potrzebach i problemach świata biznesu w obszarze e-gospodarki.**

Przy organizacji konferencji swoje siły połączyły Ministerstwo Gospodarki i **Ministerstwo Administracji i Cyfryzacji** oraz **Instytut Logistyki i Magazynowania**, który jest inicjatorem wydarzenia.

Konferencja ma umożliwić wypracowanie i przekazanie do administracji państwowej oczekiwań biznesu oraz niezbędnych rozwiązań w zakresie kierunków rozwoju e-gospodarki w Polsce.
Ważnym punktem konferencji będą także prezentowane dobre praktyki, rozwiązania i wdrożenia z zagranicznych rynków, które mogą się stać inspiracją, jak i wzorem do naśladowania. Na konferencje zostali zaproszeni prelegenci z krajów, które są liderami w obszarze gospodarki elektronicznej. Konferencja to nie tylko wystąpienia ekspertów, panele dyskusyjne oraz prezentacje dobrych praktyk, to również warsztaty, podczas których przedstawione zostaną nowe rozwiązania dedykowane samorządom oraz wystawa, która ma prezentować doświadczenia samorządów w zakresie e-administracji oraz nowe rozwiązania dedykowane samorządom.

Pierwsza edycja konferencji poświęcona będzie tematowi elektronicznej administracji. Od wielu lat szuka się sposobów na uzdrowienie administracji publicznej i budowę jej elektronicznej odmiany. Dotychczas fundusze wydane na jej rozwój nie dają tak spektakularnych efektów, jakich można byłoby się spodziewać. Przyczyn takiego stanu rzeczy można się doszukiwać między innymi w braku współpracy pomiędzy administracją a biznesem i tworzeniem usług, które nie są poparte analizą potrzeb przedsiębiorców.

Konferencja adresowana jest do przedstawicieli administracji rządowej i samorządowej, w szczególności wdrażających politykę informatyzacji państwa oraz realizujących procedury administracyjne. **Na konferencję zapraszamy również przedstawicieli biznesu działających na styku z administracją** oraz **instytucje otoczenia** biznesu.

Patronat honorowy nad konferencją objęło Ministerstwo Sprawiedliwości, Polska Agencja Rozwoju Przedsiębiorczości, Krajowa Izba Gospodarcza, Związek Banków Polskich, Marszałek Województwa Wielkopolskiego Marek Woźniak, Prezydent Miasta Poznania Ryszard Grobelny oraz Związek Miast Polskich.

Więcej informacji o konferencji: **www.konferencja-eab.pl**

Kontakt z prasą:
Ilona Kużaj-Aydar
Instytut Logistyki i Magazynowania
www.ilim.poznan.pl
T +48 61 850 49 30, M +48 605 539 717,
ilona.kuzaj-aydar@ilim.poznan.pl

Edwin Bendyk

Koniec utopii

Internet od dawna jest narzędziem politycznych zmagań w systemach demokratycznych. I od dawna też służy politycznej walce w krajach znajdujących się pod władzą reżimów autokratycznych. Optymiści wierzący w emancypacyjną moc technologii przekonywali, że wraz z upowszechnieniem się nowych mediów spragnieni wolności ludzie podniosą głowy i zmiotą dyktatorów. Trudno o lepsze przykłady, niż przewroty w Tunezji i Egipcie, zwane Arabską Wiosną i jednocześnie też fecabookowymi rewolucjami.

Kolejno upadały rządy Ben Aliego i Mubaraka, a świat czekał kto następny czeka w kolejce do politycznej gilotyny. Wypadło na Kadafiego, tyrana Libii, tylko że władzę (i życie) nie zabrał mu Internet, lecz zbrojna interwencja zainicjowana przez Francję. O Syrii nie wspomnę. Iran, miejsce Zielonej Rewolucji przełomu 2009 i 2010 roku szykuje się właśnie do kolejnych wyborów prezydenckich. Już jednak widać, że w tym przynajmniej kraju Internet zamiast obalić władzę, stał się doskonałym narzędziem kontroli społeczeństwa.

Nowocześni tyranii wiedzą, że nie mogą sobie pozwolić na całkowite odcięcie kraju od cyfrowej łączności – to zbyt kosztowne dla gospodarki. I nieefektywne polityczne, bo irytuje znaczną część internautów, którzy mają gdzieś politykę i zaczynają protestować dopiero wówczas, gdy ktoś im zabierze dostęp do WWW. Przekonał się o tym Hosni Mubarak, który nieopatrznie wprowadził internetowy blackout i w rezultacie grono protestujących na Placu Tahrir szybko powiększyło się o wściekłych użytkowników Sieci.

Władze Iranu szybko się uczą sieciowej logiki i wiedzą, że nowoczesne narzędzia umożliwiają precyzyjne „targetowanie" przeciwników. Nie ma potrzeby wyłączać dostępu do YouTube, wystarczy ograniczyć dostęp zlokalizowanym i wybranym wrogom systemu. Narzędzia są coraz doskonalsze, do niedawna w ich produkcji specjalizowały się firmy zachodnie, chętnie zresztą sprzedające swoje technologie każdemu, kto gotów był zapłacić. Świat idzie jednak do przodu i dziś Iran nie jest ograniczony do rozwiązań z Europy, może skorzystać z życzliwości i rosnących kompetencji Chin.

Eric Schmidt i Jared Cohen z Google'a w wydanej niedawno książce „The New Digital Age" piszą, że widać wyraźnie postępującą bałkanizację Internetu. Dyktatorzy szybko się uczą i zachowują o wiele subtelniej, niż satrapowie dawnych czasów. Aleksiej Nawalny, słynny rosyjski blogger polityczny trafi do łagru nie za blogowanie, lecz za jakieś pospolite przestępstwo, np. rzekome oszustwo podatkowe. Czyż za to samo nie wsadza się do więzień na demokratycznym Zachodzie?

Schmidt i Cohen nie mają więc złudzeń, ich zdaniem przewroty w Tunezji i Egipcie to ostatnie już takie rewolucje, poza tym zakończone umiarkowanym sukcesem.

Oczywiście, nie można wykluczać kolejnych rewolt i buntów, podobnie jednak jak w Iranie nie przyniosą zmiany, bo zostaną szybko spacyfikowane przez coraz bardziej cyfrowo kompetentne służby policyjne. Co więc zostaje? Konsolidować zdobycze zachodniej demokracji. Tu jednak pojawia się pewien problem, a zwrócił nań uwagę Julien Assange, założyciel słynnego WikiLeaks w swej recenzji „The New Digital Age" napisanej dla „The New York Times". To fakt, że coraz trudniej będzie zdemokratyzować reżimy niedemokratyczne i nie ma co się łudzić demokratyzacyjnym potencjałem Sieci.

Więcej, to państwa demokratyczne zaczynają czerpać inspirację z dyktatur wprowadzając coraz bardziej przenikliwe systemy inwigilacji swoich obywateli. Oczywiście, wszystko odbywa się w ramach demokratycznego przyzwolenia, które wzrosło bardzo po 11 września 2001 r. Walka z terrorem łatwo uzasadnia konieczność gromadzenia kolejnych danych, jawnych i niejawnych. Gorzej, wszelkie próby przeciwstawienia się tej logice metodami cyberaktywistycznymi traktowane są jako działania niemal terrorystyczne. Assange sam jest najlepszym przykładem.

W rezultacie granica między systemami demokratycznymi niedemokratycznymi zaciera się, przynajmniej jeśli chodzi o techniki kontroli społeczeństw. Różnica niezmiennie polega na możliwości kontroli władzy przez społeczeństwo. Ta ciągle w krajach demokratycznych jest nieporównanie większa, to jednak Rosjanie uciekają z Moskwy do Londynu, mimo że jest miastem o najbardziej na świecie rozwiniętym systemie cyfrowej inwigilacji i monitoringu.

Assange podpadł Amerykanom, bo ujawnił ich tajne informacje – czy chińskie lub rosyjskie depesze dyplomatyczne są mniej ciekawe? Nie sądzę, tylko jakoś w tamtych systemach trudno coś ciekawego wydobyć na światło dzienne (chyba, że jak w PRL miało się pułkownika Kuklińskiego). Najprawdopodobniej chiński lub rosyjski Bradley Manning (to ten żołnierz dostarczył WikiLeaks kopie depesz) nie doczekałby nawet procesu, więc nie miałby szansy stać się tematem medialnej debaty.

Internet, jak każda przełomowa innowacja komunikacyjna jest wyzwaniem dla systemów politycznych, zarówno demokratycznych, jak i autorytarnych. Protokoły TCP/IP i http nie są przepisami na władzę, tylko na sposób przetwarzania informacji. Władza należy do tych, którzy wiedzą jak zrobić użytek z informacji.

Relacja z konferencji Predictive Solutions, KORELACJE 2013

Kolejna konferencja Predictive Solutions w Krakowie dobiegła końca. W dniach 22-24 maja br. Kraków po raz kolejny gościł miłośników i ekspertów analizy danych. W tym roku w konferencji wzięło udział niemal

100 uczestników. Konferencja KORELACJE organizowana przez Predictive Solutions jest corocznym wydarzeniem ułatwiającym wymianę doświadczeń, a także zaczerpnięcie inspiracji i nawiązywanie kontaktów. Wśród 22 prelegentów znaleźli się przedstawiciele niemal wszystkich branż. Zróżnicowana tematyka wystąpień i równoległy układ prelekcji pozwalały na dobór wystąpień do własnych oczekiwań. Duże zainteresowanie wywołała prelekcja dr Bedyńskiej ze Szkoły Wyższej Psychologii Społecznej - „ Czego naukowcy nauczyli się od łososia norweskiego". Wystąpienie pod tym nieco przewrotnym tytułem, kryło bardzo jasny przekaz by testowanie hipotez zawsze wiązało się z doborem odpowiednich testów. Wśród wystąpień z branży badawczej należy zwrócić uwagę na wystąpienie Pawła Wójcika z 4P Research Mix - „Irracjonalność decyzji konsumenckich". W oparciu o wyniki badań zostały przedstawione determinanty sprzecznych bądź irracjonalnych postaw konsumenckich.

Na konferencji z zakresu analizy danych nie mogło zabraknąć niezwykle popularnego obecnie tematu,tj. „Big data". Poruszyła go w swoim wystąpieniu Joanna Draszanowska z Naszej Klasy „Big data, a badania deklaratywne - substytucyjne czy komplementarne ?". Prowadząca wskazała nie tylko na wartość i ogromny wolumen danych, które zostawiamy w Internecie, ale także na konieczność ich uzupełniania o dane pochodzące z badań. Nie można nie wspomnieć o prelekcji Łukasza Piskorskiego z Allegro, który prezentował wykorzystywane przez tę firmę narzędzia pomiaru satysfakcji i lojalności użytkowników.

Interesująca dla badaczy była prelekcja w temacie - w jaki zaś sposób radzić sobie z brakami danych w badaniach, Piotra Jabkowskiego z Uniwersytetu Ekonomicznego w Poznaniu. Zaprezentował porównanie dwóch procedur ważenia danych w oparciu o dane z PGSS. Jak przekonywał prelegent procedura propencity weight score prowadzi do znacznego zmniejszenia całkowitego błędu pomiaru, w porównaniu z klasycznymi technikami post-stratyfikacyjnymi.

Z obszaru wykorzystania analizy danych w bankowości, trzeba zwrócić uwagę na dwa wystąpienia. Prelekcja Piotra Szykownego oraz Iwony Kowalskiej z Banku BGŻ, zaprezentowała analizę danych jako niezbędny element efektywnego systemu zarządzania sprzedażą. Drugie z nich to wystąpienie Justyny Martyniak (BNP Paribas), która prezentowała działanie systemu rekomendacji szans sprzedażowych i wyniki jakie daje wykorzystanie analitycznego CRM w kampaniach realizowanych przez bank.

Uzupełnieniem części wystąpień i dyskusji w kuluarach, były dwa spędzone wspólnie wieczory w Krakowie. Pierwszy z nich spędziliśmy na tarasie Planetarium w hotelu Galaxy, gdzie prócz doskonałej kolacji i dobrego wina, można było posłuchać aranżacji rockowych utworów granych na pianinie. Pierwszy wieczór był jednak tylko zapowiedzią tego, co wydarzyło się następnego dnia. W Bunkier Cafe, w którym gościliśmy nie po raz pierwszy, na uczestników czekała gorąca kolacja i bogato zastawione stoły oraz bar. Jednak największą radość sprawił wszystkim występ artystki Aldony Jankowskiej, która przedstawiła swój program pt." Jak nie ja, to kto?" Doborowe monologi i satyryczne piosenki kabaretowe oraz żywy udział publiczności w występie wprawił wszystkich w dobry nastrój. Po występie tradycyjnie zabawa do rana, i nie jest to jedynie pusty zwrot :).

Konferencje zakończyliśmy zabawą dla cierpliwych i najbardziej zaangażowanych. Swoich „nowych właścicieli" znalazły: Tablet Samsung Galaxy Note N8000, smartfon Nokia Lumia 620 oraz zestaw bezprzewodowy Logitech MK520. Zwycięzcom gratulujemy, a wszystkim uczestnikom dziękujemy za spędzone wspólnie chwile.

Relacja z Seminarinarium „Blaski i cienie przetwarzania w chmurze (Cloud Computing)"

24 czerwca 2013 r. w Krajowej Szkole Administracji Publicznej w Warszawie Polska Izba Informatyki i Telekomunikacji (PIIT) w uzgodnieniu i pod patronatem Ministerstwa Administracji i Cyfryzacji (MAiC) zorganizowała Seminarium Robocze „Blaski i cienie przetwarzania w chmurze (Cloud Computing)".

W seminarium wzięło udział ponad 70 przedstawicieli najważniejszych urzędów państwowych i samorządowych, uczestniczący w budowaniu programu informatyzacji państwa i mający wpływ na wybór technik jego realizacji, a także zaproszeni goście z branży teleinformatycznej.

Otwarcia konferencji dokonali Jan Pastwa – Dyrektor KSAP, Andrzej Ręgowski – Podsekretarz Stanu w Ministerstwie Administracji i Cyfryzacji, Włodzimierz Marciński - Pełnomocnik Ministra Administracji i Cyfryzacji oraz dr inż. Wacław Iszkowski – Prezes Polskiej Izby Informatyki i Telekomunikacji.

Gość seminarium Dr Wojciech Wiewiórowski – Generalny Inspektor Ochrony Danych Osobowych wygłosił referat nt. Prawnych aspektów udostępniania usług administracji publicznej w modelu chmury obliczeniowej (cloud computing).

Istotną nowością tego seminarium było to, że prelegenci wygłaszający referaty na poszczególne, zaplanowane wcześniej tematy, wyłonieni zostali w drodze konkursu.

Seminarium wzbudziło znaczne zainteresowanie jego uczestników. Wydaje się za celowe kontynuowanie tej inicjatywy przez organizację wspólnie z MAiC podobnych seminariów z zastosowaniem przyjętej metody wyboru tematów oraz prelegentów.

Zapraszamy do udziału

WARSZTATY

PRAKTYCZNE PRAWNE ASPEKTY OCHRONY DANYCH OSOBOWYCH I BAZ DANYCH

Warszawa, 10.12.2013

Komisja Europejska przedstawiła projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Rozporządzenie wprowadza nowe ramy ochrony danych osobowych w Unii Europejskiej.

Celem szkolenia jest zapoznanie uczestników z głównymi zasadami oraz zmianami w zakresie ochrony danych osobowych wynikającymi z przedstawionego projektu Rozporządzenia o ochronie danych osobowych. Ponadto, w ramach szkolenia przedstawione zostaną w praktyczny sposób wybrane aktualne problemy prawne związane z ochroną danych osobowych, w tym przetwarzania danych osobowych w związku z monitoringiem pracowników oraz przetwarzaniem danych biometrycznych. Omówione zostaną praktyczne konsekwencje biznesowe ostatniej nowelizacji przepisów powodującej objęcie ochroną danych indywidualnych przedsiębiorców. Uczestnicy szkolenia poznają również zasady powierzenie przetwarzania danych osobowych w tym sporządzania umów o powierzenie danych osobowych w sposób zgodny z wymaganiami ustaw, wymaganiami GIODO oraz najlepszymi standardami. W ramach szkolenie przedstawione zostaną również zasady ochrony baz danych obejmujących dane osobowe. Szkolenie oparte będzie na analizę najnowszego orzecznictwa sądowego, opinii Grupy 29 oraz dobrych praktyk w zakresie ochrony danych osobowych.

Więcej informacji: **www.cpi.com.pl**

Zamówienie prenumeraty kwartalnika

„Czas informacji"

WYŚLIJ FAKSEM 22 871 85 56 lub 22 870 69 95

PRENUMERATA NA ROK 2013

Zamawiamy prenumeratę kwartalnika „**Czas Informacji**"

okres trwania prenumeraty (ilość egzemplarzy)	ilość zamawianych prenumerat	**cena**
prenumerata roczna 2013 od numeru 1(13)/2013 - 4 kolejne numery		98zł+5% VAT
prenumerata półroczna		65zł +5% VAT

Prenumeratę prosimy przesłać do niżej wymienionego adresata

PRENUMERATOR		FIRMA	
imię		nazwa	
nazwisko		NIP	
stanowisko		ulica	
nr telefonu		kod, miasto	
nr faksu		nr telefonu	
e-mail		nr faksu; e-mail	

Wyrażam zgodę/ Nie wyrażam zgody na wykorzystywanie przez Centrum Promocji Informatyki sp. z o. o., Warszawa, ul. Międzyborska 50, moich danych (w tym adresu poczty elektronicznej), pod warunkiem przestrzegania przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. jedn. Dz. U. z 2002 r. Nr 101, poz. 926), w zakresie prowadzonej przez CPI działalności gospodarczej (a w szczególności działalności marketingowej i na przekazywanie danych uczestnika firmom biorącym udział w opracowaniu programów szkoleń). Mam świadomość prawa do wglądu, poprawiania lub usunięcia swoich danych w bazie danych osobowych CPI oraz dobrowolności ich podania. W związku z obowiązkiem wynikającym z ustawy z dnia 18 lipca 2002 r. (Dz. U. nr 144, poz. 1204) o świadczeniu usług drogą elektroniczną wyrażam zgodę na

Oznaczoną należność z tytułu kosztów prenumeraty w wysokości _____zł wpłacę w terminie 14 dni od daty otrzymania faktury.

Należy wypełnić i odesłać faksem na numer
22 871 85 56 lub 22 870 69 95

.....
pieczęć i podpis osoby upoważnionej

redaktor naczelny: Wiesław Paluszyński
wieslaw.paluszynski@czasinformacji.pl

kolegium redakcyjne: Izabela Adamska, Dariusz Bogucki, Tomasz Kulisiewicz, Piotr Waglowski, Wojciech Wiewiórowski

sekretarz redakcji i reklama: Agata Soboń Modzelewska
redakcja@czasinformacji.pl

redakcja: Centrum Promocji Informatyki sp. z o. o.
ul. Międzyborska 50, 04-041 Warszawa
tel. 22 870 69 78, 22 871 85 51
fax 22 870 69 95, 22 871 85 56
info@czasinformacji.pl
www.czasinformacji.pl

projekty graficzne: Mikołaj Ostaszewski
mikolaj.ostaszewski@zsrr.pl

skład i łamanie: Michał Nowosielski
michal@nowosielscy.com.pl

nakład: 400 egz.

prenumerata: prenumerata@czasinformacji.pl
www.czasinformacji.pl/prenumerata

Zamówienia prenumeraty również u kolporterów.

Redakcja nie zwraca materiałów niezamówionych oraz zastrzega sobie prawo do ich redagowania i skracania.

wydawca:

Centrum Promocji Informatyki sp. z o. o.
www.cpi.com.pl

rada naukowa:

prof. dr hab. Jacek Gołaczyński
prof. dr hab. Mirosław Kutyłowski
dr hab. Artur Nowak-Far
prof. dr hab. Ewa Nowińska
prof. dr hab. Witold M. Orłowski
dr hab. Grażyna Szpor

W części naukowej kwartalnika umieszczane są prace naukowe publikowane w języku polskim (ze streszczeniem), które podlegają recenzjom rady.

www.czasinformacji.pl/prenumerata.php

Czas Informacji

Zapraszamy do składania zamówień na prenumeratę na 2013 rok.