Czas informacji
Prawo nowych technologii • Informacja w administracji i gospodarce
ISSN 2081-6189 kwartalnik 4(5)/2010

Unia innowacji

Teleinformatyka
w czterech obszarach
Wacław Iszkowski

Pieczęć elektroniczna
Mirosław Kutyłowski

Wnioski z przeglądu projektów
realizowanych w ramach VII POiG
Michał Tabor

Wolne oprogramowanie
w zamówieniach publicznych
Bohdan Widła

Zmiany w podatku VAT
a umowy w sprawie
zamówienia publicznego
Wojciech Kaliński

cpi
centrum promocji informatyki
www.cpi.com.pl

Czas informacji

Kwartalnik „**Czas Informacji**" jest scaloną formą czasopism „elektroniczna Administracja" i „Prawo Nowych Technologii", które Centrum Promocji Informatyki wydawało do 2009 roku. Pismo adresowane jest do przedstawicieli administracji oraz środowisk prawniczych.

Zapraszamy do składania zamówień na prenumeratę na 2011 rok.

www.czasinformacji.pl/prenumerata.php

cpi
centrum promocji informatyki
www.cpi.com.pl

4 **Teleinformatyka (ICT) w czterech obszarach**
Wacław Iszkowski

NAUKA

7 **Podsumowanie konsultacji Komisji Europejskiej w sprawie otwartego Internetu oraz neutralności sieci**
Jacek Kowalski

18 **Czynniki społeczno-psychologiczne hamujące rozwój elektronicznej administracji w Polsce**
Edyta Marcinkowska

23 **Przetwarzanie danych osobowych stanowiących tajemnicę bankową w świetle orzecznictwa sądów administracyjnych**
Beata Bińkowska-Artowicz

33 **Długofalowe bezpieczeństwo podpisu osobistego**
Przemysław Kubiak

38 **Pieczęć elektroniczna**
Mirosław Kutyłowski

PUBLICYSTYKA

43 **Unia innowacji**
Dariusz Bogucki

47 **Wnioski z przeglądu projektów realizowanych w ramach VII POiG**
Michał Tabor

53 **Wolne oprogramowanie w zamówieniach publicznych – kilka uwag na marginesie orzecznictwa Krajowej Izby Odwoławczej**
Bohdan Widła

60 **Program Ramowy na rzecz Innowacyjności i Konkurencyjności a wspieranie rozwoju technologii informacyjnych i komunikacyjnych (CIP ICT PSP)**
Dariusz Bogucki

67 **Potwierdzenie tożsamości w elektronicznym obrocie gospodarczym a elektroniczna administracja – część I**
Izabela Adamska

71 **W oczekiwaniu na elektroniczne akty prawne**
Anita Jackiewicz

77 **e-Zdrowie - fakty i mity**
Marcin Kędzierski

81 **Zmiany w podatku VAT a umowy w sprawie zamówienia publicznego. Problematyka wpływu stawki podatkowej do czasu zawarcia umowy w sprawie zamówienia publicznego**
Wojciech Kaliński

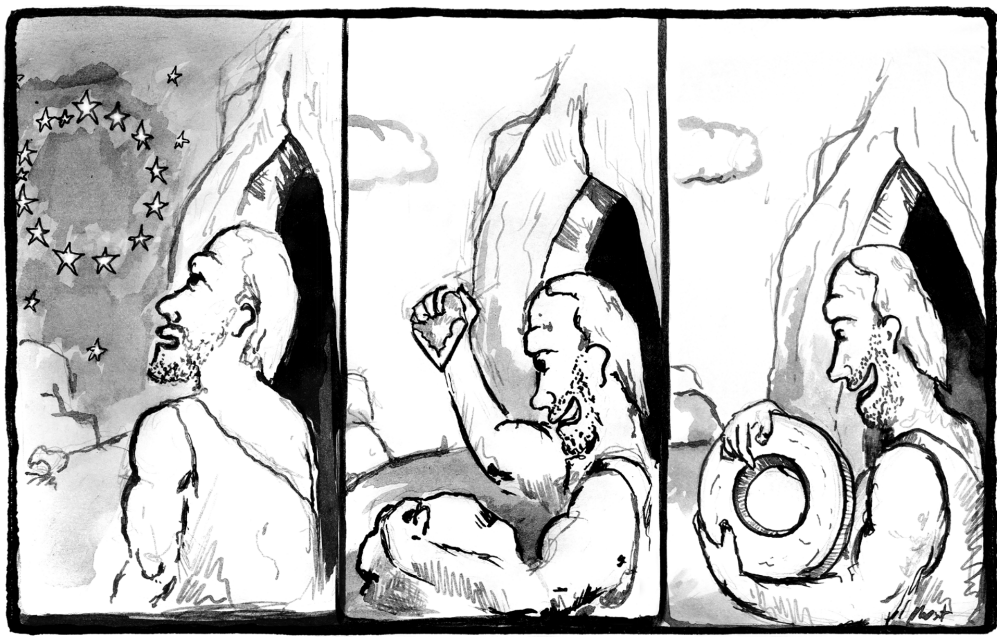
89 **Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne - część IV**
Wojciech Kaliński

STAŁE RUBRYKI

93 **Przegląd orzecznictwa w zakresie zamówień publicznych: Wyrok Krajowej Izby Odwoławczej z 2 marca 2010 r., sygn. akt KIO/UZP 184/10**
Wojciech Kaliński

96 **Julian Assange – Robin Hood społeczeństwa informacyjnego**
Edwin Bendyk

98 **Bibliografia prawa nowych technologii informacyjnych styczeń 2009 - styczeń 2010**
Wojciech R. Wiewiórowski



W kolejnym numerze

W najbliższym numerze m.in.:

- Przeciw e-wykluczeniu
  - Wacław Iszkowski
- Przepisy o informatyzacji a wymagania pozafunkcjonalne systemów IT
  - Xawery Konarski
- Artykuł 27 czy paragraf 22?
  - Robert Podpłoński
- Prawo do zapomnienia
  - Arwid Mednis
- Nowa ustawa o ochronie informacji niejawnych
  - Anita Jackiewicz
- Informatyzacja służby zdrowia czy się wreszcie powiedzie?
  - Piotr Kociński
- Jaka będzie przyszłość Elektronicznej Administracji? Część I - trendy
  - Dariusz Bogucki

oraz najciekawsze referaty wygłoszone na konferencji „Reforma ochrony prywatności", która odbyła się 16 grudnia 2010 r. na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie.

Wiesław Paluszyński redaktor naczelny
wieslaw.paluszynski@czasinformacji.pl

Pierwszy rok wydawania naszego kwartalnika już za nami. Mamy całkiem spore grono stałych autorów, a co ważniejsze - rosnące grono stałych czytelników. Witam wszystkich serdecznie i zapraszam do współpracy w proponowaniu tematów, a także do dzielenia się swoimi problemami i doświadczeniami. W tym numerze wracamy z Chin do Unii Europejskiej i piszemy piórem Dariusza Boguckiego o kwestiach innowacyjności w Unii Europejskiej, a wracając na nasze własne podwórko - o tym, jak jest naprawdę z interoperacyjnością w realizowanych projektach informatycznych 7 osi POIG, pisze Michał Tabor.

Problematyka uwierzytelniania i identyfikacji jest coraz bardziej „gorąca", więc poświęcamy jej kilka artykułów, aby temat pokazać z różnych stron. Także Edwin Bendyk nie pozwoli nam przejść obok najgorętszych problemów w najnowszym felietonie „Julian Assange – Robin Hood społeczeństwa informacyjnego".

Szczególne cieszymy się z wizyty na naszych łamach Wacława Iszkowskiego, Prezesa Polskiej Izby Informatyki i Telekomunikacji. Zachęcam do przeczytania czwartego numeru od pierwszej do ostatniej strony, bo warto, a okres świąteczny sprzyja lekturze.

Zachęcam też do pozostania z nami w 2011 roku. Do pierwszego numeru szykujemy niespodziankę w postaci nowego działu poświęconego problematyce ochrony danych osobowych, w którego redagowaniu pomoże nam Biuro GIODO. Będziemy chcieli przybliżyć czytelnikom najciekawsze problemy, z jakimi Generalny Inspektor Ochrony Danych Osobowych się spotyka, interpretacje prawa, planowane zmiany. Warto przypomnieć, iż UE przygotowuje nowelizację przepisów dotyczących danych osobowych i prywatności. Publiczną dyskusję dotyczącą tej problematyki rozpoczęto 16 grudnia konferencją na Uniwersytecie Kardynała Stefana Wyszyńskiego z udziałem Rzecznika Praw Obywatelskich prof. Ireny Lipowicz i Generalnego Inspektora Ochrony Danych Osobowych dr Wojciecha Wiewiórowskiego. W numerach pierwszym i drugim postaramy się przedstawić najciekawsze artykuły z tej konferencji, która odbyła się pod kierunkiem prof. Grażyny Szpor. Do tematu będziemy wracać wraz z rozwojem dyskusji. W trakcie uzgodnień międzyresortowych jest też większość rozporządzeń do znowelizowanej ustawy «O Informatyzacji podmiotów realizujących zadania publiczne", które postaramy się omówić w pierwszej połowie 2011 roku. Do tego jeszcze parlament rozpoczął w drugiej połowie grudnia prace nad zmianami dotyczącymi podpisu elektronicznego... Oj, będzie się działo.

Korzystając zaś z okazji grudniowego spotkania z Państwem, życzę wszystkim naszym Czytelnikom i Sympatykom, a także Przygodnym Gościom wszelkiej pomyślności w Nowym 2011 Roku. Aby sprzyjał realizacji inicjatyw, był rzeczywiście przełomowy w realizacji wielu ważnych dla rozwoju społeczeństwa informacyjnego projektów informatycznych, by spotkało Państwa wiele przyjemności, czytając kolejne numery „Czasu Informacji"

Teleinformatyka (ICT) w czterech obszarach

Dr inż. Wacław Iszkowski

W wielu dyskusjach o stosowaniu teleinformatyki (ICT[1]) w społeczeństwie i w gospodarce często trudno jest dojść do porozumienia przy wielu argumentach oraz różnych punktach widzenia. Przy jednej takiej dyskusji nagle mnie olśniło, że mówimy o różnych polach aktywności teleinformatyki – jedni o badaniach w informatyce, inni o wykorzystaniu superkomputerów, o zastosowaniach w administracji, a wreszcie pozostali przywołują umiejętności korzystania z potęgi Internetu przez ich dzieci, a nawet wnuki.

Po zastanowieniu można określić cztery obszary aktywności teleinformatyki:

- **Teleinformatyka w badaniach, rozwoju i innowacjach** (ICT R&D&I) – obejmuje opracowywanie nowych idei i algorytmów oraz projektowanie nowych rozwiązań teleinformatycznych – sprzętu cyfrowego (od komputera do sieci), oprogramowania i serwisów. Działania te są finansowane z funduszy publicznych lub własnych prywatnych oraz firmowych. Mogą być też wykonywane na zamówienie pod określone potrzeby lub też są tak innowacyjne, że trzeba dopiero wytworzyć na nie popyt (np. e-tablety).
- **Teleinformatyka profesjonalna** (Professional ICT[2]) – jest wykorzystywana w przedsiębiorstwach, przemyśle, energetyce, transporcie, nauce, bankowości i finansach, medycynie, wojsku i administracji itp., w której superkomputery, mainframe'y i serwery łącznie z zaawansowanymi systemami i sieciami teleinformatycznymi oraz aplikacjami przetwarzania informacji są kupowane i stosowane w rozwoju tych sektorów, badaniach oraz obsłudze finansów, a także są wykorzystywane w produkcji zaawansowanych technologicznie produktów – samochodów, reaktorów, uzbrojenia, tomografów i innego podobnego sprzętu. Efektywność ponoszonych nakładów finansowych na zakup technologii i rozwiązań teleinformatycznych jest mierzona i oceniana okresem i wartością zwrotu z tych inwestycji.

---

1 ICT – w środowisku toczone są dyskusje, jaki polski termin najlepiej określa Information and Telecommunication Technology. Rozważane są trzy możliwości:
- Technologie Informacyjne i Komunikacyjne (TIK) – jako najprostsze przetłumaczenie wersji angielskiej, bez wnikania w sens otrzymanego terminu,
- Techniki Informacyjne i Komunikacyjne (TIK) – przy stwierdzeniu, że nie zawsze angielskie „Technology" jest „technologią", bo często i w tym przypadku jest to też „technika",
- Teleinformatyka – argumentując, że można to zastąpić prostszym i bardziej zrozumiałym terminem poszerzającym – nieistniejący w świecie angielsko-amerykańskim – dobrze nam już znanym terminem „informatyka".

Dla rozstrzygnięcia tego sporu Polskie Towarzystwo Informatyczne zwróciło się oficjalnie do Rady Języka Polskiego o opinię w tej sprawie.

2 Professional ICT – położyliśmy nacisk na profesjonalizm, ale również jest możliwe nazwanie tego obszaru Business ICT, gdyż jego wyróżnikiem jest też ekonomiczne uzasadnienie ponoszonych nakładów na zakup nowych technologii i serwisów teleinformatycznych.

- **Teleinformatyka użytkowa** (Consumer ICT[3]) – jest wykorzystywana obecnie przez miliardy osób korzystających z telefonów, komputerów, telewizorów, konsol, dostępu do Internetu oraz serwisów i innych teleinformatycznych gadżetów dla ich własnych celów kontaktu z innymi użytkownikami, rozrywki oraz dostępu do informacji i korzystania z usług elektronicznych. Jest ona finansowana głównie z zakupów sprzętu cyfrowego oraz z opłat za dostęp do sieci (Internetu). Efektywność inwestycji w tej sferze jest liczona wartością masy sprzedaży oraz liczbą użytkowników korzystających z danych serwisów.
- **Teleinformatyka socjalna** (Social ICT[4]) – jest wykorzystywana przez podmioty i agendy publiczne dla podniesienia jakości życia obywateli i społeczności oraz uproszczenia im kontaktów z administracją, powszechnej edukacji, opieki zdrowotnej i możliwości rozwoju kulturalnego. Środki na zakup rozwiązań teleinformatycznych pochodzą tutaj z budżetu państwa oraz samorządów, a także z różnego rodzaju funduszy i fundacji. Efektywność tych nakładów jest liczona w skali zadowolenia ludności i spełnienia założonych i deklarowanych planów rozwoju cywilizacyjnego – popularnie nazwanych rozwojem społeczeństwa informacyjnego.

Ten „czysty" podział w rzeczywistości nie jest tak jednoznaczny i obszary te się wzajemnie przenikają. Każdy z trzech obszarów teleinformatyki profesjonalnej, użytkowej i socjalnej korzysta z dorobku badań i rozwoju technologii teleinformatycznych już gotowych do innowacyjnego wdrożenia w praktyce. Z teleinformatyki profesjonalnej wykorzystywanej w bankowości elektronicznej system jest dostępny w obszarze teleinformatyki użytkowej. Podobnie usługi administracji elektronicznej realizowane w obszarze teleinformatyki socjalnej są dostępne w obszarze użytkowym. Nakłady na nowe technologicznie procesory, opracowane w informatyce profesjonalnej, zwrócą się tylko po zainstalowaniu ich w milionach urządzeń przeznaczonych do powszechnego użytku. I odwrotnie – poprawne funkcjonowanie Internetu jest możliwe tylko przy profesjonalnie funkcjonujących centrach wymiany, przechowywania i przetwarzania informacji korzystających z milionów serwerów odpowiednio oprogramowanych i zabezpieczonych oraz zdublowanych i profesjonalnie zainstalowanych.

Mam nadzieję, że czytelnicy już chwycili na czym polega to „odkrycie", które jest tak proste, że aż dziwne, że dotychczas nie było powszechnie stosowane. Przyjęcie bowiem takiego podziału i opatrywanie tą etykietą analiz rozwoju i stosowania teleinformatyki ułatwia prowadzenie dyskusji i zrozumienie wartości każdego argumentu. Trudno jest bowiem zgodzić się, że umiejętności informatyka (którym po niewczasie okazuje się uczeń szkoły podstawowej) można porównywać z informatykiem z centrum superkomputerowego, ale też ten ze szkoły może być użyteczny przy „odkryciu" nowego rodzaju serwisu społecznościowego. Chyba nie ma dalej potrzeby uzasadniać, jak bardzo istotne jest przyswojenie tego podziału teleinformatyki na obszary i potem twórcze jego rozwijanie w kolejnych dyskusjach i opracowaniach. Warto też zauważyć, że każdy z tych obszarów jest poddany

3 Consumer ICT – dzisiaj obejmuje już, dotychczas wyróżniany osobno, sprzęt RTV, gdyż obecnie odbiorniki telewizyjne oraz systemy nagrywania i odtwarzania audio i wizji stają się cyfrowe (i chociaż odnotowano ostatnio koniec walkmana i taśmy kasetowej, to jednak chyba zapis analogowy będzie powracać).

4 Social ICT – socjalna teleinformatyka dla obywateli opłacana ze środków publicznych, może też być nazywana teleinformatyką administracji, ale też obejmuje edukację, kulturę i opiekę zdrowotną, a nie wszystkie te dziedziny zawsze podlegają rządowej czy samorządowej administracji.

innym zasadom ekonomicznego rachunku rozliczania środków inwestycyjnych oraz wyliczania korzyści z tych inwestycji.

Z ostatniej chwili. A jednak ten podział już się ujawnił przy opisie zapowiedzi nowej postaci Targów CeBIT w Hanowerze w 2011 roku. Zaproponowano tam cztery platformy prezentacji teleinformatyki (ICT):

- lab – Badania i rozwój dla innowacyjnej teleinformatyki (ICT),
- pro – Rozwiązania profesjonalnej teleinformatyki (ICT) dla działań biznesowych,
- life – Rozwiązania teleinformatyczne (ICT) dla konsumentów,
- gov – Rozwiązania teleinformatyczne (ICT) dla sektora publicznego.

I jak tu nie mówić o telepatycznym przekazie idei, gdy w określonych warunkach przy podobnym zgromadzeniu wiedzy i doświadczenia dochodzimy do podobnych konkluzji, a tylko pierwszy w odkryciu takiej konkluzji nabywa pierwotnych praw autorskich lub uzyskuje prawo do opatentowania swojego pomysłu.

Dr inż. Wacław Iszkowski
Waclaw@Iszkowski.pl

Zapraszamy do udziału

WARSZTATY

FINANSOWANIE PROJEKTÓW INWESTYCYJNYCH SEKTORA MEDYCZNEGO ZE ŚRODKÓW POMOCOWYCH UE DO ROKU 2013

18 stycznia 2011 r., Warszawa

Celem warsztatu jest przedstawienie informacji na temat przygotowania i oceny efektywności projektów inwestycyjnych współfinansowanych z funduszy europejskich skierowanych do sektora medycznego. Uczestnicy będą mieli możliwość zapoznania się z najważniejszymi, dostępnymi w chwili obecnej działaniami, obowiązującymi regulacjami, jak również zagadnieniami przygotowania i skutecznego aplikowania o wsparcie na realizację projektów inwestycyjnych na wybranych przykładach. Przedstawiona zostanie analiza wykonalności projektu ze szczególnym uwzględnieniem planowania finansowego i budżetowania. Omówione zostaną potencjalne ryzyka występujące przy realizacji projektu i scenariusze przeciwdziałania. 30% czasu zajęć będą stanowić elementy praktyczne i uczenie przez doświadczanie.

Warsztat poprowadzi Marcin Postawka, trener Centrum Rozwiązań Menadżerskich SA.

Adresaci szkolenia:sektor medyczny - kadra zarządzająca, menedżerowie projektów, pracownicy działów finansowych.

W PROGRAMIE

- Wprowadzenie do tematyki szkolenia.
- Procedura ubiegania się o dotację. Ocena efektywności projektów inwestycyjnych.
- Rozliczenie projektu, obowiązki beneficjenta.
- Case study - przykłady zakończonych przedsięwzięć inwestycyjnych/ lub realizacja zadań w grupach na praktycznych przykładach („krok po kroku" z wypełniania dokumentacji niezbędnej do pozyskania środków unijnych, na przykładzie dokumentacji dostępnej w ramach danego działania/programu).

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Podsumowanie konsultacji Komisji Europejskiej w sprawie otwartego Internetu oraz neutralności sieci

Jacek Kowalski

Konsultacje Komisji Europejskiej w sprawie otwartego Internetu oraz neutralności sieci trwały od 30 czerwca do 30 września 2010 r. W konsultacjach wzięło udział 318 podmiotów związanych z rynkiem internetowym, tj. operatorzy sieci, dostawcy usług internetowych, organy państw członkowskich zrzeszenia konsumentów i organizacje społeczeństwa obywatelskiego oraz obywatele. Głos w tej sprawie zajął również Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC). Powyższa liczba świadczy o znaczeniu podjętych konsultacji oraz o potrzebie bliższego przyjrzenia się zagadnieniom poruszonym w tej debacie. W trakcie konsultacji Komisji Europejskiej zostały poruszone takie zagadnienia, jak:

1. znaczenie zapewnienia otwartości Internetu – obecne i przyszłe problemy oraz znaczenie ram regulacyjnych sektora telekomunikacyjnego Unii Europejskiej,
2. istota zarządzania ruchem w Internecie – konieczność, przejrzystość oraz zarządzanie usługami w sieci Internet,
3. struktura rynku internetowego,
4. konsumenci na rynku internetowym oraz jakość usługi dostępu do Internetu,
5. polityczny, kulturalny oraz socjalny wymiar Internetu.

Niniejsza publikacja ma na celu przybliżenie stanowisk podmiotów, które zabrały głos w dyskusji, a w szczególności opinii BEREC. Z uwagi na poruszaną problematykę oraz znaczenie poszczególnych tematów związanych z funkcjonowaniem rynku telekomunikacyjnego oraz przejrzystością ofert usług dostępu do Internetu w dalszej części publikacji zostaną omówione pierwsze 4 tematy.

Otwarty Internet – obecne i przyszłe problemy oraz znaczenie ram regulacyjnych EU

Komisja Europejska w dokumencie konsultacyjnym zwróciła uwagę na znaczenie zasady „end-to-end", która zdaniem wielu ekspertów jest kluczem do rozwoju Internetu. Zgodnie z zasadą „end-to-end" protokoły odpowiedzialne za sposób przepływu danych powinny znajdować się na krawędzi systemu komunikacyjnego albo jak najbliżej źródła będącego pod kontrolą użytkownika końcowego. W praktyce oznacza to, że operatorzy sieci traktują pakiety w równy sposób, bez względu na pochodzenie, typ kontentu czy też miejsce przeznaczenia. W przeciwieństwie do tradycyjnych operatorów telekomunikacyjnych, którzy instalują „inteligentne" urządzenia w szkielecie sieci, zwolennicy zasady „end-to-end" uważają, że powinny one być zlokalizowane na jej krawędzi (np. w urządzeniach podłączonych do sieci – komputery).

Zatem konsumenci oraz dostawcy usług/kontentu, których urządzenia są podłączone do sieci, płacą dostawcy usług internetowych za dostęp do Internetu i to do nich należy decyzja w zakresie poruszania się w tym środowisku oraz udostępniania określonych, zgodnych z prawem treści. Możliwość korzystania z kontentu umieszczonego w Internecie jest na dzień dzisiejszy mniej lub bardziej ograniczona. W odróżnieniu jednak od modelu „ogrodzonego ogrodu" (*walled garden*), w którym operator zachowuje ścisłą kontrolę, dokonując na przykład wcześniejszej selekcji kontentu przed umieszczeniem w sieci, to do użytkowników końcowych należy wybór, ograniczony jedynie pod względem technologicznym, używanego sprzętu oraz przepływności łącza.

W trakcie dyskusji na temat otwartości Internetu często poruszany jest temat czynników wpływających na fakt, że dostawcy usług internetowych są zainteresowani dostarczaniem szerokiego rodzaju kontentu. Eksperci zwracają uwagę, iż podmioty działające w Internecie czy też zapewniające dostęp do sieci działają na rynku wielostronnym (*multi-sided market*), co powoduje, że w interesie wszystkich jest zapewnienie otwartości Internetu. Odnosząc się do sektora telekomunikacji, rynek wielostronny charakteryzuje się:

1) występowaniem przynajmniej dwóch wyróżniających się grup odbiorców. Dla przykładu mogą to być twórcy oprogramowania oraz ich użytkownicy, osoby sprzedające na aukcjach internetowych oraz kupujący. Nie muszą oni jednak być przypisani tylko i wyłącznie do określonej grupy. Osoby sprzedające mogą również kupować na aukcjach internetowych, a osoby korzystające z telefonów komórkowych mogą zarówno wykonywać połączenia, jak i je odbierać.
2) istnieniem zewnętrznych powiązań, które powodują, że powyższe grupy łączą się ze sobą lub ich działania w jakiś sposób są koordynowane. Użytkownicy sieci telekomunikacyjnych zyskują, gdy wzrasta ich liczba, ponieważ mogą połączyć się z większą liczbą osób. Istnieją jednak dwie grupy użytkowników (np. wykonujący połączenia oraz je odbierający), którzy w zależności od wykonywanej czynności mogą ponosić różne opłaty ustalone przez przedsiębiorcę telekomunikacyjnego.
3) istnieniem pośrednika wykorzystującego zewnętrzne powiązania i łączącego określone grupy. Dla przykładu, osoby mogłyby wysyłać do siebie listy tradycyjną pocztą, ale ze względu na szybkość dostarczenia informacji korzystają z poczty elektronicznej. Dostawcy usług internetowych wykorzystują zatem preferencje użytkowników końcowych. Pośrednik zmniejsza między innymi czas oraz ewentualne koszty związane z przepływem informacji, pozwalając tym samym określonym grupom korzystać z efektu powiązania.

Ponadto Komisja Europejska zwróciła uwagę, że konkurencja na rynku usług dostępu do Internetu umożliwiła konsumentom wybór różnych platform oraz form płatności, co przyczyniło się do zachowania otwartości Internetu.

Biorąc jednak pod uwagę zwiększający się ruch przechodzący przez sieci telekomunikacyjne oraz rozwój nowych form przesyłu danych, które zmieniają modele biznesowe zapewniające dostarczanie usług poprzez te sieci, pojawiły się zdaniem Komisji Europejskiej przykłady nierównego traktowania przez operatorów sieci usług albo przepływu danych, co skłania do zastanowienia się, czy otwartość albo neutralność Internetu może być zagrożona.

W raporcie podsumowującym konsultacje Komisja Europejska podniosła, że operatorzy sieci, dostawcy usług internetowych oraz producenci infrastruktury telekomunikacyjnej na dzień dzisiejszy nie widzą zagrożenia dla otwartości Internetu oraz neutralności sieci w Unii Europejskiej. W ich opinii zarządzanie ruchem w sieci istnieje w celu wspierania sprawnego przeprowadzania operacji w Internecie oraz nie ma ono negatywnego wpływu na możliwości konsumentów. Niektórzy z nich wręcz utrzymują, że praktyki te obecnie umożliwiają rozwój usług telekomunikacyjnych po niższych kosztach. Ponadto utrzymują, że operatorzy nie angażują się w niesprawiedliwą dyskryminację w sposób, który szkodzi konsumentom czy też konkurencji. Ten pogląd został również zaprezentowany przez niektóre kraje członkowskie.

Z drugiej strony BEREC, odnosząc się do zasady neutralności sieci, podkreślił, że mogą występować pewne usprawiedliwione odstępstwa w interesie użytkowników końcowych, ale inne formy dyskryminacji mogą stworzyć zagrożenie dla konkurencji i społeczeństwa. BEREC, wskazując na incydenty związane z niezachowaniem neutralności sieci, podał

takie przykłady jak: spowalnianie wymiany plików w aplikacjach p2p albo transmisji Video czy też blokowanie usług VoIP w sieciach mobilnych. Podobne przykłady były również wymieniane przez organizacje konsumenckie.

Jednocześnie dostawcy kontentu, biorąc pod uwagę ewentualne przyszłe problemy związane z zachowaniem otwartości Internetu, zwrócili uwagę, że może ona być zagrożona w przyszłości. Nowe modele prowadzenia działalności internetowej, a w szczególności podmioty pobierające określone opłaty z tytułu korzystania z Internetu lub umieszczania treści, mogą zniszczyć otwartość Internetu oraz ograniczyć inwestycje w rozwój kontentu. W szczególności podkreślili, że obecnie nie może być mowy o darmowym wdrażaniu usług w sieci Internet. Dostawcy kontentu inwestują w rozwój swoich aplikacji i są zainteresowani, by użytkownik końcowy miał efektywny dostęp do ich zasobów z uwagi na fakt, że podmioty te same płacą za podłączenie do Internetu oraz przeznaczają środki na budowę infrastruktury niezbędnej do świadczenia usług.

Z drugiej strony niektórzy uczestnicy konsultacji (w szczególności przedsiębiorcy telekomunikacyjni) uważają, że tego rodzaju opinie są nieusprawiedliwione. Ich zdaniem, rozwój konkurencji oraz przejrzystość komercyjnych ofert telekomunikacyjnych, umożliwiających konsumentom wybór najkorzystniejszej dla nich usługi, pozwala na zapewnienie otwartości Internetu.

Natomiast w opinii BEREC w przyszłości mogą pojawić się problemy związane z wykorzystywaniem technik zarządzania ruchem w sieci w celu dyskryminacji określonych usług. Jednocześnie nie jest jeszcze jasne, w jaki sposób wpłyną one na dotychczasową strukturę rynku internetowego. Zagrożona może być również możliwość swobodnego wyrażania opinii oraz prawo do prywatności użytkowników końcowych. Niejednokrotnie BEREC w swoim stanowisku przestrzega przed ewentualnym brakiem przejrzystości informacji w zakresie zarządzania ruchem przedstawianych użytkownikom końcowym. Konsument może nie być świadomy, czy regularne spowolnienie działania usług internetowych może wynikać z technik zarządzania ruchem czy też przeciążenia sieci.

Dla krajowych organów regulacyjnych istotną kwestią jest również granica, której przekroczenie powoduje, że zarządzanie ruchem prowadzi do dyskryminacji i hamuje rozwój konkurencji. Pojawianie się nowego typu usług (np. IPTV) o gwarantowanej jakości ich świadczenia wymaga zastosowania określonych technik zarządzania ruchem, co powoduje, że operatorzy sieci oraz dostawcy usług internetowych mogą decydować się na wertykalną integrację na rynkach kontentu, aplikacji i usług. Istnieje obawa, że w takim przypadku operatorzy sieci/dostawcy usług mogą dyskryminować usługi konkurencji poprzez nieoferowanie odpowiedniej jakości ich świadczenia, czy też nawet aktywne degradowanie usług konkurencji. Tego rodzaju działania mogą być dokonywane poprzez określonego typu traktowanie przepływu danych czy też restrykcyjną politykę interkonektową (świadczenie usług wymaga podpisywania umów o połączeniu sieci tzw. umów interkonektowych). Ocena takich działań może być problematyczna z uwagi na obowiązek wzięcia pod uwagę wielu czynników, m.in. czy operator posiada znaczącą pozycję na rynku oraz czy mowa jest o usługach zarządzanych (*managed services*) albo tzw. usługach „best effort".

Za usługi „*best effort*" uważane są usługi, dla których nie są ustanowione gwarancje w zakresie ich świadczenia (ani priorytety, ani gwarancje, że dane zostaną dostarczone). Istotne jest jednak podkreślenie, że nie oznacza to równocześnie niskiego poziomu ich jakości. Ogólna zasada związana z tego typu usługami przyjmuje, że każdy popyt zwiększający ruch w sieci jest akceptowany. W przypadku gdy maksymalna

przepustowość sieci zostanie osiągnięta, jakość świadczenia usług zmniejsza się. W sieciach, za pomocą których świadczone są usługi „*best effort*", również wykorzystuje się techniki zarządzania ruchem, ale w znacznym stopniu mniejszym niż w przypadku usług zarządzanych.

Natomiast dla użytkowników usług zarządzanych są ustanawiane przez operatorów sieci gwarancje (np.: odpowiednia jakość usługi, bezpieczeństwo). Z punktu widzenia technicznego usługi zarządzane są zależne od technik zarządzania ruchem oraz restrykcji w zakresie dostępu. Ostatni czynnik jest kluczowy dla odróżnienia usług *„best effort"* oraz usług zarządzanych. W pierwszym przypadku, gdy limit przepustowości zostanie osiągnięty, klientowi wciąż będzie świadczona usługa (o niższej jakości), natomiast w przypadku usług zarządzanych klient może spodziewać się odmowy w korzystaniu z usługi.

Jednocześnie uczestnicy konsultacji uważają, że nowy pakiet telekomunikacyjny Unii Europejskiej jest wystarczający, by zapobiec degradacji otwartości Internetu. Jednak ich zdaniem na ostateczną ocenę należy poczekać do momentu, w którym odpowiednie dyrektywy zostaną implementowane w poszczególnych krajach.

Zarządzanie ruchem – konieczność, przejrzystość oraz zarządzane usługami w sieci

Nowy pakiet telekomunikacyjny dopuszcza możliwość zarządzania siecią oraz ruchem w Internecie w celu świadczenia zróżnicowanych usług oraz zapewnienia wydajnego funkcjonowania sieci. Musi się to jednak odbywać zgodnie z przyjętymi ramami regulacyjnymi, a w szczególności klient powinien zostać poinformowany o minimalnej jakości usług. Jednocześnie istnieją ograniczenia dotyczące ustanawiania priorytetów dla określonego ruchu, który odbiega od natury Internetu zbudowanego z wielu różnych sieci. Zgodnie z punktem 34 Dyrektywy Parlamentu Europejskiej i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniającej m.in. Dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników w celu sprostania wymogom dotyczącym jakości operatorzy mogą stosować procedury służące pomiarowi i organizowaniu ruchu na połączeniu z siecią tak, aby zapobiec osiągnięciu pojemności łącza lub jej przekroczeniu, co spowodowałoby przeciążenie sieci i obniżenie jej wydajności. Oznacza to, że priorytaryzacja jest dopuszczalna, jeśli wszystkie połączone sieci, które łączą dostawcę usługi z konsumentem, zezwalają na wprowadzenie określonej metodologii i narzędzi w celu ustanowienia odpowiednich preferencji.

W praktyce priorytaryzacja określonego ruchu jest możliwa tylko na określonym poziomie architektury sieci Internet w momencie, gdy ruch znajduje się w sieci pojedynczego dostawcy usług internetowych, do której określony dostawca kontentu/strony internetowej jest podłączony.

Komisja Europejska w dokumencie konsultacyjnym zwróciła uwagę, że kwestia jakości usług internetowych w kontekście zarządzania ruchem pojawia się w sytuacji, gdy sieć jest nadmiernie przeciążona (poziom ruchu osiąga maksimum pojemności sieci i użytkownicy końcowi mają trudność w uzyskaniu dostępu do sieci). W takim przypadku operator sieci ma możliwość:

- zwiększenia przepustowości sieci by zaspokoić popyt,
- wprowadzenia technik zarządzania ruchem w sieci (m.in. na podstawie miejsca pochodzenia, przeznaczenia lub typu kontentu) w celu szybszego przesyłania danych wrażliwych na czas dostarczenia, a tam, gdzie jest to konieczne, spowalniania transmisji danych, które nie wymagają natychmiastowego przesyłu. Wybór ten odnosi się do wprowadzania parametrów jakości usługi internetowej w praktykach zarządzania ruchem w sieci.

Zarządzanie ruchem może przybierać różnorodne formy. Ruch może być zarządzany w celu zapewnienia określonej jakości usług (dla usług głosowych) albo świadczenia usług w czasie rzeczywistym, które w przeciwnym razie byłyby narażone na spowolnienie ze strony innych, wymagających odpowiedniej przepustowości usług. Komisja Europejska podkreśliła również, że w przyszłości ruch może być zarządzany w celu spełnienia wymogów przepisów prawa, na przykład poprzez blokowanie nielegalnego kontentu.

Komisja Europejska dostrzegła również wzrost zainteresowania takimi usługami jak IPTV, przetwarzaniem w chmurze (cloud computing – użytkownik usługi nie jest m.in. świadomy, gdzie oprogramowanie jest faktycznie zainstalowane, gdzie są ewentualnie zapisywane dane) albo aplikacjami związanymi z sektorem medycznym. Tego rodzaju aplikacje mogą być dostarczane przez podmioty trzecie, niezależnie od firm zapewniających dostęp do Internetu. Trend ten może prowadzić do wzrostu znaczenia usług zarządzanych. Tym samym operatorzy sieci mogą być zainteresowani podpisywaniem umów również z dostawcami kontentu, którzy chcą zapewnić odpowiedni, gwarantowany poziom dla świadczonej usługi. Niektórzy zwracają zatem uwagę na zagrożenie związane z oferowaniem warunków świadczenia usługi o lepszej jakości w sposób selektywny tylko dla niektórych dostawców określonego typu kontentu albo aplikacji, co może mieć negatywny wpływ na innych dostawców kontentu oraz użytkowników końcowych.

W dokumencie konsultacyjnym porównano również możliwość korzystania z usług VoIP w sieciach stacjonarnych oraz mobilnych. W przeciwieństwie do sieci stacjonarnych, gdzie usługi VoIP są postrzegane jako czynnik mogący mieć wpływ na przejście użytkowników końcowych z wąskopasmowego na szerokopasmowy dostęp do Internetu, operatorzy sieci mobilnych nadal blokują usługi VoIP od postronnych dostawców albo umożliwiają na korzystanie z nich za dodatkową opłatą. Mobilni operatorzy usprawiedliwiają blokowanie usług VoIP zarówno ze względów technicznych, jak i komercyjnych.

Regulaminy niektórych przedsiębiorców telekomunikacyjnych w zakresie usługi mobilnego szerokopasmowego Internetu zakazują korzystania z usług VoIP oraz aplikacji p2p. Nie jest jednak jasne, na jakim poziomie technicznym blokowanie ma miejsce: czy u operatora, który może bezpośrednio zablokować tego typu usługi w swojej sieci, czy na terminalach użytkowników końcowych przez firmy je wytwarzające na żądanie operatora.

Komisja Europejska podkreśliła, że praktyki operatorów sieci oraz dostawców usług internetowych związane z ruchem internetowym są trudne do monitorowania oraz oszacowania. W jej opinii w związku z inwestowaniem przez operatorów w sieci następnej generacji (*Next Generation Networks*) oraz coraz szerszą możliwością zarządzania ruchem istotne jest określenie, gdzie istnieje granica rozsądnego zarządzania ruchem oraz co może być zaakceptowane zarówno przez krajowe organy regulacyjne oraz konsumentów.

W opinii BEREC w sieciach telekomunikacyjnych muszą być ustanowione pewne reguły w celu świadczenia za ich pomocą usług o odpowiedniej jakości. Zarządzanie ruchem (w odróżnieniu od usług zarządzanych) stanowi podzbiór takich reguł. Reguły zarządzania ruchem są ustanawiane na różnych warstwach sieci i są one konieczne w celu świadczenia wszystkich usług o wysokiej jakości.

Zarządzanie ruchem może być prowadzone niezależnie lub zależnie od kontentu, aplikacji, usługi, urządzenia, adresu nadawcy oraz odbiorcy. Nie w każdym przypadku będzie ono stanowić naruszenie zasady neutralności sieci. BEREC wskazał, że będzie to zależało od celu, w jakim zarządzanie ruchem jest

ustanowione, okoliczności sprawy oraz wpływu na cele określone w Dyrektywie (wpływ na rozwój konkurencji, inwestycje mające na celu poprawę efektywności sieci telekomunikacyjnych oraz otwartość Internetu).

Jednocześnie Komisja Europejska w podsumowaniu do konsultacji na temat otwartości i neutralności Internetu wskazała, że podmioty biorące w nich udział są zgodne co do konieczności zarządzania ruchem w Internecie. W ich opinii techniki te są używane w celu przeciwdziałaniu przeciążeniu sieci oraz gwarantują zachowanie bezpieczeństwa. Natomiast nie są one skierowane przeciwko zasadom związanym z neutralnością Internetu. Organizacje konsumenckie są jednak zaniepokojone gwarancjami zachowania prywatności, w szczególności wykorzystywaniem takich technik jak *Deep Packet Inspection* (DPI). DPI może być stosowane w celu zarządzania ruchem w sieci i wykorzystywane w celu prowadzenia monitoringu działań podejmowanych w Internecie, co ma m.in. umożliwić kierowanie reklam do określonych użytkowników końcowych. Pogląd ten jest podzielany przez Europejskiego Pełnomocnika ds. Ochrony Danych, który wskazał na takie praktyki jak przechwytywanie danych o ruchu. Jego zdaniem Komisja Europejska w dyskusji na temat polityki w zakresie neutralności sieci powinna wziąć również pod uwagę takie aspekty, jak fundamentalne prawo do zachowania tajemnicy komunikacji oraz ochrony danych.

W debacie na temat zarządzania ruchem w sieci istotne było również określenie, czy odpowiednie zasady dotyczące stosowania tego rodzaju technik powinny być tożsame w sieciach stacjonarnych oraz mobilnych.

BEREC w konsultacjach wyraził opinię, że podejście do zachowania neutralności sieci nie powinno się różnić w zależności od typu sieci. W przypadku operatorów mobilnych należy mieć jednak na uwadze, że w związku z ograniczoną przepustowością sieci mobilnych niektóre usługi nie mogą być realizowane. Operator takiej sieci może podjąć działania mające na celu uniknięcie sytuacji, w której tylko niektórzy użytkownicy wykorzystują całą pojemność sieci. Istotne jest zatem zagwarantowanie użytkownikom końcowym możliwości korzystania z podstawowych usług takich jak usługi telefoniczne, możliwość przegląda stron internetowych czy też wysłania e-maili. Możliwość korzystania z Internetu w sieciach mobilnych może być ograniczana dla użytkowników końcowych (bardziej niż w przypadku stacjonarnych sieci, których pojemność jest większa) w pewnych okolicznościach i do momentu, w którym nie dotyczy to selektywnego traktowania kontentu, neutralność sieci nie będzie zagrożona. Techniki zarządzania ruchem w sieci będą zatem różnić się zasadniczo w przypadku sieci mobilnych i stacjonarnych, bowiem sieci mobilne ze względu na swoją pojemność wymagają zastosowania szerszego zakresu reguł zarządzania siecią. Jednocześnie większość podmiotów, biorąc udział w konsultacjach, podziela ww. pogląd.

Struktura rynku

Komisja Europejska podkreśliła, że Internet jest złożonym ekosystemem, na który składają się określonego rodzaju działania oraz gracze (włączając w to usługi online i dostawców kontentu). Umożliwia on różnym technologiom i usługom na połączenie ze sobą oraz wzajemne oddziaływanie. Wszyscy gracze są istotni z punktu widzenia ekonomicznego oraz potrzebują siebie nawzajem w celu zdobycia zainteresowania konsumentów. Operatorzy sieci oraz dostawcy usług internetowych potrzebują atrakcyjnych aplikacji oraz kontentu, który skłoni użytkowników do podpisania z nimi umowy o świadczenie szerokopasmowych usług lub wybrania nowej, o lepszej jakości. Jednocześnie dostawcom kontentu oraz usług online zależy na odpowiednim połączeniu z Internetem, by skierować swoją ofertę do potencjalnych klientów. Konsumenci tym samym ze względu na możliwość korzystania z aplikacji oraz usług świadczonych za pośrednictwem Internetu są zainteresowani uzyskaniem dostępu do tej sieci.

Jednocześnie istnieje pokusa dla przedsiębiorców telekomunikacyjnych w poszukiwaniu zysków z usług świadczonych za pośrednictwem ich sieci, bowiem opłaty z tytułu zawartych umów z użytkownikami końcowymi mogą być niewystarczające na finansowanie przyszłych inwestycji w rozwój sieci. Uzgodnienia pomiędzy operatorami sieci oraz dostawcami kontentu/usług są obecnie przedmiotem komercyjnych negocjacji.

Przepływ ruchu pomiędzy sieciami, który ostatecznie dostarcza kontent do użytkownika końcowego, jest złożony. Może on następować na podstawie umów peeringowych, które często zapewniają bezpłatną wymianę ruchu (w przypadku gdy wymiana ruchu pomiędzy sieciami jest zbilansowana). Komisja Europejska zwróciła uwagę, że podczas gdy tego rodzaju umowy są normą pomiędzy operatorami sieci szkieletowych, to operatorzy sieci również zawierają tego rodzaju kontrakty z firmami internetowymi, nawet wtedy gdy ruch pomiędzy nimi jest asymetryczny. Innym sposobem jest podpisanie umowy w zakresie IP tranzyt. W tym przypadku pobierana jest opłata za dostęp do sieci szkieletowej całego środowiska internetowego.

BEREC w omawianych konsultacjach podkreślił między innymi, że dochód dostawców usług internetowych jest uzależniony od liczby zawartych umów z użytkownikami końcowymi, którzy głównie pobierają dane z Internetu, natomiast w mniejszym stopniu od umów zawartych z dostawcami kontentu/aplikacji. Można ewentualnie wyróżnić przedsiębiorców telekomunikacyjnych znajdujących się wysoko w hierarchii sieci (określone poziomy Tier), którzy zawierają umowy w zakresie IP tranzyt i czerpią z nich dodatkowe zyski. W związku z powyższym, zdaniem BEREC, należy rozróżnić relacje pomiędzy dostawcami usług internetowych a użytkownikami końcowymi oraz dostawcami usług internetowych i dostawcami kontentu/aplikacji.

Biorąc pod uwagę pierwszy typ relacji oraz przepływ pieniężny, od użytkowników końcowych do dostawców usług internetowych, przedsiębiorcy telekomunikacyjni podnoszą, że płynące zyski są nieproporcjonalne do ponoszonych kosztów związanych z zapewnieniem odpowiedniej infrastruktury. Ich zdaniem jednolita stawka za dostęp do sieci Internet w przypadku wymiany danych w godzinach szczytu nie pokrywa wszystkich kosztów dostawcy usług internetowych. Przedsiębiorcy telekomunikacyjni rozważają w tym zakresie możliwość określania maksymalnego przesyłu danych albo podwyższenie ceny w abonamencie. Wprowadzenie ograniczenia maksymalnego przesyłu danych lub ceny za odpowiedni pakiet danych możliwy do wykorzystania w abonamencie może być niezależne od typu danych (na przykład w sytuacji określenia pakietu danych możliwych do wykorzystania w danym okresie lub limitu przepływności) albo zależne od typu kontentu (spowalnianie wymiany danych w aplikacjach p2p). Pierwsza z metod w opinii BEREC nie stanowi odstępstwa od zasady neutralności sieci, natomiast druga łamie tę zasadę z uwagi na traktowanie w odmienny sposób określonego typu danych.

BEREC jako przykład stosowania pierwszej metody podał stosowanie w regulaminach przez dostawców usług internetowych klauzuli „sprawiedliwego dostępu" (*Fair Use Policy*), która jest zazwyczaj sformułowana w sposób ogólny i polega na ograniczeniu przepustowości łącza u tych użytkowników, którzy nadmiernie przeciążają łącza.

Przy ocenie tego typu praktyk, zdaniem BEREC, należy brać pod uwagę dwa aspekty. Po pierwsze użytkownicy, którzy nadmiernie wykorzystują przepustowość łącza, mogą być początkującymi abonentami usługi dostępu do Internetu i w dłuższym okresie czasu będą w rozsądny sposób korzystać z Internetu. Tym samym może istnieć

zagrożenie w zakresie możliwości zdobywania doświadczenia przez nowych użytkowników. Po drugie ograniczenie przepustowości łącza nie oznacza koniecznie rozwiązania problemu przeciążania w godzinach szczytu. W opinii BEREC w każdym z powyższych przypadków powinna być zapewniona przejrzystość zasad świadczenia usługi dostępu do Internetu. W regulaminach powinny być umieszczone informacje na temat określonych parametrów, a nie jedynie odniesienie się do polityki „sprawiedliwego dostępu".

Biorąc pod uwagę przepływ pieniężny od dostawców kontentu/aplikacji do dostawców usług internetowych, BEREC podkreślił, że występuje on zazwyczaj w przypadku bezpośredniego połączenia tych podmiotów. Usługi hostingowe oraz w zakresie łączenia lokalnej sieci nie są jednocześnie regulowane. W przypadku gdy dostawca kontentu/aplikacji nie jest podłączony do określonego dostawcy usług internetowych, wymiana ruchu odbywa się na podstawie umów peeringowych/tranzyt pomiędzy określonymi przedsiębiorcami telekomunikacyjnymi. BEREC wskazał równocześnie, że tego typu umowy są w przeważającej części poza przedmiotem działań krajowych organów regulacyjnych, co może być usprawiedliwione występowaniem konkurencji na rynku tranzyt na poziomie sieci szkieletowej IP. Jednocześnie zdaniem BEREC obecne porozumienia pomiędzy ww. podmiotami są adekwatne do panującej sytuacji na rynku, a krajowe organy regulacyjne powinny go stale monitorować w celu podjęcia ewentualnych działań w przyszłości.

Konsumenci na rynku internetowym oraz jakość usługi dostępu do Internetu

Komisja Europejska zauważa, że na rynku, na którym występuje konkurencja, konsumenci korzystający z usługi telekomunikacyjnej o pogarszającej się jakości, mogą zmienić jej dostawcę.

Jednocześnie w przypadku gdy tylko określone usługi i aplikacje działają „wolniej", nie zawsze jest jasne, gdzie leży przyczyna takiego ich funkcjonowania oraz ewentualna odpowiedzialność odpowiedniego podmiotu. Komisja Europejska dostrzega problemy z jakimi mogą spotkać się konsumenci, którzy wyrażają wolę zmiany przedsiębiorcy telekomunikacyjnego. W szczególności dotyczy to okresu, na jaki zawierana jest umowa, usług wiązanych, w których tylko jedna z usług jest świadczona poniżej odpowiedniej jakości, czy też obszarów, na których nie działają inni dostawcy usługi dostępu do Internetu.

Jednocześnie w przypadku występowania ograniczonej konkurencji na danym rynku oraz ewentualnych wysokich kosztów związanych ze zmianą dostawcy usługi dostępu do Internetu udzielanie konsumentom przejrzystych informacji na temat zarządzania ruchem może być niewystarczające.

W konsultacjach BEREC, odnosząc się do obowiązku udzielania przejrzystych informacji przez dostawców usług internetowych użytkownikom końcowym, powołał się na przepisy Dyrektywy 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (Dyrektywa). Zgodnie z art. 20 ust. 1 lit b) punkt 2 Dyrektywy umowa o świadczenie publicznie dostępnych usług łączności elektronicznej powinna zawierać informacje o wszelkich warunkach ograniczających dostęp do usług i aplikacji lub korzystania z nich w przypadku, gdy warunki takie dopuszcza prawo krajowe zgodnie z prawem wspólnotowym. BEREC podkreślił, że fundamentalne dla konsumentów jest otrzymanie informacji, która pozwoli im na zidentyfikowanie odstępstw od zasad związanych z neutralnością sieci. W przypadku blokowania określonych portów konsument powinien zostać również

poinformowany o aplikacjach, z których nie może korzystać. Dla konsumentów ważny jest dostęp do przystępnych informacji, pozwalających bez trudu dowiedzieć się, jak ograniczenia ustanowione przez dostawcę usługi internetowej będą działać w praktyce.

Ponadto zgodnie z art. 20 ust. 1 lit. b punkt 3 Dyrektywy umowa o świadczenie publicznie dostępnych usług łączności elektronicznej musi zawierać minimalne oferowane poziomy jakości usług, a mianowicie czas wstępnego przyłączenia, a w odpowiednich przypadkach także inne parametry jakości usług określone przez krajowe organy regulacyjne. W opinii BEREC w przypadku usługi dostępu do Internetu określenie parametrów jakości może okazać się trudne. Przede wszystkim trzeba zwrócić uwagę, że dostęp do Internetu jest zazwyczaj asymetryczny (większa przepływność dla odbierania niż wysyłania danych) i jest istotne właściwe określenie prędkości dla obydwu kierunków. Jednocześnie w przypadku tej usługi jakość jej świadczenia nie może być nawet zagwarantowana dla określonego dostawcy usług internetowych, pomimo podpisanych porozumień w zakresie IP Peering albo IP tranzyt. Zdaniem BEREC jednym ze sposobów poprawy przejrzystości usług dostępu do Internetu może być podawanie odpowiednich wartości jakości usługi dla poziomu ostatniej mili (ostatni poziom sieci, to znaczy odcinek pomiędzy węzłem sieci szkieletowodystrybucyjnej a użytkownikiem końcowym) oraz dodatkowo dla poziomu interkonektowego.

BEREC zwrócić jednocześnie uwagę na obecne warunki umów o świadczenie usługi dostępu do Internetu, które w zakresie informacji o jakości świadczenia tej usługi ograniczają się do sformułowań: „do" określonej prędkości, „nieograniczony" dostęp, „darmowy" dostęp. Przedstawione powyżej regulacje Dyrektywy mogą przyczynić się tym samym do zmniejszenia różnic pomiędzy maksymalną przepływnością łącza określoną w warunkach ww. umów a faktycznie możliwą do wykorzystania przez użytkownika końcowego.

Umowa o świadczenie publicznie dostępnych usług łączności elektronicznej powinna również zawierać informacje dotyczące wszelkich procedur wprowadzonych przez przedsiębiorstwo w celu pomiaru i organizacji ruchu tak, aby zapobiec osiągnięciu pojemności łącza lub jej przekroczeniu oraz informacje o tym, jak procedury te mogą wpłynąć na jakość usług. Powyższy obowiązek wynika z art. 20 ust. 1 lit. b pkt 4 Dyrektywy. Zdaniem BEREC tego rodzaju informacja może być niezrozumiała dla użytkownika końcowego i wymagać od niego pewnej wiedzy technicznej. Niemniej jednak może ona stanowić narzędzie dla krajowych organów regulacyjnych w celu monitorowania sytuacji na rynku telekomunikacyjnym oraz ochrony użytkowników końcowych.

Niezależnie od powyższego istotne jest wskazanie, że zgodnie z art. 22 ust. 3 Dyrektywy, aby zapobiec pogorszeniu się jakości usług oraz utrudnieniom lub spowolnieniu ruchu w sieciach, krajowe organy regulacyjne państwa członkowskie będą mogły nałożyć na przedsiębiorstwo lub przedsiębiorstwa udostępniające publiczne sieci łączności minimalne wymogi w zakresie jakości usług. W opinii BEREC przepis ten może być implementowany przez kraje członkowskie m.in. poprzez umożliwienie krajowym organom regulacyjnym monitorowanie jakości usług „ex ante". Tym samym wszyscy operatorzy sieci mogą być monitorowani. Przepis ten, zdaniem BEREC, może być również interpretowany jako ewentualne upoważnienie do rozstrzygania przez krajowe organy regulacyjne sporów pomiędzy określonymi podmiotami. Na przykład dostawca kontentu mógłby złożyć skargę, iż jego usługa jest

w sposób nieuzasadniony degradowana przez dostawcę usług internetowych. Krajowe organy regulacyjne mogłyby zatem interweniować w związku z korzystaniem przez przedsiębiorców telekomunikacyjnych z określonych technik zarządzania ruchem.

Wymaga również pokreślenia, że zgodnie z art. 22 Dyrektywy krajowe organy regulacyjne przekazują Komisji Europejskiej – w odpowiednim czasie przed ustanowieniem wymogów w zakresie jakości usług – podsumowanie podstawy do działania, przewidywane wymogi i proponowany przebieg działań. Informacje te udostępniane są również BEREC. Po zbadaniu takich informacji Komisja Europejska może zgłaszać do nich uwagi lub wydawać zalecenia, w szczególności w celu zapewnienia, aby przewidywane wymagania nie wpływały niekorzystnie na funkcjonowanie rynku wewnętrznego. Przy podejmowaniu decyzji dotyczącej wymogów krajowe organy regulacyjne uwzględniają w jak największym stopniu uwagi lub zalecenia Komisji Europejskiej.

Znaczenie konsultacji

Konsultacje Komisji Europejskiej będą stanowić wkład w przygotowywane przez nią sprawozdanie na temat otwartości Internetu oraz neutralności sieci. Przyjmując pakiet dyrektywy zmieniający dotychczasowe ramy regulacyjne sektora telekomunikacyjnego, Komisja Europejska wydała wraz z nimi Oświadczenie w sprawie neutralności sieci. Komisja Europejska podkreśliła, że przywiązuje wielką wagę do zachowania otwartości i neutralności Internetu, z pełnym uwzględnieniem intencji współustawodawców, którzy pragną uczynić z neutralności sieci jeden z celów polityki i zasad regulacyjnych promowanych przez krajowe organy regulacyjne, a także do wzmocnienia związanych z tym wymogów w zakresie przejrzystości oraz dania krajowym organom regulacyjnym uprawnień pozwalających im zapobiegać pogarszaniu się jakości usług i utrudnianiu lub spowalnianiu ruchu w sieciach publicznych. Komisja Europejska zobowiązała się do uważnego obserwowania wdrażania przepisów dyrektyw regulujących rynek telekomunikacyjny w państwach członkowskich, w szczególności uwzględniając ochronę „swobód sieciowych" obywateli europejskich w swoim corocznym sprawozdaniu z postępu prac przedkładanym Parlamentowi Europejskiemu i Radzie. Komisja Europejska będzie jednocześnie monitorować wpływ rozwoju wydarzeń na rynku i postępu technicznego na „swobody sieciowe" i przedstawi Parlamentowi Europejskiemu i Radzie sprawozdanie mówiące o tym, czy potrzebne są dodatkowe wytyczne, a także będzie korzystać ze swych aktualnych uprawnień w zakresie prawa o konkurencji, aby odpowiednio reagować na wszelkie ewentualne działania antykonkurencyjne.

Źródła:

1. Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, Dziennik Urzędowy L 108 z 24.04.2002, str. 51-77
2. Dyrektywa Parlamentu Europejskiego i Rady 2009/136 WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dziennik Urzędowy L 337 z 18.12.2009, str. 11-36

3. *Oświadczenie Komisji w sprawie neutralności sieci*, Komisja Europejska, Dziennik Urzędowy C 308 z 18.12.2010, str. 2. Dokument dostępny na stronie internetowej: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:308:0002:0002:P L:PDF
4. *The Antitrust Economics of multi-sided platform markets*, David S. Evans, LECG 2004, pierwotnie opublikowany w Yale Journal on Regulation, Volume 20, 2003. Dokument dostępny na stronie internetowej: http://www.lecg.com/Files/Publication/d4379b52-3da7-43e7-b38a-e0c05c6216c1/Presentation/PublicationAttachment/53a94436-749d-4702-b20b-e48fe812198e/the_antitrust_economi cs_of_multi-sided_platform_markets.pdf
5. *Questionnaire for the public consultation on the open Internet and net neutrality in Europe*, European Commission, 30 June 2010. Dokument dostępny na stronie internetowej: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/nn_questionnaire.pdf
6. *Report on the public consultation on the open internet and net neutrality in Europe*, European Commission, 9 November 2010. Dokument dostępny na stronie internetowej: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf
7. *BEREC response to the consultation on the open Internet and net neutrality in Europe*, Body of European Regulators for Electronic Communications, 4 October 2010. Dokument dostępny na stronie internetowej: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/04eu_national_regional_ministries_authorities_incl_berec/berec_x.pdf

Abstract

Summary of European Commission public consultation on "The open internet and net neutrality"

The public consultation on the issue of net neutrality and open Internet launched by the European Commission (EC) began on June 30, 2010, and ended on September 30, 2010. The prepared by the EC questionnaire for the public consultations focused on such subjects as:

1. The open internet – current problems, future problems and the suitability of the EU framework.
2. Traffic management – necessity, transparency and managed services.
3. Market structure.
4. Consumers and quality of service.
5. The political, cultural and social dimension.

As many as 318 stakeholders in the telecommunications market presented their opinion (ex. operators, internet service providers, consumer and civil society organizations, as well as individuals), among them the European Regulators for Electronic Communications (BEREC). The number and source of submitted opinions underlines the importance of a new telecom framework. The aim of the publication is to show different views of stakeholders submitted for the consultation concerning 1-4 subjects, especially focusing on the input provided by BEREC.

Jacek Kowalski - Główny Specjalista w Departamencie Detalicznego Rynku Telekomunikacyjnego Urzędu Komunikacji Elektronicznej

Czynniki społeczno-psychologiczne hamujące rozwój elektronicznej administracji w Polsce

Edyta Marcinkowska

W kwietniu 2010 roku Organizacja Narodów Zjednoczonych opublikowała raport *United Nations E-Goverment Survey 2010. Leveraging e-goverment at a time of financial and ekonomic crisis*[1], stanowiący analizę postępów we wdrażaniu technologii informatycznych w administracji publicznej w poszczególnych krajach. Polska w zestawieniu tym uplasowała się na 45 miejscu i odnotowała spadek o 12 pozycji w stosunku do roku 2008, kiedy to zajmowała 33 miejsce. W budowaniu elektronicznej administracji prześcigają nas Węgrzy, Czesi, Słowacy i Bułgarzy. Tylko w nieznacznym stopniu Polska wyprzedza Rumunię, Ukrainę i Białoruś.

Raport ONZ składa się z szeregu komponentów, wśród których warto zwrócić szczególną uwagę na trzy. W obszarze kapitału ludzkiego Polska zajmuje 31 miejsce, w obszarze usług administracyjnych dostępnych online miejsce 50, zaś w obszarze dostępności infrastruktury telekomunikacyjnej - 53 miejsce. Nie jest to wynik satysfakcjonujący, zważywszy, że trzy lata temu,

Tab. 1

Country	E-government development index value		World e-government development ranking	
	2010	2008	2010	2008
Hungary	0,6315	0,6494	27	30
Czech Republic	0,6060	0,6696	33	25
Slovakia	0,5639	0,5889	43	38
Bulgaria	0,5590	0,5719	44	43
Poland	0,5582	0,6134	45	33
Romania	0,5479	0,5383	47	51
Ukraine	0,5181	0,5728	54	41
Russian Federation	0,5136	0,5120	59	60
Belarus	0,4900	0,5213	64	56
Republic of Moldova	0,4611	0,4510	80	93
Sub-regional average	0,5449	0,5689		
World average	0,4406	0,4514		

1 Źródło: http://www2.unpan.org/egovkb/global_reports/10report.htm

23 listopada 2010 r., gdy Donald Tusk przedstawiał w Sejmie program działania nowego rządu[2], wśród prawie dwustu postulatów wskazał dwa dotyczące potrzeby wdrażania nowych technologii w obszar funkcjonowania administracji publicznej oraz jeden dotyczący rozwoju szerokopasmowego Internetu.

„Chcielibyśmy zmienić zasady funkcjonowania administracji publicznej, aby wreszcie umożliwić administracji efektywne wykorzystanie nowoczesnych technologii informatycznych. To będzie niezbędne, żeby praca administracji i samorządowej, i rządowej była rzeczywiście przejrzysta, dużo szybsza, wygodniejsza i bardziej przyjazna też dla obywateli, nie tylko dla wykonawców tej pracy."

„Chcielibyśmy uzyskać takie efekty, jak choćby likwidacja części dokumentów identyfikacyjnych, na przykład przez wprowadzenie tak zwanego e-dowodu osobistego, a więc elektronicznego potwierdzania tożsamości w Internecie. Chciałbym także, abyśmy mogli udostępniać obywatelom i instytucjom dane z podstawowych rejestrów publicznych właśnie drogą informatyczną."

„Współczesna komunikacja to przede wszystkim Internet. Jest to jeden z kluczowych czynników sukcesu gospodarczego i cywilizacyjnego naszego kraju. Szczególną wagę przywiązujemy do zapewnienia powszechnego dostępu do Internetu szerokopasmowego. To także wymóg nowoczesnego patriotyzmu. Stworzymy mechanizmy, dzięki którym wszędzie w Polsce, także w małych miejscowościach i na polskiej wsi, ludzie będą mogli skorzystać z dobrodziejstwa globalnej sieci".

Mimo że budowa elektronicznej administracji w Polsce jest jednym z priorytetów obecnego rządu, to nieustannie ponosi on na tym polu druzgocącą porażkę. Przyczyn takiego stanu rzeczy jest kilka. Po pierwsze brakuje zdolności do wypracowania właściwej wizji elektronicznej administracji i narzucenia jej wszystkim podmiotom administracji publicznej. Po drugie, budując systemy informatyczne, za bardzo skupiono uwagę na aspektach technologicznych, a nie na rzeczywistych potrzebach ludzi i firm. Jednak to nie brak narzędzi informatycznych jest największym hamulcem w rozwoju elektronicznej administracji, lecz – paradoksalnie – są nim sami urzędnicy.

Skostniałość organizacyjna

Współczesna administracja pod względem strukturalnym nieznacznie różni się od administracji dziewiętnastowiecznej[3], którą scharakteryzował Max Weber – niemiecki historyk, socjolog i ekonomista. Polska administracja nie jest wyjątkiem. Charakteryzuje się wysokim poziomem sformalizowania i wyraźnie zaznaczoną hierarchią - urzędy niższe kontrolowane są przez urzędy zwierzchnie.

Wszystkie działania, także stosunki i zależności między poszczególnymi urzędnikami, są uregulowane określonymi przepisami. Ich nadmiar, zauważalny zwłaszcza po wstąpieniu Polski do Unii Europejskiej i związany z dostosowaniem polskiego prawodawstwa do unijnych regulacji, prowadzi do sytuacji kuriozalnych, gdy przestrzeganie przepisów staje się ważniejsze od realizacji celów, do jakich dany urząd został powołany lub gdy urząd, skupiając się na własnym funkcjonowaniu, zaprzestaje świadczeniu usług na rzecz obywateli.

2 Źródło:http://orka2.sejm.gov.pl/Debata6.nsf/91668423b136667cc12573930043a099/c2f0913296a12fedc12573ad0041f851?OpenDocument

3 Antonina Kłoskowska, *Biurokracja,* w: *Encyklopedia socjologii, t. 1.,* Warszawa 1998, s. 69.

Zadania kierowane są zgodnie z ustaloną strukturą organizacyjną i przekazywane jako obowiązki służbowe. Każdy urzędnik ma wyraźnie określony obszar działania, zgodny ze swoimi kompetencjami, za który jest odpowiedzialny i poza który stara się nie wykraczać, by nie narazić się na zarzut przekroczenia kompetencji. Jednak nadmierne dyscyplinowanie urzędnika nieuchronnie prowadzi do kurczowego trzymania się przez niego przepisów. Wywołuje zachowania o charakterze rytualizmu i formalizmu, wyuczoną bezradność, nieudolność oraz brak sprawnego działania w przypadku sytuacji nietypowych, które nie zostały uwzględnione w obowiązujących przepisach.

Niepotrzebne mnożenie liczby ekspertów w ramach jednego urzędu sprawia, że trudniej wypracować wizję danego działania oraz zbudować na jej podstawie odpowiednią strategię komunikacji. Obecność zbyt dużej liczby niemogących dojść do porozumienia ekspertów staje się zarzewiem nierozstrzygalnych konfliktów między bazującymi na wiedzy i doświadczeniu ekspertami a urzędnikami, dla których najważniejsza jest struktura organizacyjna i związane z nią określone zadania.

Administracja publiczna wypracowała charakterystyczny sposób komunikacji. W modelu tym wymiana informacji następuje tylko poprzez przekazywanie oficjalnych dokumentów, które - gromadzone w szafach - stają się mało funkcjonalną pamięcią danego urzędu. Ze względu na strukturę organizacyjną i procedury określone w Kodeksie Postępowania Administracyjnego proces wymiany informacji pomiędzy urzędami rozciąga się w czasie. W wielu urzędach po wdrożeniu systemu elektronicznego obiegu dokumentów okazywało się, że zaczęły funkcjonować dwa równoległe obiegi – elektroniczny i tradycyjny. Kilkusetletnie przyzwyczajenie do fizycznego przenoszenia papieru między urzędami, pokojami, szafami i segregatorami było tak silne, że nie potrafiono zaakceptować nowych narzędzi.

Urzędnicy są charakterystyczną grupą zawodową; dostrzegają szereg problemów związanych z wdrażaniem nowych rozwiązań. Zwłaszcza rozwiązania innowacyjne są dla nich nietypowe, bo wymagają nie tylko reorganizacji stanowiska pracy, ale także istniejącej struktury organizacyjnej, do której zdążyli przywyknąć.

W urzędach znajduje się ogromna liczba dokumentów i informacji w nich zawartych. Jednak nie wypracowały one narzędzi, dzięki którym mogłyby szybko i skutecznie je przetwarzać i przekazywać między sobą. W związku z tym obywatel jest nieustannie proszony o wypełnianie tych samych formularzy i podawanie informacji, które dany urząd już posiada, a nawet takich, które w danym postępowaniu nie są wymagane. Mając powyższe na uwadze, należy zauważyć, że praca sporej liczby urzędników ogranicza się do bezrefleksyjnego wprowadzania do systemów po wielokroć tych samych danych.

Cechą charakterystyczną urzędników jest dążenie do utrzymania trwałości ukształtowanych już struktur biurokratycznych, ponieważ gwarantują one zachowanie poczucia bezpieczeństwa oraz uzyskanie maksimum korzyści przy minimalnym nakładzie pracy.

Niska wydajność pracy

Kariera urzędników i awans w ramach organizacji są zależne od ich stażu pracy i zgodne z obowiązującymi przepisami. W Polsce dzięki regulacjom prawnym trudno pozbawić urzędnika pracy. Poczucie stałości zatrudnienia aż do emerytury - gwarantowane już na początku kariery zawodowej - przyczynia się do szerzenia postawy konformizmu wśród urzędników, a także rodzi szereg postaw negatywnych. Wśród urzędników w wyniku rutyny mogą nasilać się uprzedzenia czy antypatie wpływające na atmosferę pracy. Wewnątrz instytucji mogą pojawić się również nieformalne grup,

które mają duży wpływ na jej funkcjonowanie, głównie w odniesieniu do zdobywania władzy i realizacji partykularnych interesów.

Mimo znacznie rozszerzonej od początku tego roku swobody zarządzania kadrami większość polskich urzędów nie stosuje żadnych form premiowania efektywności. Do obniżenia wydajności pracy przyczynia się również archaiczny system wynagradzania urzędników. Premiowana jest wysługa lat, a nie kompetencje i wydajność. Analizując z tej perspektywy, urzędnikowi nie opłaca się zatem ani podnosić kwalifikacji, ani angażować w wypracowanie mechanizmów podnoszących jakość pracy w danej instytucji. Urzędnicy nie podlegają także karom za podejmowanie błędnych decyzji administracyjnych. W związku z tym brak motywacji zarówno pozytywnej, jak i negatywnej przyczynia się do urzędniczej opieszałości.

Polska administracja cierpi na syndrom Prakinsona, który głosi, że jeżeli pracownik ma określony czas na wykonanie danego zadania, to zostanie ono wykonane w możliwie najpóźniejszym terminie. Oznacza to, że wzrost liczby pracowników nie jest związany ani z ilością pracy, ani z jej rodzajem. W Polsce zatrudnianiem nowych urzędników próbuje się rekompensować niską wydajność administracji.

Przerost zatrudnienia

Tylko w drugim kwartale 2010 r. liczba pracujących w sektorze administracji publicznej (w tym obrony narodowej i obowiązkowych zabezpieczeń społecznych, bez zatrudnionych w działalności w zakresie obrony narodowej i bezpieczeństwa publicznego, czyli bez żołnierzy, policjantów i funkcjonariuszy służb specjalnych) wzrosła do 643,7 tys., podczas gdy pod koniec czwartego kwartału 2009 r. wynosiła 620,6 tys.[4] Według danych Głównego Urzędu Statystycznego urzędnicy w pierwszym półroczu stanowili ok. 7,7% zatrudnionych.[5]

Średnie wynagrodzenie urzędników rośnie w stosunku do średniego wynagrodzenia w całej gospodarce. W pierwszym półroczu 2010 r. średnie wynagrodzenie urzędników wynosiło 3746,28 zł brutto miesięcznie i było wyższe od średniej w sektorze prywatnym o 1,08%.[6]

Trudno się zatem dziwić obawom urzędników związanym z utratą miejsc pracy, skoro administracja publiczna oferuje nie tylko atrakcyjniejsze wynagrodzenie, lecz także stabilniejsze warunki pracy.

Biurokracja po polsku

Wśród cech charakterystycznych dla polskiej administracji wskazać należy przede wszystkim niechęć do jakichkolwiek zmian, strach przed wdrażaniem innowacyjnych rozwiązań, niewydajność pracy, przerost zatrudnienia oraz strach przed utratą pracy. Wymienione wyżej czynniki, gwarantujące zachowanie *status quo* urzędnika, przyczyniają się jednak nie tylko do skutecznego hamowania rozwoju elektronicznej administracji w Polsce, a co za tym idzie utraty konkurencyjności polskiej gospodarki, lecz także przekładają się na jakość życia obywateli.

Urzędnicy mają nie tylko wpływ na to, jak wygląda okolica, w której mieszkamy, pracujemy, wypoczywamy - odpowiadają za budowę

4 *Zatrudnienie i wynagrodzenia w gospodarce narodowej w I półroczu 2010 r.*, oprac. Teresa Żelazny, Warszawa 2010, s. 33.
5 Tamże, s. 15.
6 Tamże, s. 16.

kanalizacji, dróg, rozwój infrastruktury oraz pozyskiwanie środków z Unii Europejskiej, lecz także mają pośredni wpływ na jakość naszego życia. Gdyby byli otwarci na nowe technologie, działali szybko, sprawnie i rzetelnie, to już dziś można by było założyć firmę, zarejestrować samochodu, zameldować się w nowym miejscu zamieszkania, uzyskać pozwolenie na wycinkę drzewa, umorzyć podatek, uzyskać pozwolenia na budowę, czy otrzymać odpisu aktu stanu cywilnego, nie wychodząc z domu. Wystarczyłby tylko komputer i dostęp do Internetu. Jednak urzędnicy skutecznie blokują rozwój tego typu usług.

Bez współpracy między resortami i budowy podmiotu odpowiedzialnego za koordynację działań informatyzacyjnych nie można liczyć na szybką poprawę. Polska administracja, by sprostać wymaganiom XXI wieku, musi przejść gruntowną reformę, bo w przeciwnym razie pozostaniemy z elektronicznie zacofaną administracją.

Streszczenie

Dlaczego Polska, mimo wsparcia finansowego Unii Europejskiej, nie radzi sobie z wdrożeniem elektronicznej administracji? Po pierwsze dlatego, że brakuje zdolności do wypracowania właściwej wizji elektronicznej administracji i narzucenia jej wszystkim podmiotom administracji publicznej. Po drugie, gdy budowano systemy informatyczne, za bardzo skupiono uwagę na aspektach technologicznych, a nie na rzeczywistych potrzebach ludzi i firm. Jednak głównej przyczyny takiego stanu rzeczy należy upatrywać na płaszczyźnie psychologiczno-społecznej. Największym hamulcem w rozwoju elektronicznej administracji w Polsce wydają się być sami urzędnicy.

Edyta Marcinkowska - zajmuje się komunikacją społeczną, medialną i kulturową. Od połowy 2009 r. związana z Centrum Projektów Informatycznych Ministerstwa Spraw Wewnętrznych i Administracji.

Proponujemy

X edycja seminarium w cyklu NOWOCZESNE MUZEA I GALERIE „SYSTEMY KATALOGOWANIA I DOKUMENTOWANIA ZBIORÓW MUZEALNYCH"

1 lutego 2011 r., Warszawa

Fakt organizacji X edycji seminarium w cyklu Nowoczesne Muzea i Galerie zobowiązuje do szczególnej atrakcyjności treści merytorycznych programu. Wybraliśmy temat dotyczący katalogowania i dokumentowania zbiorów, ponieważ sugestie i postulaty uczestników poprzednich edycji wyraźnie wskazywały ten obszar tematyczny. Poza tym uznaliśmy, iż prezentacja tego tematu zawiera ciekawe wątki zarówno technologiczne, jak i organizacyjno-prawne. Jeden z tematów programu, czyli archiwizacja przestrzennych dzieł sztuki, wydał się na tyle nośny i merytorycznie atrakcyjny, że postanowiliśmy poświecić mu odrębny warsztat w terminie 23 marca 2011 r.

W PROGRAMIE:

- Społeczeństwo informacyjne a nowe wyzwania dla muzeów.
- Międzynarodowe standardy opisu obiektów muzealnych jako podstawa katalogowania zbiorów.
- Opis dóbr kultury - tradycja a digitalna współczesność.
- Metadane na poziomie kolekcji muzealnych.
- System 3DMADMAC - skaner trójwymiarowy do archiwizacji przestrzennych dzieł sztuki.
- Wykorzystanie przez muzea własnych zbiorów do promocji i jako źródła dodatkowych dochodów - problemy prawne.
- Rozpowszechnianie utworów w Internecie przez muzea.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Przetwarzanie danych osobowych stanowiących tajemnicę bankową w świetle orzecznictwa sądów administracyjnych

Beata Bińkowska-Artowicz

Wprowadzenie

Celem niniejszego artykułu jest przedstawienie problematyki stanowiącej przedmiot orzecznictwa sądowoadministracyjnego z zakresu łączącego prawo gospodarcze (bankowe) oraz prawo o ochronie danych osobowych.

W pierwszej kolejności wyjaśnienia wymaga wyrażenie zawarte w tytule opracowania: "przetwarzanie danych osobowych stanowiących tajemnicę bankową". W art. 105a ust. 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe [t. jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.] (dalej: uPrB), statuującym uprawnienia w zakresie dysponowania danymi przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4 uPrB, ustawodawca zawarł sformułowanie: *„przetwarzanie informacji stanowiących tajemnicę bankową"*. Jak słusznie zauważono w literaturze przedmiotu[1], omawiana ustawa nie zawiera definicji legalnej pojęcia „przetwarzanie informacji stanowiących tajemnicę bankową". Uwagi na temat konieczności wprowadzenia owej definicji przekroczyłyby ramy niniejszego artykułu, natomiast dla potrzeb poniższego zestawienia słuszne wydawało się zastąpienie ustawowych *"informacji w zakresie dotyczącym osób fizycznych"* przez *„dane osobowe"*[2], czyli pojęcie zdefiniowane w art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [t. jedn. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.] (dalej: uodo): „*W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej."*

Pojęcie tajemnicy bankowej zostało natomiast zdefiniowane w art. 104 uPrB: *"wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje"*.

Tematyka niniejsza wydaje się istotna m.in. z uwagi na rolę, jaką w działalności bankowej spełnia instytucja powołana do przetwarzania i udostępniania informacji stanowiących tajemnicę bankową– Biuro Informacji Kredytowej SA (dalej: BIK SA).

Przed omówieniem orzecznictwa należy zatem scharakteryzować tę instytucję ze wskazaniem norm regulujących jej działanie i zawartych w przepisach prawa powszechnie obowiązującego oraz skrótowo przedstawić prawne podstawy rozstrzygania w przedmiotowych sprawach.

BIK SA został utworzony w dniu 29 października 1997 r. przez kilkanaście banków działających na terenie Polski oraz Związek Banków

1 M. Krzysztofek, *Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej,* LexisNexis, Warszawa 2010, str. 22, str. 305

2 Naczelny Sąd Administracyjny w wyroku z 4 kwietnia 2003 r. sygn. akt II SA 2935/02 (LEX nr 149895) stwierdził, iż „Pojęcie danych osobowych klienta banku mieści się w pojęciu informacji i tajemnicy bankowej".

Polskich w celu zbudowania kompleksowej bazy danych, zawierającej dane o zobowiązaniach klientów banków oraz zaoferowania bankom narzędzi wspomagających decyzję o udzieleniu kredytu, zarządzanie pojedynczym rachunkiem kredytowym na każdym etapie jego istnienia, zarządzanie portfelem kredytowym oraz decyzje strategiczne[3]. Podstawę do utworzenia BIK SA stanowił art. 105 ust. 4 uPrB, w którym wskazano, że *„banki mogą, wspólnie z bankowymi izbami gospodarczymi, utworzyć instytucje do gromadzenia, przetwarzania i udostępniania:*

1) *bankom - informacji stanowiących tajemnicę bankową w zakresie, w jakim informacje te są potrzebne w związku z wykonywaniem czynności bankowych,*
2) *innym instytucjom ustawowo upoważnionym do udzielania kredytów - informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie, w jakim informacje te są potrzebne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń"* [4](stan prawny obowiązujący w dacie utworzenia BIK SA).

Przetwarzanie danych osobowych w działalności bankowej odbywa się na zasadach przewidzianych przepisami uodo oraz art. 105 i nast. uPrB. Zgodnie z art. 12 ust. 1 i 2 uodo kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych należy do zadań Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO).

Akty administracyjne wydawane przez GIODO mogą stać się natomiast przedmiotem skargi do sądu administracyjnego na podstawie art. 3 §2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi [Dz. U. Nr 153, poz. 1270 z późn. zm.] (dalej: ppsa). Wojewódzki sąd administracyjny może skargę uwzględnić, uchylając decyzję lub postanowienie w całości albo w części (art. 145 §1 pkt 1 ppsa), stwierdzić nieważność decyzji lub postanowienia w całości lub w części (art. 145 §1 pkt 2 ppsa) lub stwierdzić wydanie decyzji lub postanowienia z naruszeniem prawa (art. 145 §1 pkt 3 ppsa), jak również skargę oddalić (art. 151 ppsa). Od wyroku WSA na podstawie art. 173 ppsa co do zasady przysługuje skarga kasacyjna do Naczelnego Sądu Administracyjnego, który może oddalić skargę kasacyjną (art. 184 ppsa), uchylić zaskarżone orzeczenie w całości lub w części i przekazać sprawę do ponownego rozpoznania (art. 185 §1 ppsa) lub też – uchylić wydane w sprawie orzeczenie i rozpoznać skargę (art. 188 ppsa).

Przegląd orzecznictwa

W szeregu orzeczeń sądy administracyjne zwracały uwagę na legalność przetwarzania danych z uwagi na ochronę innych wartości niż ochrona danych osobowych.

Już w wyroku z 20 kwietnia 2006 r. sygn. akt II SA/Wa 2227/05[5] (dotyczącym wprawdzie przetwarzania innych danych niż objętych tajemnicą bankową) WSA w Warszawie zawarł cytowane następnie wielokrotnie

3 *Główna Broszura Informacyjna BIK*, luty 2003 r.

4 Przepis ten został zmieniony mocą art. 1 pkt 12 lit. b ustawy z dnia 26 stycznia 2007 r. o zmianie ustawy – Prawo bankowe [Dz. U. Nr 42, poz. 272] i otrzymał następujące brzmienie: „*Banki mogą, wspólnie z bankowymi izbami gospodarczymi, utworzyć instytucje upoważnione do gromadzenia, przetwarzania i udostępniania:*
   1) *bankom – informacji stanowiących tajemnicę bankową w zakresie, w jakim informacje te są potrzebne w związku z wykonywaniem czynności bankowych oraz w związku ze stosowaniem metod statystycznych, o których mowa w art. 128 ust. 3 oraz w art. 128d ust. 1,*
   2) *innym instytucjom ustawowo upoważnionym do udzielania kredytów – informacji stanowiących tajemnicę bankową w zakresie, w jakim informacje te są niezbędne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń."*

w orzecznictwie stwierdzenie, iż **ochrona danych osobowych na podstawie przepisów uodo nie powinna być oderwana od przepisów służących ochronie innych wartości.**

Wyprowadzając normę prawną z art. 105 ust. 4 uPrB, NSA wskazał, iż przewiduje on czynność powołania do życia **nowego podmiotu o charakterze publicznym**, zajmującego się w państwie określonym zakresem spraw, a nie powierzenia spraw podmiotowi, który już istniał wcześniej i prowadził inną działalność. Twierdzenie to sąd wysnuł na tle rozpoznawanej sprawy (wyrok NSA z 18 września 2003 r. II SA 2199/01[6]), w której rozstrzygał kwestię, czy umowa wspólników skarżącej spółki zawarta w 1999 r. w formie aktu notarialnego, dotycząca poszerzenia jej dotychczasowego przedmiotu działania, m.in. o *„zbieranie i udostępnianie bankom informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie, w jakim informacje te są potrzebne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń"*, była aktem utworzenia instytucji przewidzianej w art. 105 ust. 4 Prawa bankowego. Posługując się wykładnią systemową, sąd uznał, iż *„musi to być czynność powołania do życia nowego podmiotu o charakterze publicznym, zajmującego się w państwie określonym zakresem spraw, a nie powierzenia spraw podmiotowi, który już istniał wcześniej i prowadził inną działalność. Taka instytucja, w rozumieniu organizacyjnym, musi być funkcjonalnie powiązana z działalnością systemu bankowego"*. W stanie faktycznym rozpoznawanej sprawy spółka wnioskująca o rejestrację zbioru danych zawierających powyższe informacje została utworzona w 1993 r. przez kilka banków spółdzielczych w celu prowadzenia szerokiego wachlarza usług – m.in. akwizycji artykułów konsumpcyjnych, doradztwa finansowego, usług marketingowych, handlu artykułami konsumpcyjnymi, pośrednictwa usług ubezpieczeniowych i emerytalno-rentowych oraz usług detektywistycznych, ochrony osób i mienia. Sąd orzekł, iż banki-założyciele spółki bezzasadnie powierzyły takiemu podmiotowi gospodarczemu te tak ważne i specyficzne zadania do wykonywania przez zaledwie jednego pracownika i uznał za legalne odmowę rejestracji zbioru powyższych danych i nakazanie skarżącej usunięcia danych ze zbioru.

W orzeczeniu z 26 maja 2009 r. sygn. akt I OSK 808/08 [7] NSA wypowiedział się natomiast w kwestii tego, czy przepis art. 23 uodo pozwalał bankowi na przetwarzanie danych osobowych klienta poprzez ich **udostępnienie innemu podmiotowi bez jego zgody**. Sąd stwierdził, że zbycie przez bank wierzytelności przysługującej temu podmiotowi wobec skarżącego na rzecz banku stanowiło działanie mieszczące się w pojęciu dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej, gdyż spółka przejęła prawa i obowiązki banku wynikające z zawartej z nim umowy o korzystanie z karty kredytowej wobec skarżącego i miała prawo przetwarzać jego dane osobowe, w oparciu o przesłankę wynikającą z art. 23 ust. 1 pkt. 5 uodo, czyli prawnie usprawiedliwiony cel.

W innym orzeczeniu WSA w Warszawie wypowiedział się w kwestii zgodności przetwarzania danych stanowiących tajemnicę bankową z Konstytucją. Sąd uznał, że w przypadku braku możliwości przymusowego egzekwowania roszczenia banku wobec skarżącej (z uwagi na skutecznie podniesiony zarzut przedawnienia) pozostaje ona dłużnikiem banku – tak więc ZBP jako instytucja, o której mowa w art. 105 ust. 4 uPrB, w sposób w pełni uprawniony pozyskał od banku i poddał procesowi dalszego

5 http://orzeczenia.nsa.gov.pl
6 LEX nr 149555
7 LEX nr 513109

przetwarzania dane osobowe skarżącej w zakresie dotyczącym jej zobowiązań względem banku. – *"Jeżeli przyjąć, że* ***celem Bankowego Rejestru jest ochrona banków, a zwłaszcza ich depozytariuszy****, to przekazanie do rejestru prowadzonego przez ZBP danych osobowych kredytobiorcy Banku, który nie wykonał zobowiązania, znajduje uzasadnienie w art. 105 ust. 4 i art. 105a ust. 1 uPrBankowe oraz uodo, a tym* ***samym brak jest podstaw do zarzutu naruszenia art. 51 ust. 4 Konstytucji RP****"* (uzasadnienie wyroku WSA w Warszawie z 3 lutego 2009 r. II SA/Wa 1430/08[8]).

Dla celów przetwarzania danych osobowych stanowiących tajemnicę bankową ważne jest także utrwalone już w orzecznictwie sądów administracyjnych stanowisko, zgodnie z którym *„gdyby uznać każdy wypadek przetwarzania danych osobowych dłużnika (będącego konsumentem) za godzący w jego prawa i wolności, doszłoby z jednej strony do niczym nieuzasadnionej ochrony osób niewywiązujących się ze swoich zobowiązań, z drugiej natomiast do* ***naruszenia zasady swobody działalności gospodarczej, co z pewnością nie było zamiarem ustawodawcy*** *przy uchwalaniu ustawy o ochronie danych osobowych"*[9] (uzasadnienie wyroku WSA w Warszawie z dnia 30 listopada 2004 r., sygn. akt II SA/Wa 1057/04[10]).

Dla oceny roli, jaką odgrywa przetwarzanie przez banki oraz instytucje do tego upoważnione danych osobowych stanowiących tajemnicę bankową, szczególnie istotny wydaje się wyrok WSA w Warszawie z 27 lutego 2004 r., sygn. akt II SA 291/03[11], w którym sąd uznał, że *„z uwagi na obowiązki banków wynikające z przepisów art. 105-107 Prawa bankowego oraz ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu w prowadzeniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz przeciwdziałaniu finansowaniu terroryzmu, nakładającej na nie obowiązki jako instytucji obowiązanej, należy przyjąć, że* ***banki są w istocie instytucjami zaufania publicznego****"*.

Zgodnie z wykładnią dokonaną przez WSA w Warszawie niewątpliwym i oczywistym prawem banku jest również przetwarzanie danych osobowych nie tylko samej strony umowy kredytowej, ale też **wszystkich osób, których dane zostały zasadnie i w usprawiedliwionym zakresie zgromadzone w związku z zawarciem i wykonywaniem tej umowy** - poręczyciela, małżonka kredytobiorcy (ważnego z uwagi na majątkowy ustrój małżeński), jego dzieci (gdyż ich ilość i wiek wpływa na ocenę zdolności kredytowej), a także inne osoby, które mają znaczenie w praktyce umów bankowych – *„(...) nawet w razie uznania, że poręczyciel nie jest stroną umowy kredytowej, albo jest tą stroną dopiero w razie niewywiązania się ze swoich zobowiązań przez dłużnika głównego, bank uprawniony jest do przetwarzania danych poręczyciela. Jeśli takiego uprawnienia nie statuuje art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych, to niewątpliwe jest takie uprawnienie wynikające z punktu 5 tego przepisu, tj. z tzw. klauzuli usprawiedliwionego interesu. Trudno bowiem wyobrazić sobie umowę bankową, w której bank nie zgromadziłby odpowiednich informacji o swoim kliencie i innych osobach z nim związanych - zobowiązuje do*

8 http://orzeczenia.nsa.gov.pl

9 Orzeczenie to ma również niebagatelne znaczenie dla podmiotów prowadzących działalność w ramach biur informacji gospodarczych, utworzonych i działających na podstawie przepisów ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczej i wymianie danych gospodarczych [Dz. U. Nr 81, poz. 530]. Biura te spełniają funkcję baz danych o nierzetelnych dłużnikach.

10 LEX nr 236507

11 Lex nr 569664

tego nie tylko wzgląd na konieczność prawidłowego zabezpieczenia interesów banku, a także interesów ich klientów, ale explicite przesądza o takim obowiązku 70 ust. 1 Prawa bankowego, który nakazuje każdemu bankowi uzależnić udzielenie kredytu od zdolności kredytowej swojego klienta" (uzasadnienie wyroku WSA w Warszawie z 3 października 2006 r. II SA/Wa 871/06[12]). W powyższym wyroku sąd zwrócił uwagę także na sformułowaną w art. 26 ust. 1 pkt 2 uodo tzw. zasadę niezmienności celu przetwarzania danych osobowych, zgodnie z którą gromadzenie danych osobowych dla konkretnego, ściśle oznaczonego i wynikającego z konkretnych przesłanek celu, nie upoważnia administratora danych do ich wykorzystywania w celach innych niż te, dla których pierwotnie zostały zgromadzone. Zdaniem sądu w tym kontekście szczególne znaczenie ma legalność przetwarzania danych osobowych poręczyciela umowy kredytu w celach oceny zdolności kredytowej i oceny ryzyka kredytowego banku[13]. Sąd zauważył również, że na przetwarzanie danych osobowych strony skarżącej przez bank pozwalają uwarunkowania prawne wynikające z terminów przedawnienia roszczeń cywilnoprawnych - „*(...) jest oczywiste, iż każdy uczestnik cywilnego obrotu prawnego może zachować informacje o swoich kontrahentach nawet po wykonaniu przez nich swoich zobowiązań. Takie zachowanie danych byłego dłużnika stanowi usprawiedliwiony cel administratora danych. Usunięcie danych dłużnika natychmiast po wykonaniu przez niego zobowiązania z pewnością mogłoby spowodować negatywne, wymierne skutki materialne. Wymóg dbałości o bezpieczeństwo finansowe każdego wierzyciela, a zwłaszcza wyspecjalizowanych instytucji finansowych, jakimi są banki, nakazuje zachowywać informacje o swoich byłych klientach na wypadek podniesienia przez nich roszczeń po wykonaniu umowy kredytowej."*

W uzasadnieniu innego wyroku WSA w Warszawie uznał z kolei za oczywiste, że **w celu obracania wierzytelnościami oraz umożliwienia ich dochodzenia** na mocy art. 509 i nast. Kodeksu cywilnego, art. 96 ust. 1 i 2 oraz art. 97 ust. 1 uPrB, art. 758 i nast. oraz art. 801 §1 i 2 Kodeksu postępowania cywilnego konieczne jest przetwarzanie danych osobowych dłużnika zarówno przez wierzyciela, jak i organ egzekucyjny (wyrok z 7 lutego 2008 r. sygn. akt II SA/Wa 645/07[14]).

W ocenie WSA w Warszawie **prawidłowość wypowiedzenia umowy pożyczki czy wystawienia weksla co do zasady nie mają wpływu na legalność przetwarzania danych** osobowych skarżącej, o ile – jak w rozpoznawanej sprawie – strona skarżąca złożyła oświadczenie, że „*została poinformowana o przekazywaniu jej danych osobowych oraz informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie w jakim informacje te są niezbędne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń celem umieszczenia ich w bazie danych „Kredytobiorcy" oraz udostępnianie ich na zasadzie wzajemności*

12 Lex nr 283579

13 Powyższe stwierdzenie może budzić wątpliwości. Skoro bowiem z treści art. 876 i nast. ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny [Dz. U. Nr 16, poz. 93 z późn. zm.] wynika, że istotą instytucji poręczenia jest zobowiązanie się względem wierzyciela do wykonania zobowiązania na wypadek, gdyby dłużnik zobowiązania nie wykonał, to już pierwotny cel gromadzenia danych na temat poręczyciela z istoty rzeczy obejmuje ocenę jego zdolności kredytowej i ocenę ryzyka kredytowego banku – na wypadek, gdyby dłużnik główny zobowiązania nie wykonał. Z drugiej jednak strony w doktrynie (J. Barta, R. Markiewicz: Ochrona danych osobowych. Komentarz, Zakamycze 2007, komentarz do art. 26 ust. 1 pkt 2 uodo) podkreśla się, że wątpliwości dotyczące celu należy poczytywać na niekorzyść administratora, tj. w razie sporu uznawać cel za oznaczony tak, aby adekwatne do niego było przetwarzanie danych osobowych w węższym zakresie.

14 Lex nr 506285

bankom, instytucjom finansowym będącym podmiotami zależnymi od banków, a związanych z wykonywaniem przez te instytucje czynności bankowych oraz instytucjom ustawowo upoważnionym do udzielenia kredytów w zakresie określonym powyżej, a także przysługującym mu, zgodnie z przepisem art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych, prawem dostępu do jej danych oraz ich poprawiania. Pożyczkobiorca wyraża zgodę na przetwarzanie przez S. oraz B. powyższych informacji przez okres nie dłuższy niż 5 lat od dnia wygaśnięcia zobowiązania wynikającego z zawartej umowy" (uzasadnienie wyroku z 31 stycznia 2008 r. II SA/Wa 1958/07[15]).

W szeregu orzeczeń WSA w Warszawie wypowiadał się również odnośnie do tego, czy podmiot utworzony na podstawie art. 105 ust. 4 uPrB może legalnie przetwarzać dane osobowe kredytobiorcy dla **celów stosowania metod statystycznych**[16] bez jego zgody, skoro dane te otrzymał od banku dla innych celów, tj. oceny zdolności kredytowej.

W uzasadnieniu wyroku z 4 grudnia 2008 r. II SA/Wa 917/08[17] sąd ten wskazał, iż art. 105a ust. 4 uPrB wprowadził samodzielną przesłankę legalizującą przetwarzanie danych osobowych

15 Lex nr 506279

16 Od dnia 16 czerwca 2005 r. na mocy art. 3 pkt 2 ustawy z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw [Dz. U. nr 85 poz. 727], dodającego art. 105a uPrB, rozszerzony został katalog celów, dla których dopuszczalne jest przetwarzanie informacji stanowiących tajemnicę bankową:

Art. 105a. 1. Przetwarzanie przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, informacji stanowiących tajemnicę bankową w zakresie dotyczącym osób fizycznych (konsumentów) może być wykonywane, z zastrzeżeniem art. 104, 105 i 106-106c, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

2. Instytucje, o których mowa w ust. 1, mogą, z zastrzeżeniem ust. 3, przetwarzać informacje stanowiące tajemnicę bankową w zakresie dotyczącym osób fizycznych (konsumentów) po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, pod warunkiem uzyskania pisemnej zgody osoby, której informacje te dotyczą. Zgoda ta może być w każdym czasie odwołana.

3. Instytucje, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową oraz informacje, o których mowa w art. 105 ust. 4 pkt 2 w zakresie dotyczącym osób fizycznych (konsumentów) po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, jeśli spełnione są łącznie następujące warunki:

1) osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów,

2) po zaistnieniu okoliczności, o której mowa w pkt 1, upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank lub inną instytucję ustawowo upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody.

4. Przetwarzanie informacji stanowiących tajemnicę bankową w przypadkach, o których mowa w ust. 3, może być wykonywane przez okres nie dłuższy niż 5 lat od dnia wygaśnięcia zobowiązania.

Również NSA w wyroku z 14 września 2005 r., sygn. akt I OSK 39/05 (Lex nr 194722) orzekł, iż „przetwarzanie danych osobowych kredytobiorców, będących dłużnikami banku, przez biura informacji kredytowej, jest możliwe wyłącznie nie dłużej niż 5 lat od dnia wygaśnięcia zobowiązania. Ponadto przekazywanie tych danych musi być niezbędne dla udzielania kredytów i pożyczek pieniężnych."

Zmiana art. 105a ust. 4 uPrB nastąpiła z dniem 1 kwietnia 2007 r. - na mocy art. 1 pkt 13 ustawy z dnia 26 stycznia 2007 r. o zmianie ustawy - Prawo bankowe [Dz. U. Nr 42, poz. 272]:

Art. 105a 1. Przetwarzanie przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, informacji stanowiących tajemnicę bankową w zakresie dotyczącym osób fizycznych może być wykonywane, z zastrzeżeniem art. 104, art. 105 i art. 106–106c, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

(...)3. Instytucje, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank lub inną instytucję ustawowo upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody.

4. Banki oraz instytucje, o których mowa w art. 105 ust. 4, mogą przetwarzać informacje stanowiące tajemnicę bankową dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, dla celów stosowania metod statystycznych, o których mowa w art. 128 ust. 3.

5. Przetwarzanie informacji stanowiących tajemnicę bankową w przypadkach, o których mowa w ust. 3, może być wykonywane przez okres nie dłuższy niż 5 lat od dnia wygaśnięcia zobowiązania, a w przypadku, o którym mowa w ust. 4, przez okres 12 lat od dnia wygaśnięcia zobowiązania.

6. Zakres przetwarzanych informacji, o których mowa w ust. 3 i 4, może obejmować dane dotyczące osoby fizycznej lub dane dotyczące zobowiązania.

W stanie prawnym obowiązującym jeszcze przed 1 kwietnia 2007 r. WSA w Warszawie wskazywał, iż w świetle art. 105 ust. 1 i 4 uPrB *„nietrafne jest twierdzenie, że stanowi on przesłankę przetwarzania danych w formie przechowywania ich i udostępniania przez okres siedmiu lat na podstawie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Przepis ten bowiem stanowi wyłącznie podstawę do utworzenia B. SA w celu realizacji określonych w nim zadań. Nie można z niego natomiast wywieść delegacji ustawowej dla ustalenia takiego rozumienia art. 23 ust. 1 pkt 2 Ustawy o ochronie danych osobowych. Przepisami zezwalającymi na przetwarzanie danych nie są również postanowienia regulaminu zbierania i udostępniania informacji, stanowiącego załącznik do umowy. Jest to bowiem akt wewnętrzny nieposiadający przymiotu źródła prawa powszechnie obowiązującego, z uwagi na treść art. 87 ust. 1 Konstytucji RP."* (uzasadnienie wyroku z 25 sierpnia 2004 r. II SA/Wa 547/04, Lex nr 194484).

17 Lex nr 521919

dla celów stosowania metod statystycznych[18]. Ponadto zgodnie ze stanowiskiem sądu zawartym w wyroku z 10 września 2009 r. II SA/Wa 357/09[19] *„nie może mieć istotnego znaczenia fakt, że dane skarżącego zostały omyłkowo przekazane jako dłużnika „nierzetelnego" i niezwłocznie po stwierdzeniu nieprawidłowości usunięte ze zbioru danych dłużników, gdyż zakres danych przeznaczonych do przetwarzania w ten sposób został precyzyjnie określony w §3 rozporządzenia Ministra Finansów z dnia 27 marca 2007 r. w sprawie szczegółowego zakresu przetwarzanych informacji dotyczących osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów oraz trybu usuwania tych informacji".*

Podobnie do zagadnienia przetwarzania informacji stanowiących tajemnicę bankową w celach statystycznych podszedł WSA w Warszawie w wyroku z 27 stycznia 2009 r. II SA/Wa 1569/08[20]. Sąd uznał, że na gruncie wykładni gramatycznej nie jest możliwe jednoznaczne stwierdzenie, czy przepis art. 105a ust. 4 uprawnia do samodzielnego decydowania o zmianie celu przetwarzania danych – *„dlatego też niezbędne jest odwołanie się do wykładni celowościowej tego przepisu oraz uwzględnienie kontekstu normatywnego. Utworzenie instytucji, o której mowa w art. 105 ust. 4 wraz z jednoczesnym przyznaniem jej przez ustawodawcę w art. 105a ust. 4 uprawnień do przetwarzania przekazanych jej przez banki danych osobowych dla celów stosowania metod statystycznych wskazuje, że dla dokonywania przetwarzania nie jest potrzebne spełnienie przez B. żadnych dodatkowych warunków, gdyż art. 105a ust. 4 stanowi wystarczającą podstawę do dokonywania przetwarzania danych. Przyjęcie odmiennego rozwiązania prowadziłoby do sytuacji, w której B. mogłoby przetwarzać dla celów stosowania metod statystycznych, wyłącznie dane otrzymane przez banki z tym właśnie przeznaczeniem. Interpretacja taka stoi w jawnej sprzeczności z celem regulacji art. 105a ust. 4, którym jest, zdaniem Sądu, zapewnienie bankom łatwego i szybkiego dostępu do danych statystycznych niezbędnych do prawidłowego obliczania wymogów kapitałowych. Przepis ten służy zatem dobru publicznemu, jakim niewątpliwie jest optymalizacja działalności kredytowej banków."*

W ocenie sądu przyjęcie tego sposobu wykładni jest tym bardziej uzasadnione w świetle treści art. 26 uodo, który stwierdza, że przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, o ile nie narusza praw i wolności osoby, której dane dotyczą, jeżeli następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych. Zatem, zdaniem sądu, cel przeprowadzenia badań statystycznych stanowi przesłankę wyłączającą ustawowy zakaz przetwarzania danych osobowych w innym celu niż ten, dla którego zostały zebrane.

W sprawie o sygn. akt I SA/Kr 115/08[21] przedmiotem oceny WSA w Krakowie stała się natomiast legalność decyzji Dyrektora Izby Skarbowej. W uzasadnieniu tego wyroku z 20 maja 2008 r. sąd wyjaśnił, że *„organ kontroli*

18 „Zmiana ta wynikała z konieczności dostosowania polskich regulacji do przepisów wspólnotowych, w tym przede wszystkim do dyrektyw: 2006/48/WE w sprawie podejmowania i prowadzenia działalności przez instytucje kredytowe i 2006/49/WE w sprawie adekwatności kapitałowej przedsiębiorstw inwestycyjnych i instytucji kredytowych, zwanych łącznie dyrektywą CRD" - A. Tupaj-Cholewa, R. Kaszubski, *Dopuszczalność przetwarzania informacji stanowiących tajemnicę bankową dla celów statystycznych,* Przegląd Prawa Handlowego, październik 2008

19 http://orzeczenia.nsa.gov.pl

20 http://orzeczenia.nsa.gov.pl

21 Lex nr 475534

skarbowej może zwrócić się do banku o ujawnienie informacji objętych tajemnicą bankową, m.in. wskazanie osoby będącej posiadaczem karty płatniczej (debetowej bądź kredytowej) jako informację podstawową (operacyjną), jedynie w stosunku do kontrolowanego. ***Informacje dotyczące osób trzecich, nawet ściśle powiązanych ze sprawą, nie mogą być przez bank ujawnione*** *pod rygorem odpowiedzialności odszkodowawczej na podstawie art. 105 ust. 5 cyt. ustawy Prawo bankowe. Natomiast stosownie do art. 180 §1 O. p. jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. Ujawnienie przez bank posiadaczy kart płatniczych byłoby zatem sprzeczne z wyżej omówionymi przepisami o tajemnicy bankowej i nie mogłoby stanowić dowodu w postępowaniu kontrolnym ani odwoławczym".*

Omawiając orzecznictwo z zakresu przetwarzania danych osobowych stanowiących informację bankową, nie sposób pominąć wyroku NSA z 30 lipca 2009 r. wydanego w sprawie oznaczonej sygn. akt I OSK 1049/08[22], w którym sąd orzekł, iż **administrator danych osobowych nie może uzależniać wykonania obowiązku informacyjnego** określonego w art. 33 ust. 2 ustawy o ochronie danych osobowych od wniesienia przez wnioskodawcę z góry opłaty na poczet kosztów przesłania pisemnej informacji na wskazany przez wnioskodawcę adres. Sąd powołał się na treść art. 12 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[23] i wskazał, iż to państwa członkowskie reprezentowane przez organy ustawodawcze, a nie podmioty gospodarcze działające w tych państwach, wyznaczają możliwość nałożenia odpłatności, jakich administrator danych może żądać od osób ubiegających się o udostępnienie ich danych osobowych. Wyjaśnił, że ustawodawca polski świadomie nie skorzystał z możliwości ustalenia wysokości obciążeń właśnie w zakresie dostępu do danych osobowych, co mógł uczynić i co zrobił w innych aktach – *„skoro bowiem chodzi o ustawowy obowiązek, o realizację ustawowego prawa wnioskodawcy, to ograniczenie tego prawa, jego uwarunkowanie spełnieniem przez uprawnionego określonych przesłanek musi być zawarte wprost, wyraźnie w przepisach ustawowych - na podstawie ustawy."*

W wyroku z 7 listopada 2006 r. II SA/Wa 1289/06[24] WSA w Warszawie ujął kompetencje utworzonego na podstawie art. 105 ust. 4 uPrB Biura w szerszym kontekście. Z funkcji, jaką wykonuje ta instytucja (udostępniania informacji potrzebnych do wykonywania czynności bankowych), sąd wywiódł, że **celem przetwarzania przezeń danych jest nie tylko ochrona banków** (już samo to w ocenie sądu uzasadniałoby przetwarzanie danych także po zamknięciu rachunku), **lecz również ochrona innych klientów**. *„Uprawnieniem i obowiązkiem Biura jest realizacja zadań wynikających z art. 105 ust. 4 Prawa bankowego w zakresie (także czasowym) pozwalającym na efektywną, rzeczywistą i bezpieczną realizację przez banki i inne instytucje czynności bankowych i parabankowych. Jednocześnie też podstawą przetwarzania danych przez Biuro jest art. 23 ust. 1 pkt 5 ustawy. Za prawnie usprawiedliwiony cel B. SA uznać należy bowiem przetwarzanie danych klientów banków, nawet po zamknięciu ich rachunków kredytowych, skoro dane te służą do oceny zdolności kredytowej, a ocena taka jest prawem*

22 Lex nr 513728
23 Dz. Urz. UE L 95.281.31
24 Lex nr 301749

i obowiązkiem banku". Sąd nie zgodził się natomiast z twierdzeniem, że na przetwarzanie danych w sprawie zezwala art. 23 ust. 1 pkt 4 uodo – *„Usługowa wobec banków i innych instytucji* ***funkcja Biura nie pozwala jeszcze ocenić, że realizuje ono zadania dla dobra publicznego****. Bezpieczeństwo depozytów, sprawność funkcjonowania systemu bankowego i stabilność obrotu gospodarczego nie stanowią ‚dobra publicznego' w rozumieniu tego przepisu. Takie cele muszą być bowiem w sposób wyraźny, jednoznaczny określone prawem, a ponadto zalicza się do nich wyjątkowe okoliczności przetwarzania danych, które nie są objęte innymi przesłankami i które wymagają takiego przetwarzania na zasadzie ultima ratio. Przykładowo zalicza się do nich zadania z zakresu bezpieczeństwa publicznego, walki z przestępczością, opieki zdrowotnej, udzielania pomocy ofiarom klęsk żywiołowych itp."*

Podsumowanie

Orzeczenia sądów administracyjnych nie mają wprawdzie mocy powszechnie obowiązującej, jednak w praktyce (w pewnym zakresie) spełniają rolę prawotwórczą. Ważną funkcję spełnia bowiem korekta aksjologiczna norm, która może wyznaczać dość konsekwentną linię orzecznictwa sądowoadministracyjnego, uzupełniając prawo pisane[25].

Rolą sędziego, który w sprawowaniu swego urzędu jest niezawisły i podlega jedynie Konstytucji oraz ustawom[26], jest interpretacja przepisu prawnego w sposób, który ma wydobyć normę prawną odpowiadającą danemu stanowi faktycznemu[27].

Powyższy wybór tez orzeczeń precyzuje w drodze wykładni sądowej dopuszczalny model przetwarzania danych osobowych stanowiących tajemnicę bankową. Dla obrotu informacją bankową podstawowe znaczenie ma fakt, iż w świetle omawianych orzeczeń sądów administracyjnych istotne są również inne wartości[28] niż ochrona danych osobowych. W świetle przedstawionego orzecznictwa instytucja utworzona na podstawie art. 105 ust. 4 uPrB jest podmiotem o charakterze publicznym, którego funkcją jest ochrona banków (będących instytucjami zaufania publicznego) i ich depozytariuszy. Dopuszczalne jest przetwarzanie przez bank danych wszystkich osób zasadnie i w usprawiedliwionym zakresie zgromadzonych w związku z zawarciem i wykonywaniem umowy, jak też przetwarzanie przez banki danych stanowiących tajemnicę bankową w celu obracania wierzytelnościami i umożliwienia ich dochodzenia. Od 1 kwietnia 2007 r. prawnie dopuszczalne jest także przetwarzanie przedmiotowych danych w zakresie niezbędnym dla celów stosowania metod statystycznych, o których mowa w art. 128 ust. 3 uPrB, bez zgody podmiotu, którego te dane dotyczą.

25 A. Gomułowicz, *Aspekt prawotwórczy sądownictwa administracyjnego*, Wolters Kluwer Polska, Warszawa 2008, s. 91

26 Art. 178 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. [Dz. U. Nr 78 poz. 483 z późn. zm.]

27 „Nie można jednak stwierdzić, że raz dokonana interpretacja przepisu prawnego będzie zawsze adekwatna do nowych stanów faktycznych, które w dynamicznie zmieniającej się rzeczywistości muszą rozstrzygać sądy" - R. Hauser, *Wpływ orzecznictwa Naczelnego Sądu Administracyjnego na tworzenie projektów ustaw*, Przegląd Legislacyjny, Warszawa 2006 r., Nr 1 (53), s. 86

28 „Orzecznictwo sądu administracyjnego nie jest bowiem ograniczone wyłącznie do ujawniania błędów, niedopatrzeń, uchybień i ułomności w stosowaniu prawa przez poddane kontroli organy administracji publicznej, chociaż jest to ważna jego funkcja, lecz do kształtowania takich wartości systemu prawa, którym ma być podporządkowana działalność administracji publicznej w celu zagwarantowania skutecznej ochrony prawnego interesu jednostkowego oraz interesu publicznego w granicach przedmiotowego porządku prawnego." – B. Adamiak, J. Borkowski, *Metodyka pracy sędziego w sprawach administracyjnych,* Oficyna, Warszawa 2009, s. 89

Abstract

Processing of personal data concerning bank secrecy in case law of administrative courts

The article examines the review of the Polish administrative courts' judgments concerning the issues of banking law as well as data protection law.

The introductory part deals with the concept of the processing of personal data and the bank secrecy. It also indicates on the legal basis and the role of Credit Information Bureau (BIK SA) as an authorized organization established to process and share bank data.

Subsequently, the author analyses the cases in which the courts presented their views on the conditions under which processing of bank data is legitimate.

As a conclusion, the administrative judiciary's legislative is considered.

Beata Bińkowska-Artowicz jest doktorantką Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz asystentem sędziego w Wojewódzkim Sądzie Administracyjnym w Warszawie.

SPSS predictive SOLUTIONS

KORELACJE
KONFERENCJA SPSS POLSKA

KORELACJE 2010 za nami!

Piąta Konferencja SPSS Polska, KORELACJE 2010, za nami. W dniach 22-24 września w Krakowie po raz kolejny spotkali się pasjonaci i eksperci wykorzystania analizy danych. Impreza zgromadziła blisko stu uczestników reprezentujących szeroki wachlarz firm, instytucji administracji publicznej i uczelni.

Tematem przewodnim, którym prezes SPSS Polska, Piotr Komornicki, otworzył konferencję w swoim wystąpieniu, były analizy predykcyjne. Zagadnienie to kontynuował gość specjalny, prof. dr hab. Jarosław Górniak z Uniwersytetu Jagiellońskiego, który przewrotnie postawił pytanie „Czy przewidywanie przyszłości ma przyszłość?"

Największą wartością KORELACJI, podnoszoną przez samych uczestników, jest możliwość skorzystania z doświadczeń innych. Zdecydowana większość prezentacji mówiła właśnie o zrealizowanych projektach i wdrożeniach. Szczególnie licznie na tegorocznych KORELACJACH reprezentowane były instytucje administracji publicznej. Wystąpienie Michała Filipowicza z Opolskiego Obserwatorium Rynku Pracy pokazywało, na ile możliwe jest realizowanie efektywnych projektów aktywizacyjnych na rynku pracy. Następnie Ewa Wildner zaprezentowała zmianę, jaka dokonuje się w administracji publicznej na przykładzie realizacji badań przez Ministerstwo Pracy i Polityki Społecznej w zakresie realizacji badań.

Konferencja obfitowała też w prezentacje z innych obszarów biznesowych, jak również nie mogło na niej zabraknąć informacji na temat najnowszych wersji oprogramowania IBM SPSS, w tym IBM SPSS Statistics 19 oraz aktualności na temat platformy badawczej IBM Data Collection w wersji 6.

Na KORELACJACH stawiamy na relacje, które w toku prezentacji i dyskusji tworzyły się w iście geometrycznym postępie. Atrakcją Konferencji był wieczór w Klubie Barka, niezwykle klimatycznym lokalu znajdującym się na prawdziwej 120-letniej barce.

Pełna relacja z konferencji na stronie organizatora — www.spss.pl.

Długofalowe bezpieczeństwo podpisu osobistego

Przemysław Kubiak

Trudno jest przewidzieć postęp w kryptoanalizie w długim przedziale czasowym (10 lat i więcej). Rekomendacje krótkookresowe wzbudzają większe zaufanie, ponieważ do złamania algorytmu kryptograficznego dochodzi najczęściej stopniowo, w kilku rozłożonych w czasie krokach (por. rozdz. 7.3 raportu [1]). Aby zatem zwiększyć zaufanie do systemu, który wydawać będzie użytkownikom klucze na dziesięć lat (taki jest okres ważności dowodu osobistego) i który wdrożony będzie na skalę państwa, proponuje się zastosować dodatkowe środki ochrony. Proponowane środki mają charakter organizacyjny - w tym wybór architektury systemu (por. opracowanie [2]) oraz kryptograficzny (por. rozdz. 7 raportu [3] oraz pracę [4]).

Podpis wewnętrzny

Naturalnym podejściem wzmacniającym system jest zastosowanie dwóch niezależnych schematów podpisów elektronicznych (por. rozdz. 7.3 raportu [1]). Zwykle niesie to za sobą zwiększenie długości wynikowego, podwójnego podpisu, jednak tak być nie musi. Proces składania podpisu rozpoczyna się od obliczenia wartości funkcji skrótu na podpisywanej wiadomości, czyli od obliczenia tzw. odcisku palca wiadomości. Później dopiero ów skrót/odcisk palca, a nie wiadomość, jest poddawany przekształceniom narzuconym przez algorytm podpisu. Jest tak, ponieważ najczęściej wiadomości są za długie, by je bezpośrednio podpisywać. Wartości popularnych funkcji skrótu mieszczą się w przedziale 160-512 bitów. Rekomendowane aktualnie długości to 224, 256, 384, 512 bitów.

Przyjrzyjmy się teraz algorytmowi RSA. Jest on publicznie znany od 1978 roku i mimo zwiększania się długości przełamywalnych kluczy (por. niedawny atak [5], wykonany z wykorzystaniem komputerów ogólnego przeznaczenia, a nie wyspecjalizowanych maszyn, jak projekty TWINKLE czy TWIRL) oraz mimo sukcesów w kryptoanalizie szczególnych przypadków, jak np. ataki na krótki wykładnik tajny, sam algorytm w ogólnej postaci nie został złamany. RSA obok ECDSA cieszy się zatem największą popularnością.

Gdyby algorytm podpisu RSA stosować bezpośrednio do skrótu wiadomości, mielibyśmy do czynienia z niepożądaną w przypadku podpisów własnością homomorfizmu: iloczyn dwóch podpisów wykonanych tym samym kluczem tajnym na skrótach dwóch wiadomości byłby równy podpisowi iloczynu tychże skrótów. Własność ta osłabia algorytm podpisu, dlatego do wartości skrótu stosuje się dodatkowo kodowanie (ang. *padding*), które złamie homomorfizm. Bardzo dobrą opinię ma kodowanie EMSA-PSS znane ze standardu [6]. Kodowanie to wykorzystuje tzw. salt. Salt to wartość niezależna od wiadomości i zgodnie z [6] może być to wartość losowa, ale może być to także wartość stała. Wymogiem standardu jest by (w uproszczeniu) suma długości salt oraz długości wartości funkcji skrótu była nie większa niż długość modułu RSA pomniejszona o 2 bajty. Zatem nawet dla modułów RSA 1024 bitowych (od których się dziś odchodzi - por. [5]) dla 256 bitowego skrótu zostaje w kodowaniu EMSA-PSS wystarczająco dużo miejsca na salt ponad 700 bitowy. Co więcej, salt jest odzyskiwany z podpisu RSA na etapie weryfikacji podpisu. Salt może więc

z powodzeniem przenosić np. podpis ECDSA pod tą sama wiadomością, co podpis RSA. Mamy zatem podpis RSA i zagnieżdżony w nim, wewnętrzny podpis wykonany innym algorytmem. Ponieważ dla RSA trzymaliśmy się standardu, stare oprogramowanie, nieświadome tego, że w salt przenoszony jest drugi podpis, poprawnie zweryfikuje poprawny podpis RSA, zaniecha jedynie weryfikacji podpisu przenoszonego w salt. Mamy zatem wsteczną kompatybilność.

Determinizm

Algorytm RSA jest także korzystny z innego względu - pomijając sposób kodowania (w którym może być np. losowy salt), jest to algorytm w pełni deterministyczny. Wykładnik tajny jest ustalony i generowanie podpisu polega właśnie na wykonaniu potęgowania modularnego z wykorzystaniem wykładnika tajnego. Jeśli podczas generowania podpisu algorytm musiałby wytwarzać dane losowe, tak jak to robi np. ECDSA, to otwiera się furtka dla ataków kleptograficznych [7]. Ataki te polegają na złośliwej implementacji algorytmu przez wytwórcę sprzętu w taki sposób, że w podpisie, dzięki odpowiedniemu doborowi danych losowych, wyciekają bity klucza tajnego. Co więcej, wyciekające dane mogą być zaszyfrowane kluczem asymetrycznym, ustalonym przez wspomnianego złośliwego wytwórcę sprzętu i pozostaną czytelne tylko dla niego, nawet po poznaniu klucza szyfrowania przez strony trzecie. Z uwagi na skalę integracji układów elektronicznych wykrycie ataku kleptograficznego jest bardzo trudne. Z tego względu proponujemy [3, 4] wykorzystanie algorytm BLS [8] do generowania podpisu wewnętrznego. BLS to deterministyczny schemat podpisów oparty o krzywe eliptyczne.

W rezultacie uzyskujemy w pełni deterministyczne kodowanie EMSA-PSS, w którym jednak salt ma wartość nieprzewidywalną dla stron nieznających klucza tajnego schematu BLS (zauważmy, że umiejętność przewidywania wartości podpisu bez posiadania klucza tajnego jest równoważna umiejętności fałszowania podpisu). Jest to na pewno stan nie gorszy niż kodowanie EMSA-PSS z salt będącym wartością stałą, a jak wspomniano powyżej, ten ostatni przypadek jest także dopuszczany w standardzie [6].

Podpis zewnętrzny i czas złożenia podpisu

Aby dane określające czas złożenia podpisu były wiarygodne dla odbiorcy oraz aby były zintegrowane ze złożonym przez obywatela podpisem, powinny razem z owym podpisem zostać podpisane. Podpis powinien być wygenerowany przez serwer dołączający wspomniane dane do podpisu osobistego. Mamy zatem trzeci podpis (możemy go nazwać podpisem zewnętrznym), który może wykorzystywać zupełnie inny algorytm niż wymienione do tej pory.

Daną pozwalającą na określenie czasu złożenia podpisu może być po prostu wartość czasu, ale znacznie lepiej, jeśli wykorzystamy tutaj dodatkowo tzw. łańcuch hashy, czyli oprócz wartości czasu dołączymy do podpisu wartość skrótu (hasha) z ostatnio przetwarzanych przez serwer danych, tzn. z poprzednio znakowanego na serwerze podpisu osobistego, dołączonych doń danych oraz podpisu serwera.

Czyli w danych przekazywanych obywatelom wartości hashy stanowią ślad pozwalający na odtworzenie kolejności znakowania czasem podpisów - i to bez względu na wpisywane przez serwer znakujący wartości czasu. W ten sposób serwer znakujący czasem ma bardzo ograniczone możliwości dokonywania fałszerstw, tj. znakowania nowych podpisów czasem przeszłym: jeśli czas ten ma być wcześniejszy niż czas naniesiony na ostatnio wydany podpis, to ów nowy podpis nie może być dopisany na końcu istniejącego łańcucha, ale musi być „wciśnięty'' gdzieś w środek. Jednak wstawienie nowego rekordu w środek łańcucha spowoduje

zmianę rekordu po nim następującego (bo zawiera on wartość funkcji skrótu ze swojego poprzednika) i także rekordu następującego po tym następniku itd. Czyli od miejsca wstawienia nowego rekordu zmieniony zostaje cały łańcuch hashy i dane przechowywane na serwerze znakującym stają się niespójne z danymi wydanymi obywatelom. Wystarczy zatem, by łańcuch przechowywany na serwerze podlegał okresowej kontroli przez jednostkę/jednostki zewnętrzne. Kontrolerzy mogliby sprawdzać integralność łańcucha i zgodność posiadanych przez siebie danych (jako obywatele wysyłaliby przecież wcześniej pewne podpisy do oznakowania czasem) z odpowiadającymi im rekordami w łańcuchu hashy. Takich możliwości kontroli (czyli wykrywania fałszerstw) nie daje zwykłe znakowanie czasem.

Zauważmy, że w przypadku podpisu osobistego długość łańcucha hashy nie będzie rosła bardzo dynamicznie, np. liczba 300 mln nowych rekordów rocznie (jest to liczba przykładowa, przytoczona na potrzeby niniejszego artykułu, zdaniem autora jest ona zawyżona) nie wydaje się dużym obciążeniem dla systemu.

Poza polepszeniem mechanizmów kontroli łańcuchy hashy mają jeszcze jedną przewagę nad zwykłym znakowaniem czasem znanym z podpisów kwalifikowanych. Zacytujmy art. 7 ust. 3 ustawy z 18 września 2001 r. o podpisie elektronicznym: „Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę''. Aby zatem zwykły znacznik czasu na długo przechowywanym dokumencie elektronicznym nadal był wiarygodny, należy go „konserwować'' nowym podpisem po wygaśnięciu ważności certyfikatu, który był używany dla poprzedniego podpisu pod znacznikiem czasu. Pociągałoby to za sobą koszty co najmniej organizacyjne i obliczeniowe wobec rosnącej liczby e--dokumentów w rejestrach państwowych. Z łańcuchami hashy jest inaczej: z przechowywanym dokumentem stowarzyszone są dane, które są także w łańcuchu hashy - i to ich obecność w odpowiednim miejscu łańcucha potwierdza fakt istnienia dokumentu w odpowiednim czasie:

- omawiane dane są związane z dokumentem, zawierają jego skrót!
- dodanie tych danych z datą wsteczną do łańcucha powodowałoby zmianę całego łańcucha od miejsca dodania, łącznie z głową łańcucha, tj. jego najświeższym rekordem!

Te mechanizmy bezpieczeństwa bazują na trudności znajdowania drugiego przeciwobrazu wartości funkcji skrótu (second preimage resistance) - własności znacznie trudniejszej do przełamania niż odporność funkcji skrótu na znajdowanie kolizji. Wystarczy teraz, że certyfikat klucza podpisu serwera znakującego czasem będzie ważny dla najświeższych rekordów w łańcuchu, by zabezpieczyć wszystkie rekordy wcześniejsze - nie trzeba zatem „konserwować'' znaczników pod starymi dokumentami przechowywanymi w rejestrach. Widać, że bezpieczeństwo klucza podpisów do znakowania czasem jest tutaj bardzo ważne - powinno mieć to wpływ na wybór algorytmu, długość klucza i częstotliwość zmian tego klucza.

Architektura systemu - mediator

Idea podpisów z mediatorem pojawiła się w pracy [9]. Rozwiązanie to polega na podzieleniu klucza tajnego pomiędzy dwie niezależne jednostki: użytkownika (czyli jego kartę elektroniczną) i centralny serwer zwany mediatorem. Klucz publiczny pozostaje

bez zmian. Konsekwencją tego podziału jest niemożność złożenia podpisu samodzielnie przez każdą ze stron protokołu. Składanie przez użytkownika podpisu pod dokumentem jest teraz dwuetapowe: użytkownik wykorzystuje swój składnik klucza tajnego i generuje tzw. pre-podpis. Pre-podpis jest przesyłany do mediatora, gdzie jest finalizowany do pełnego podpisu przy użyciu przez mediatora jego składnika klucza tajnego. Po finalizacji mediator weryfikuje wynikowy podpis.

Rozwiązanie to pozwala na szybkie blokowanie możliwości generowania podpisów w sytuacji, gdy użytkownik traci do tego uprawnienia lub gdy traci kontrolę nad swoja karta elektroniczną - mediator przed finalizacją sprawdza status klucza danego użytkownika i jeśli klucz jest unieważniony lub czasowo zablokowany (np. codziennie od 15:00 do 7:00), nie finalizuje podpisu. Efektem ubocznym takiej procedury jest brak konieczności sprawdzania list CRL lub wykonywania protokołu OCSP przy późniejszych weryfikacjach sfinalizowanego podpisu - ważność klucza użytkownika w momencie składania podpisu została już sprawdzona przez mediatora. Upraszcza to więc proces odbioru przez jednostkę administracji opatrzonego podpisem osobistym e-dokumentu.

W przypadku schematu RSA gdyby któraś ze stron protokołu znała rozkład modułu RSA na czynniki, wówczas samodzielnie mogłaby wygenerować wykładnik tajny i samodzielnie mogłaby składać podpisy. Klucz RSA musi być więc wygenerowany przez zaufaną stronę trzecią (specjalny dedykowany serwer MSWiA) lub wygenerowany w sposób rozproszony (por. np. prace [10], [11]).

Zauważmy, że stosując mediatora w podpisie osobistym opartym o RSA, możemy klucz tajny do podpisu wewnętrznego (BLS) generować z udziałem karty lub całkowicie przez kartę. Takie rozwiązanie zapewnia, że MSWiA nie zna całego prywatnego materiału kryptograficznego karty. Mediator po finalizacji podpisu RSA weryfikuje oczywiście także podpis wewnętrzny.

Rozwiązanie z mediatorem pozwala znacząco wzmocnić system: karta obywatela i serwer centralny, jakim jest mediator, mogą współdzielić pewien dodatkowy sekret (inny dla każdej karty), który po złożeniu kolejnego podpisu zgodnie ewoluuje po każdej ze stron protokołu. W przypadku sklonowania karty i wykonania pre-podpisu przez klon, mediator zrobi o jeden krok ewolucji sekretu więcej, niż zrobiła do tej pory oryginalna karta. Przy pierwszej próbie podpisu przez oryginalną kartę niezgodność stanów sekretu wyjdzie na jaw.

Poza potencjalną możliwością wykrywania sklonowania kart mediator umożliwia zmuszenie użytkownika do rezygnacji ze słabej funkcji skrótu. Dowód osobisty ma być wydawany na 10 lat - i w tym czasie mogą zostać odkryte słabe strony funkcji skrótu (por. historie kryptoanalizy funkcji MD5, SHA-1 oraz atak [12]). Aby wymusić zmianę słabej funkcji skrótu, mediator może odmówić finalizacji podpisu w przypadku jej użycia. Jeśli funkcja wskazana jest w certyfikacie, użytkownik może teraz złożyć wniosek o wydanie certyfikatu z nową funkcją skrótu, ale z tymi samymi kluczami podpisu. Nowy certyfikat oraz (ewentualnie) aplet z implementacją nowej funkcji skrótu zostanie umieszczony na karcie. W ten sposób można wymienić komponent systemu bez kosztownej wymiany dowodów osobistych.

Źródła:

1. European Network of Excellence in Cryptology II: Yearly Report on Algorithms and Keysizes (2009-2010), 30 March 2010
2. Mirosław Kutyłowski, Anna Lauks: Podpis urzędowy (administracyjny) - koncepcja technologiczna z wykorzystaniem

podpisów z mediatorem, 28 listopada 2008, dokument przeznaczony do wykorzystania przez MSWiA
3. Elżbieta Andrukiewicz, Sławomir Cieśliński, Dariusz Lewicki, Mateusz Maniszewski, Maciej Nikodem, Przemysław Kubiak, Michał Tabor: Analiza aspektów bezpieczeństwa z zakresu mikroprocesorowych dokumentów tożsamości, 2 lipca 2009, Izba Rzeczoznawców PTI
4. Przemysław Błaśkiewicz, Przemysław Kubiak, Mirosław Kutyłowski: Digital Signatures for e-Government - a Long-Term Security Architecture, praca przyjęta na konferencję e-Forensic 2010, Shanghai, 12-13 listopada 2010
5. Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thome, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, Paul Zimmermann: Factorization of a 768-bit RSA modulus, Cryptology ePrint Archive, Report 2010/006
6. PKCS#1 v2.1: RSA Cryptography Standard
7. Adam Young, Moti Yung: The Dark Side of „Black-Box" Cryptography, or: Should We Trust Capstone? CRYPTO 1996, str. 89-103
8. Dan Boneh, Ben Lynn, Hovav Shacham: Short Signatures from the Weil Pairing. J. Cryptology 17(4), str. 297-319 (2004)
9. Dan Boneh, Xuhua Ding, Gene Tsudik, Chi Ming Wong: A Method for Fast Revocation of Public Key Certificates and Security Capabilities, In proceedings of the 10th USENIX Security Symposium, str. 297-308 (2001)
10. Michael Malkin, Thomas Wu, Dan Boneh: Experimenting with Shared Generation of RSA keys, In proceedings of the Internet Society's 1999 Symposium on Network and Distributed System Security (NDSS), str. 43-56 (1999)
11. Ivan Damgard, Gert Lassoe Mikkelsen: Efficient, Robust and Constant-Round Distributed RSA Key Generation, Theory of Cryptography, LNCS, 2010, Volume 5978/2010, str. 183-200
12. Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger: Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate, CRYPTO 2009

Abstract

Long-term security of personal signatures

In the paper a set of solutions for personal signatures introduced in polish law (Ustawa o podpisie osobistym) is discussed. The main tool presented is the mediated variant of RSA signature scheme. However, to strengthen the system a few other tools are proposed: internal signatures in place of salt in the RSA-PSS padding, a clone detection mechanism, and usage of hash chains which link together the documents signed with help of the mediator. The hash chains deter the time-stamping service from time-manipulation, and considerably reduce costs when the time-stamps are to be valid for a long period (e.g. in state registries).

Dr Przemysław Kubiak jest adiunktem na Politechnice Wrocławskiej, jego zainteresowania naukowe dotyczą kryptografii z kluczem publicznym.

Pieczęć elektroniczna

Mirosław Kutyłowski

Pieczęć elektroniczna pojawiła się ostatnio w propozycjach legislacyjnych rządu oraz komisji „Przyjazne Państwo". Nie jest to jednak całkowicie nowa instytucja prawna inicjująca obrót dokumentami, lecz próba znalezienia jednolitej regulacji dla już stosowanych w praktyce rozwiązań. Wejście pieczęci elektronicznej do coraz powszechniejszego użytku jest nieuniknione, a nawet wręcz warunkuje postępy informatyzacji. Doktryna prawna może być jedynie hamulcem stosowania tych efektywnych rozwiązań.

Postępująca digitalizacja obrotu danych prowadzi w wielu obszarach do stopniowego wypierania dokumentów papierowych. W sektorach takich jak bankowość proces ten osiągnął już bardzo wysoki stopień zaawansowania – dokument papierowy już po kilkunastu minutach od wytworzenia bywa digitalizowany, a papierowa wersja bezpowrotnie niszczona. Zmiany dotykają również administracji publicznej, a w szczególności udostępniania danych z systemów informatycznych prowadzonych przez podmioty publiczne.

Podstawowym problemem praktycznym dla dokumentów elektronicznych jest ich uwierzytelnianie. Rozwiązanie polegające na opatrywaniu dokumentów podpisem elektronicznym osoby fizycznej nie zdaje egzaminu, bowiem dodany w ten sposób „komponent białkowy" do systemu informatycznego jest:

- kosztowny,
- nieefektywny (nie pozwala na odpowiedzi w czasie rzeczywistym),
- złudny pod względem możliwości kontrolowania uwierzytelnianych dokumentów.

W istocie żaden z dobrze funkcjonujących systemów elektronicznego obrotu informacjami nie posługuje się podpisem elektronicznym osób fizycznych. Najczęściej albo stosowane są mechanizmy oparte o informacje uwierzytelniające generowane automatycznie przez system będący gospodarzem danych, albo dokumenty wcale nie są uwierzytelniane. To pierwsze rozwiązanie jest powszechnie stosowane przez banki internetowe: po uwierzytelnieniu klienta dane podawane są szyfrowanym kanałem przy użyciu klucza uzgodnionego z komputerem klienta. To drugie rozwiązanie zaczęło być stosowane masowo w Niemczech w przypadku wydruków z systemów informatycznych. W szczególności tak zwany „Amtlicher Ausdruck", o których mówi paragraf 78 GBV (Verordnung zur Durchführung der Grundbuchordnung), zawierać może wydruk pieczęci zamiast samej pieczęci. Pod względem faktycznym wartość dowodowa takiej pieczęci jest zerowa, a jedyna istotna okoliczność to rozciągnięcie przepisów karnych na przypadek obróbki plików w celu wprowadzenia tam obrazu pieczęci. Przy dzisiejszym stanie technik kryptograficznych wcale jednak nie jesteśmy skazani na tego typu ułomne rozwiązania powstałe w czasach, gdy metody kryptograficzne dopiero raczkowały.

Podpisy elektroniczne i ich klęska rynkowa

Praktyka pokazuje, że technika podpisów cyfrowych została przeniesiona do systemu prawnego w możliwie najgorszy sposób, dokładniej w te obszary, gdzie jej użyteczność jest najmniejsza. Mamy bowiem do czynienia z dwoma przeciwnościami:

1. tradycyjna doktryna prawna dopuszcza stosowanie podpisów jedynie przez osoby fizyczne,
2. sens stosowania podpisów cyfrowych powstaje tam, gdzie dane przetwarzane są automatycznie przez systemy informatyczne i zachodzi potrzeba uwierzytelniania tak powstałych dokumentów elektronicznych.

To, że w tradycyjnych systemach prawnych trudno jest znaleźć wzmianki o uwierzytelnianiu dokumentów automatycznie, nie jest zaskoczeniem. W przeszłości bowiem dokumenty powstawały jedynie wskutek czynności dokonywanych ręcznie. Jednak pewne „technologiczne" metody uwierzytelniania pojawiły się już w starożytności: w Chinach doprowadziło to do powstania odrębnego pisma znakowego na potrzeby pieczęci.

Z kolei stosowanie podpisu elektronicznego przez osoby fizyczne (a nie generowanie ich przez moduły HSM) wiąże się z szeregiem bardzo istotnych problemów praktycznych. Do najważniejszych należą możliwość utraty kontroli nad urządzeniem do składania podpisu (poprzez kradzież, zagubienie itp.), a także poprzez zawodność mechanizmów kontroli dostępu (takich jak PIN). W przypadku dużych systemów przetwarzania danych (takich jak rejestry państwowe) stopień ochrony powinien być co prawda znacznie wyższy, jednak zbudowanie odpowiednich chronionych komponentów systemu nie przekracza praktycznych możliwości dzisiejszej technologii.

Pieczęć elektroniczna a podpis elektroniczny

Aby przystąpić do definiowania pieczęci elektronicznej, należy się zastanowić jakie są potencjalne obszary zastosowania tego mechanizmu i jakie wymagania funkcjonalne i niefunkcjonalne z tym się wiążą. Jest to niby zasada oczywista, jednak bywa że pojawiające się propozycje legislacyjne stosują podejście dokładnie odwrotne.

W odniesieniu do pieczęci elektronicznej sformułować możemy następujące wymagania:

1. Definicja prawna pieczęci elektronicznej powinna uporządkować sytuację terminologii związanej z informatyzacją obrotu prawnego i powstrzymać proces definiowania pieczęci elektronicznej odrębnie dla każdej ustawy.
2. Pieczęć elektroniczna ma stanowić narzędzie do uwierzytelniania dokumentów generowanych automatycznie bez bezpośredniego udziału człowieka.
3. Uwierzytelnienie, o którym mowa powyżej, ma polegać na potwierdzeniu faktu istnienia określonych danych w określonym miejscu i czasie, bądź też potwierdzaniu stanu prawnego wynikającego z innych dokumentów.

Ad 1.

W obecnej chwili pieczęć elektroniczna jest wprowadzana przez ustawodawcę niejako tylnymi drzwiami w sytuacjach, w których nie sposób jej uniknąć. Przykładami są:

1. podpisy elektroniczne umieszczane w certyfikatach, zaświadczeniach certyfikacyjnych, listach CRL w myśl ustawy o podpisie elektronicznym,
2. urzędowe poświadczenia odbioru generowane elektronicznie w myśl przepisów prawa administracyjnego.

Potrzeb jest jednak więcej. Pieczęć elektroniczna mogłaby w szczególności być podstawowym i bardzo tanim mechanizmem niezaprzeczalnego uwierzytelniania dokumentów w obrocie finansowym. Dotyczyć to mogłoby na przykład:

1. uwierzytelniania faktur elektronicznych (zarówno w obrocie online, jak i wydawanych przez automaty do sprzedaży – np. stacje benzynowe),
2. uwierzytelniania dokumentów bankowych, takich jak potwierdzenie przelewu, wyciąg konta,

3. uwierzytelniania istotnych informacji, takich jak numer konta bankowego podmiotu publikowanego na przykład w ramach BIP.

Ad 2.

W coraz większym stopniu obrót danymi odbywa się za pomocą systemów informatycznych w znacznym stopniu autonomicznych wobec człowieka. Jakkolwiek ostateczne rozstrzygnięcie spraw związanych z przetwarzaniem danych osobowych nie jest dopuszczalne bez udziału człowieka, należy zdać sobie sprawę, że zdecydowana większość operacji dokonywana będzie automatycznie. W tej sytuacji istotne jest zorganizowanie obiegu prawnego w ten sposób, by informacje przekazywane pomiędzy różnymi systemami i docierające do osoby fizycznej mogły być szybko i efektywnie zweryfikowane pod względem ich autentyczności.

Ad 3.

Bardzo istotną okolicznością w przypadku elektronicznego obrotu danych jest potwierdzenie stanu faktycznego co do tego obrotu, a więc istnienia określonych danych. Dotyczy to na przykład:
1. istnienia określonego wpisu w rejestrach publicznych i innych bazach danych,
2. faktu istnienia określonego pisma wniesionego do podmiotu publicznego,
3. zarejestrowania czynności prawnej dokonanej drogą elektroniczną.

Nie mówimy tu zatem o składaniu oświadczeń woli – te bowiem czynności prawne nie mogą być dokonywane automatycznie przez maszyny.

Warto zauważyć, że niekiedy już teraz system prawny dopuszcza elektroniczne generowanie dokumentów poświadczających stan faktyczny bez odwoływania się do podpisu elektronicznego. Dobrym przykładem są faktury elektroniczne generowane w systemach EDV (w istocie, dzisiaj systemy takie nie muszą obejmować żadnych zabezpieczeń pod kątem niezaprzeczalności i integralności, jedynym mechanizmem tego typu jest prawo organów skarbowych do natychmiastowego wglądu do przechowywanych danych).

Pieczęć elektroniczna w koncepcji projektu rządowego

Przytoczmy definicję pieczęci elektronicznej według projektu z dnia 23.03.2010 (źródło: BIP Ministerstwa Gospodarki):

„Pieczęć elektroniczna – dane w postaci elektronicznej, przyporządkowane danemu podmiotowi w taki sposób, że możliwa jest jego identyfikacja, dołączone do innych danych lub z nimi logicznie powiązane tak, że każda późniejsza zmiana tych danych jest wykrywalna."

Warto definicję tę porównać z definicją zaawansowanego podpisu elektronicznego z tego samego projektu (definicja ta jest powtórzeniem zapisu Dyrektywy UE):

„Zaawansowany podpis elektroniczny – podpis elektroniczny:
a) przyporządkowany wyłącznie podpisującemu,
b) umożliwiający identyfikację podpisującego,
c) utworzony za pomocą środków, które podpisujący może mieć pod wyłączną kontrolą,
d) powiązany z danymi, do których się odnosi w taki sposób, że każda późniejsza zmiana tych danych jest wykrywalna."

Porównanie obu definicji wskazuje, że według autorów projektu pieczęć elektroniczna jest w istocie zaawansowanym podpisem elektronicznym z pominięciem zasady

wyłącznej kontroli podmiotu nad opatrywaniem pieczęcią elektroniczną (czyli projektodawca zakłada, że niekiedy podmiot ten nie będzie sprawował wyłącznej kontroli i że jest to sytuacja prawidłowa). Analizując wskazane warunki pod kątem informatycznym, można stwierdzić, że opatrzenie pieczęcią elektroniczną może polegać na obliczeniu wartości SHA-1 dla dokumentu i nazwy podmiotu oraz dopisaniu tej wartości jako MAC (Message Authentication Code).

Rola w systemie prawnym pieczęci elektronicznej wynikać ma z następującej zasady:

„Przyjmuje się, że dokument elektroniczny nie uległ zmianie po opatrzeniu go pieczęcią elektroniczną i jest autentyczny."

Ponieważ pieczęć elektroniczna jest w istocie kodem MAC, uprawnione pod względem faktycznym jest przyjęcie, że dokument nie został zmodyfikowany od momentu utworzenia. Z drugiej strony, nie mamy **żadnych** przesłanek do stwierdzenia kto taki dokument utworzył – definicja explicite eliminuje mechanizmy to umożliwiające. Zatem w intencji autorów projektu jest stworzenie zasady stwierdzania autentyczności dokumentów w sytuacji, gdy w istocie autentyczność takich dokumentów nie jest niczym poparta.

Powody przedstawiane przez autorów tego zapisu, a w szczególności przez członków Komisji Kodyfikacyjnej Prawa Cywilnego, powołują się na konieczność odróżnienia pieczęci elektronicznej od podpisu składanego pod oświadczeniem woli. Jest to dążenie słuszne, jednak sposób realizacji jest całkowicie niedopuszczalny – nie należy wystawiać na szwank bezpieczeństwa obywateli i obrotu prawnego jedynie dla zagwarantowania odrębności dwóch instytucji prawnych.

W praktyce wprowadzenie pieczęci elektronicznej w tak opisanej postaci wprowadziłoby znakomite warunki dla nieuczciwości w obrocie prawnym. Dokumenty elektroniczne, takie jak odpisy z rejestrów, mogłyby być swobodnie fałszowane, a ich odbiorca będący podmiotem publicznym byłby **zmuszony** do ich uznawania jako autentycznych. W tym miejscu pragnęlibyśmy powstrzymać się od przedstawiania konkretnych scenariuszy, by w przypadku przyjęcia projektu przez Ustawodawcę nie zostać oskarżonym o ułatwianie działalności przestępczej. Jednak warto zaznaczyć, że znalezienie takich scenariuszy nie wymaga specjalnej inwencji.

Pieczęć elektroniczna wg Komisji „Przyjazne Państwo"

Definicja pieczęci elektronicznej według tego projektu ma następującą postać:

„Pieczęć elektroniczna - zaawansowany podpis elektroniczny oznaczony jako pieczęć elektroniczna, uwierzytelniający osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej."

Warto zwrócić uwagę na różnice w stosunku do definicji podpisu zaawansowanego. Pierwszą jest wyraźne oznaczenie pieczęci elektronicznej jako pieczęci elektronicznej. Tak więc pieczęć elektroniczna nie może być mylnie wzięta za „nie-pieczęć", nawet jak zastosowane algorytmy kryptograficzne są identyczne z tymi stosowanymi dla tradycyjnych zastosowań podpisu zaawansowanego. Druga różnica polega na wykluczeniu osób fizycznych z grona „opatrujących pieczęcią elektroniczną".

Rola pieczęci elektronicznej w obrocie prawnym wynika z następujących zasad:

„Dane w postaci elektronicznej opatrzone pieczęcią elektroniczną są równoważne dokumentom opatrzonym podpisem własnoręcznym, gdy służą poświadczeniu istnienia określonego stanu prawnego lub faktycznego, w szczególności potwierdzeniu danych ujawnionych w ewidencji lub w rejestrach publicznych. W takim przypadku uznaje się równocześnie, że pieczęć elektroniczna została złożona przez właściwy organ podpisującego."

Zauważmy, że pieczęć elektroniczna sformułowana jest jako casus specialis w stosunku do projektowanego art. 6 ust. 4:

„4. Dane w postaci elektronicznej opatrzone zaawansowanym podpisem elektronicznym wywołują skutki prawne równoważne skutkom sporządzenia dokumentów opatrzonych podpisem własnoręcznym."

Tym samym skutki prawne złożenia pieczęci elektronicznej wyrażają się jedynie w wyżej sformułowanych zasadach proponowanego ust. 6 do art. 6. Jednak jeśli powstawałyby co do tego jakiekolwiek wątpliwości, Ustawodawca mógłby zastąpić słowa „*gdy służą*" słowami „*wyłącznie gdy służą"*.

Proponowana funkcja pieczęci elektronicznej to poświadczanie określonego stanu faktycznego - na przykład wpłynięcia pisma do podmiotu publicznego – lub stanu prawnego – na przykład w odniesieniu do zawartości rejestrów publicznych. Jak wskazywaliśmy uprzednio, jest to podstawowy obszar zastosowań pieczęci elektronicznej, pozwalający na znaczą redukcję kosztów i zwiększenie pewności obrotu.

Sprawą kontrowersyjną jest, w przekonaniu niżej podpisanego, dyskryminacja osoby fizycznej pod względem możliwości opatrywania pieczęcią elektroniczną dokumentów cyfrowych. Trudno bowiem będzie na przykład rozwinąć elektroniczną wersję dostarczania przesyłek pocztowych „za poświadczeniem odbioru", nawet gdy osoba fizyczna zapewni sobie w tym celu odpowiednią infrastrukturę techniczną. Oddzielenie w tym wypadku kluczy służących do opatrywania pieczęcią od kluczy do składania oświadczeń woli służyłoby bezpieczeństwu prawnemu osoby fizycznej.

Abstract

Electronic stamp

"Electronic stamp" is one of the major innovations of two legislative proposals in Polish Parliament concerning electronic signatures. In fact, introducing electronic stamp into Polish law is not a revolution, as they already occur there under different names in special cases. Since it became evident that using cryptographic stamps for improving undeniability of electronic documents is cheap and effective, a clear legal framework for electronic stamps is necessary. We analyze the definitions and legal consequences of both proposals and indicate fundamental security flaws of one of them.

Mirosław Kutyłowski jest informatykiem, profesorem zwyczajnym na Politechnice Wrocławskiej.

Unia innowacji

Dariusz Bogucki

Wprowadzenie

Przyjmując 3 marca 2010 roku Strategię Europa 2020 (Komunikatem COM(2010) 2020 „EUROPA 2020 – Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu"), Komisja Europejska zapowiedziała uruchomienie 7 tzw. inicjatyw przewodnich, dzięki którym Europa wyjdzie z kryzysu silniejsza, a jej gospodarka będzie się mogła pochwalić wysokimi wskaźnikami zatrudnienia i wydajności oraz większą spójnością społeczną. Są to:

- **„Europejska agenda cyfrowa"** – projekt na rzecz upowszechnienia szybkiego Internetu i doprowadzenia do jednolitego rynku cyfrowego Unii Europejskiej;
- **„Unia innowacji"** – projekt na rzecz poprawy warunków ramowych i dostępu do finansowania badań i innowacji tak, by innowacyjne idee przeradzały się w nowe produkty i usługi, które z kolei przyczynią się do wzrostu gospodarczego i tworzenia nowych miejsc pracy;
- **„Młodzież w drodze"** – projekt na rzecz radykalnej poprawy wyników systemów kształcenia oraz ułatwiania młodzieży wejścia na rynek pracy;
- **„Europa efektywnie korzystająca z zasobów"** – projekt na rzecz uniezależnienia wzrostu gospodarczego od wykorzystania zasobów, przejścia na gospodarkę niskoemisyjną, większego wykorzystania odnawialnych źródeł energii, modernizacji transportu oraz propagowania efektywności energetycznej;
- **„Polityka przemysłowa w erze globalizacji"** – projekt na rzecz poprawy otoczenia biznesu, szczególnie w odniesieniu do MŚP oraz wspierania rozwoju silnej i zrównoważonej bazy przemysłowej, przygotowanej do konkurowania na rynkach światowych;
- **„Program na rzecz nowych umiejętności i zatrudnienia"** – projekt na rzecz modernizacji rynków pracy i wzmocnienia pozycji obywateli poprzez rozwój kwalifikacji przez całe życie w celu zwiększenia współczynnika aktywności zawodowej i lepszego dopasowania popytu do podaży na rynku pracy, między innymi dzięki mobilności siły roboczej;
- **„Europejski program walki z ubóstwem"** – projekt na rzecz zapewnienia spójności społecznej i terytorialnej tak, aby korzyści płynące ze wzrostu gospodarczego i zatrudnienia były szeroko dostępne, a osoby ubogie i wykluczone społecznie mogły żyć godnie i aktywnie uczestniczyć w życiu społeczeństwa.

Pierwsze trzy z programów zostały już opublikowane, w tym „Europejska Agenda Cyfrowa", o której interesująco pisał p. Włodzimierz Marciński w 3/2010 numerze „Czasu Informacji". Co ważne, jednak wszystkie z tych programów zakładają istotny udział technologii teleinformatycznych (ICT) w ich realizacji. Szczególnie ważną rolę techniki informacyjne i komunikacyjne odgrywają w ogłoszonym 6 października 2010 roku programie „Unia Innowacji" i warto się temu przyjrzeć.

„Unia innowacji" – przekształcanie pomysłów w miejsca pracy i rozwój gospodarki

Ogłaszając komunikat COM(2010) 546 „Unia Innowacji", komisarz ds. badań, innowacji i nauki Máire Geoghegan-Quinn

oraz wiceprzewodniczący Komisji Antonio Tajani, który zarazem odpowiada za przemysł i przedsiębiorczość, napisali: „*Wychodząc z kryzysu w warunkach ostrej konkurencji światowej, znaleźliśmy się w nadzwyczajnej sytuacji, jeśli chodzi o innowację. Jeżeli nie przekształcimy Europy w Unię innowacji, nasze gospodarki zaczną podupadać, a pomysły i talenty zostaną zmarnowane. Innowacje stanowią klucz do zrównoważonego wzrostu oraz sprawiedliwszego i bardziej ekologicznego społeczeństwa. Radykalna poprawa wyników Europy w zakresie innowacji to jedyny sposób na utworzenie stałych i dobrze płatnych miejsc pracy, które wytrzymają presję globalizacji.*"

Ta wypowiedź w skondensowany sposób wyjaśnia, dlaczego Komisja Europejska zdecydowała się na uruchomienie ambitnej strategii, która zakładając zwiększenie inwestycji w badania i rozwój we wszystkich krajach UE do min. 3 %PKB, pozwoliłaby do 2025 r. utworzyć 3,7 mln miejsc pracy i podwyższyć roczny PKB UE nawet o 795 mld euro. Do tego w Unii Europejskiej potrzebny będzie milion naukowców więcej niż obecnie.

Punktem wyjścia „Unii Innowacji" jest refleksja, czemu wielki potencjał UE w obszarze B+R nie przekłada się na pozycje gospodarki UE. W krajach UE działają wszak naukowcy klasy światowej, firmy o zasięgu globalnym, a UE poczyniła też wielkie postępy w tworzeniu największego rynku wewnętrznego na świecie. Tym niemniej gospodarki USA i Japonii są praktycznie poza zasięgiem UE, a Chiny i Indie w błyskawicznym tempie nadrabiają zaległości. Badania przeprowadzone na zlecenie Komisji (raport P. Zagamé *„Koszt nieinnowacyjnej Europy"*) wskazują na trzy czynniki:

- Niedoinwestowanie B+R w obszarze gospodarki opartej na wiedzy, a zwłaszcza w teleinformatyce. Warto wspomnieć, że krajami przeznaczającym największy procent środków z obszaru B+R na technologie społeczeństwa informacyjnego są Indie i Chiny.
- Niekorzystne otoczenie prowadzenia B+R, począwszy od braku dostępu do źródeł finansowania, poprzez wysokie koszty ochrony własności intelektualnej, ochrony patentowej, standaryzacji i nieefektywne procedury zamówień publicznych. Jest to poważny problem w sytuacji, gdy przedsiębiorstwa mogą wybrać do inwestowania i prowadzenia badań i prac rozwojowych wiele innych krajów stwarzających bardziej korzystne ramy dla innowatorów (jak np. USA czy ostatnio Chiny).
- Fragmentacja i rozproszenie działań prowadzące często do duplikacji działań i finansowania zwłaszcza wspólnotowych inicjatyw z obszaru badań i rozwoju i inicjatyw rozwijanych w krajach członkowskich z funduszy spójności UE (czyli tego, co nazywa się w Polsce potocznie „funduszami unijnymi").

Dlatego też Komisja Europejska uważa, że nadszedł czas na zbudowanie do roku 2020 prawdziwej Unii Innowacji. Inicjatywa ta zakłada, że działania europejskie, a także współpraca z państwami trzecimi w zakresie szeroko pojętych B+R, będą się koncentrować na takich wyzwaniach jak zmiana klimatu, bezpieczeństwo energetyczne, bezpieczeństwo żywnościowe, zdrowie i starzenie się społeczeństwa. Plan zakłada również, że sektor publiczny ma stymulować sektor prywatny oraz usuwać przeszkody, które uniemożliwiają wprowadzanie pomysłów na rynek.

Dziesięć głównych elementów planu „Unia innowacji"

Komisja w komunikacie zakłada realizację dziesięciu głównych elementów planu. Co ważne, we wszystkich tych obszarach kluczowe rolę odgrywają techniki informacyjne i komunikacyjne (ICT). Dlatego też „Unia Innowacji" jest, co Komisja wielokrotnie

podkreśla w komunikacie, programem komplementarnym do Agendy Cyfrowej, dlatego też warto przyjrzeć się im bliżej:

- **Europejskie partnerstwa innowacyjne** skoncentrują zainteresowane podmioty – europejskie, krajowe i regionalne, publiczne i prywatne – wokół dobrze określonych celów, które połączą rozwiązywanie problemów społecznych z wykorzystaniem potencjału Europy w zakresie przodowania na arenie światowej. Partnerstwa pozwolą skoordynować badania i rozwój z inwestycjami, a także stymulować popyt. Komisja deklaruje zapewnienie środków, które mają przyciągnąć inwestycje z innych źródeł publicznych i z sektora prywatnego. Zakłada się, że na bazie wniosków z realizacji Inicjatywy Ambient Assisted Living (AAL) do 2011 r. powstanie **pilotażowe partnerstwo** dotyczące aktywnej i zdrowej starości. Planuje się kolejne partnerstwa w takich dziedzinach jak energia, inteligentne miasta i inteligentna mobilność, oszczędne gospodarowanie wodą oraz zrównoważony rozwój wydajnego rolnictwa. **Wszystkie te projekty bazować będą na na możliwościach technologii informacyjno-komunikacyjnych.**
- Komisja opracowała **25 wskaźników w tabeli wyników „Unii innowacji"** oraz opracowała listę kontrolną dla dobrych systemów innowacji. Powstanie też nowy wskaźnik dotyczący udziału szybko rozwijających się innowacyjnych przedsiębiorstw w gospodarce. Ponadto Komisja będzie wspierać niezależny system rankingowy uczelni wyższych, zwłaszcza pod kątem nauczania przedmiotów ścisłych.
- **Komisja opracuje środki na rzecz lepszego dostępu do finansowania**. Zaproponuje program transgranicznego *venture capital*, we współpracy z Europejskim Bankiem Inwestycyjnym będzie pracować nad rozszerzeniem programów unijnych, np. mechanizmu finansowania opartego na podziale ryzyka.
- **Istniejące inicjatywy badawcze zostaną przyspieszone.** Komisja zaproponuje konkretne działania zmierzające do wprowadzenia do 2014 r. jednolitej europejskiej przestrzeni badawczej (nota bene jest to zapis traktatu lizbońskiego). Oznacza to większą spójność między europejską polityką w dziedzinie badań i jej krajowymi odpowiednikami, zmniejszenie biurokracji i usunięcie przeszkód dla mobilności naukowców, np. braku możliwości przenoszenia uprawnień emerytalnych. Oznacza to również upowszechnienie otwartego dostępu do wyników badań finansowanych ze środków publicznych. Ósmy program ramowy będzie ściśle powiązany ze strategią „Europa 2020".
- W 2011 r. Komisja ustanowi europejską radę ds. wzornictwa oraz markę „wybitne wzornictwo europejskie".
- W 2011 r. Komisja rozpocznie **ważny program badawczy dotyczący sektora publicznego i innowacji społecznych** oraz wprowadzi pilotażową europejską tabelę wyników w zakresie innowacji w sektorze publicznym. Szczególną role w tym projekcie mają odgrywać techniki informacyjne i komunikacyjne. Ponadto Komisja uruchomi europejski pilotażowy projekt innowacji społecznych, a także zaproponowała, aby innowacje społeczne stanowiły punkt odniesienia programów Europejskiego Funduszu Społecznego.
- Komisja proponuje, aby rządy przeznaczyły specjalne budżety na **zamówienia publiczne na innowacyjne produkty i usługi, zwłaszcza w administracji publicznej**. Powinno to stworzyć rynek zamówień o wartości co najmniej 10 mld euro rocznie na innowacje, które poprawią jakość usług publicznych. Komisja deklaruje swoje wsparcie w przeprowadzeniu wspólnych tego typu zamówień przez podmioty z różnych państw członkowskich.
- Na początku 2011 r. Komisja przedłoży **wniosek legislacyjny w celu przyspieszenia i unowocześnienia procesu ustanawiania norm.**

- **Nastąpi unowocześnienie przepisów dotyczących własności intelektualnej w Europie.** Wprowadzenie patentu unijnego pozwoliłoby przedsiębiorstwom zaoszczędzić 250 mln euro rocznie. Co prawda pierwsza przymiarka do wprowadzenia jednolitego patentu unijnego zakończyła się niepowodzeniem, ale Komisja i prezydencja belgijska zamierzają wrócić do tematu w grudniu, zwłaszcza że Hiszpania deklaruje rewizję swojego stanowiska w sprawie języku patentu europejskiego.
- **Nastąpi przegląd ram finansowania strukturalnego i przyznawania pomocy państwa**. Komisja zaproponuje ramy dla funduszy strukturalnych po 2013 r., w których większy nacisk zostanie położony na innowacje.

Wnioski dla Polski

Z powyższego opisu widać, że Komisja konsekwentnie (podobnie zresztą jak to było w Agendzie Cyfrowej) planuje skoordynowanie działań zarówno na szczeblu UE, jak i krajów członkowskich. Komisja oczekuje, że wszystkie kraje członkowskie sporządzą strategie operacyjne dotyczące Planu, których realizacja będzie regularnie wspólnie oceniana przez wszystkie kraje. Co to oznacza w praktyce?

Przede wszystkim Komisja deklaruje, że ramy dofinansowania UE zmienią się i to nie tylko w zakresie środków przeznaczanych dotąd na programy z obszaru badań i rozwoju, ale i polityki spójności, czyli jak się potocznie mówi funduszy strukturalnych. Innymi słowy: nie każdy projekt finansowany dziś spełni warunki w przyszłości. Nowe ramy finansowania będą nie tylko precyzyjniejsze, ale i bardziej kompleksowe. Z jednej strony oznacza to, że nowa perspektywa finansowa rysuje się jako zdecydowanie trudniejsza w realizacji, ale wsparcie zastosowań ICT w różnych inicjatywach wspólnotowych otwiera nowe możliwości także przed polską branżą IT.

Dr inż. Dariusz Bogucki - Dyrektor ds. Sektora Publicznego, EFICOM SA.

Polecamy

WARSZTATY
BIZNESOWE I PRAWNE ASPEKTY UMÓW NA USŁUGI (SYSTEMY) IT

Dlaczego warto wziąć udział w warsztatach?
- Dowiedzą się Państwo, gdzie tkwią podstawowe zagrożenia biznesowe i prawne związane z wdrożeniem i eksploatacją systemów IT oraz poznają Państwo sposoby ich unikania.
- Wymienią Państwo doświadczenia z innymi osobami z branży.
- Będą mogli Państwo uczestniczyć w dyskusji i zadawać pytania wybitnym ekspertom.
- Uzyskają Państwo w ciągu jednego, efektywnie wykorzystanego dnia praktyczną wiedzę, bardzo przydatną w codziennej pracy zawodowej.

Warsztaty poprowadzą:
- mec. Xawery Konarski (Kancelaria Prawna Traple Konarski Podrecki),
- Bohdan Garstecki (Maxus Net Communications).

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Wnioski z przeglądu projektów realizowanych w ramach VII POiG

Michał Tabor

Niniejszy artykuł stanowi syntezę przeglądu projektów realizowanych w ramach VII POiG. W ramach środków UE jest realizowanych bardzo wiele projektów, których wspólnym mianownikiem jest dostarczenie szerokiego spektrum usług internetowych dla obywatela, przedsiębiorcy, jak i samej administracji. Należy jednak zwrócić szczególną uwagę na te projekty, które mają charakter ogólnopolski, a zapewnienie interoperacyjności może stanowić jeden z głównych współczynników sukcesu tych projektów.

Interoperacyjność

W Polsce mamy dla usług administracji publicznej dwa odniesienia do interoperacyjności, są nimi: Europejskie Ramy Interoperacyjności v. 2.0 (EIF2) oraz Ustawa o informatyzacji podmiotów publicznych. Ustawa o informatyzacji stanowi podstawę formalną, która nakłada obowiązki związane z interoperacyjnością na podmioty publiczne. EIF2 nie stanowi prawa, a jedynie zbiór zaleceń i dobrych praktyk, jednak mimo braku podstawy prawnej wydaje się być najlepszym punktem odniesienia dla usług administracji publicznej. Do niedawna funkcjonował w administracji rządowej jeszcze jeden dokument - Krajowe Ramy Interoperacyjności, które przestały być aktualne i ze względu na zmiany prawne oraz opublikowanie EIF2 nie wzięto ich pod uwagę w niniejszym artykule. Ponadto spodziewana jest nowelizacja Krajowych Ram Interoperacyjności, które zostaną opublikowane jako rozporządzenie Rady Ministrów.

Definicja Interoperacyjności

Niniejsza definicja ma źródło w Ustawie o informatyzacji:

Interoperacyjność – zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.

Europejskie Ramy Interoperacyjności określają interoperacyjność w następujący sposób:

Interoperacyjność, w kontekście świadczenia Europejskich Usług Publicznych, jest to możliwość różnorodnych i różnych organizacji do współpracy na rzecz osiągania wzajemnych korzyści i uzgodnionych wspólnych celów, za pomocą wymiany informacji i wiedzy między tymi organizacjami, obsługę procesów biznesowych, za pośrednictwem wymiany danych przez ich systemy teleinformatyczne.

W tym miejscu warto przytoczyć, jakie cele niesie za sobą interoperacyjność. Analizowanie mechanizmów interoperacyjności ma sens jedynie w sytuacji, gdy ponoszenie nakładów związanych z budową rozwiązań interoperacyjnych przyniesie wymierne korzyści.

- Celem nadrzędnym działań jest dostarczenie funkcjonalnych usług publicznych, w tym celu konieczna jest **współpraca** między organami administracji publicznej mających na celu ustanowienie tych usług.

- Wymogi prawne i zobowiązania polityczne zobowiązują administrację do zapewnienia obywatelowi i przedsiębiorcy narzędzi umożliwiających wypełnianie zobowiązań wynikających z prawa, ale także uzyskiwanie praw – aby temu podołać konieczna jest **wymiana informacji** między organami administracji publicznej w celu wypełnienia tych wymogów.
- Zmniejszenie obciążeń administracyjnych dla obywateli i przedsiębiorstw stanowi o nowoczesnym społeczeństwie, ale także służy rozwojowi gospodarczemu, aby to osiągnąć konieczne jest zapewnienie **udostępniania i wielokrotnego wykorzystywania informacji** przez organy administracji publicznej, w szczególności tej, którą sama jest w stanie łatwo pozyskać.
- **Poprawa usług publicznych** dla obywateli i przedsiębiorstw poprzez ustanowienie świadczenia usług publicznych w jednym miejscu (bez konieczności korzystania z wielu serwisów dla załatwienia pojedynczej sprawy).
- **Zmniejszenie kosztów** administracji publicznej, przedsiębiorstw i obywateli poprzez wydajne i efektywne świadczenie usług publicznych.

Pryncypia interoperacyjności

Interoperacyjność w rozumieniu Europejskich Ram Interoperacyjności obejmuje obszar znacznie szerszy niż możliwość współpracy dwóch systemów teleinformatycznych. Aby osiągnąć oczekiwaną interoperacyjność, organizacje powinny być nastawione na użytkownika, zapewniać dostępność, integrację, bezpieczeństwo, prywatność i przejrzystość, a także zapewniać uproszczenie procedur administracyjnych.

Nastawienie na użytkownika

Usługi publiczne powinny być realizowane tak, aby służyć obywatelom i przedsiębiorcom. To potrzeby użytkowników powinny ustalać, jakie usługi publiczne są udostępnione i w jaki sposób są realizowane.

Zakłada się, że obywatele oczekują realizacji usług w następujący sposób:

- przyjazny dla użytkownika dostęp do usług w bezpieczny i elastyczny sposób umożliwiający personalizację i zapewniający prywatność,
- zapewnienie, że dane przekazywane do administracji są tylko raz,
- zapewnienie jednego punktu kontaktowego, nawet jeżeli współpraca wielu podmiotów publicznych jest konieczna dla świadczenia danej usługi,
- zróżnicowany dostęp umożliwiający dostęp do usług niezależnie od medium, czasu i miejsca.

Integracja i dostępność

Korzystanie z technologii IT powinno tworzyć równe szanse dla wszystkich obywateli i przedsiębiorstw dzięki otwartym i ogólnodostępnym usługom. Celem integracji jest korzystanie z wszystkich szans, jakie dają nowe technologie, aby przezwyciężyć społeczne i ekonomiczne wady i wykluczenia. Celem dostępności jest zapewnienie osobom niepełnosprawnym i w podeszłym wieku dostępu do usług publicznych tak, aby mogli korzystać z tego samego poziomu obsługi jak inni obywatele. Integracja i dostępność muszą być brane pod uwagę w toku całego cyklu życia Europejskich Usług Publicznych odnośnie projektu, zawartości informacyjnej oraz dostarczenia tych usług. Integracja i dostępność zazwyczaj udostępniana jest przez wiele kanałów. Tradycyjne kanały dostarczania usług muszą koegzystować z nowymi kanałami, tworzonymi z wykorzystaniem nowych technologii tak, aby dać obywatelom możliwość wyboru. Integracja i dostępność może być również wzmocniona przez umożliwienie obywatelom, którzy nie mogą stale lub tymczasowo bezpośrednio korzystać z usług publicznych, aby w ich imieniu działały strony trzecie.

Bezpieczeństwo i prywatność

Obywatele i przedsiębiorstwa muszą być pewni, że kontaktują się z administracją publiczną w zaufanym środowisku oraz w pełnej zgodności z odpowiednimi regulacjami, np. ochroną prywatności i bezpieczeństwem informacji. Oznacza to, że administracja publiczna musi gwarantować,

że prywatność obywateli oraz poufność informacji zapewniana przedsiębiorstwom jest przestrzegana. Z dokładnością do ograniczeń bezpieczeństwa obywatele oraz przedsiębiorstwa powinni mieć prawo do weryfikacji informacji, które pozyskała administracja na ich temat i decydować, czy ta informacja może być wykorzystana w celach innych niż te, dla których informacje zostały pierwotnie pozyskane.

Uproszczenie procedur administracyjnych

Przedsiębiorstwa opracowują znaczne ilości informacji, często jedynie z racji zobowiązań prawnych, z których nie ma żadnych bezpośrednich zysków, ani nie są one niezbędne do osiągnięcia celów prawa, na podstawie którego wprowadzono te wymagania. To tworzy znaczące obciążenia administracyjne, które mogą być wyrażone jako koszt ponoszony przez przedsiębiorstwa.

Jest także powszechnie uznane, że istnieje wysoki stopnień nadmiaru informacji, jaki obywatele muszą dostarczyć administracji publicznej. Powtarzane żądania tej samej informacji przez administrację w różnych aspektach realizacji usług publicznych powodują narastanie obciążeń administracyjnych nakładanych na obywateli, którzy tracą czas na wielokrotne wypełnianie formularzy przekazanymi wcześniej informacjami.

Przy ustanawianiu Europejskich Usług Publicznych eliminacja żądań o zbędne informacje lub nadmiarowe informacje może wymuszać reorganizację i przeprojektowanie wysiłków w zasobach administracji.

Przejrzystość

Obywatele i przedsiębiorstwa powinni mieć możliwość zrozumienia procesów administracyjnych. Powinni mieć prawo, by śledzić procedury administracyjne, które ich dotyczą oraz mieć wgląd w uzasadnienia stojące za decyzjami na nich wpływającymi. Przejrzystość pozwala również obywatelom i przedsiębiorstwom na wyrażanie swoich opinii na temat jakości świadczonych usług oraz w efekcie na wnoszenie wkładu w ulepszenie usług i tworzenie nowych usług administracji publicznej.

Zabezpieczenie informacji

Archiwa i informacje w formie elektronicznej przechowywane przez administrację w celu dokumentowania procedur i decyzji muszą być zabezpieczone. Celem jest pewność, że archiwa i inne formy informacji zachowują swoją czytelność, wiarygodność i integralność w czasie i są dostępne przy zachowaniu bezpieczeństwa i poufności.

Aby zagwarantować długoterminowe zabezpieczenie elektronicznych archiwów i innych typów informacji, formaty powinny być wyselekcjonowane tak, żeby zapewnić długoterminową dostępność, włączając w to zabezpieczenie dołączonych podpisów elektronicznych i innych elektronicznych certyfikatów , w zgodzie z wymaganiami.

Poziomy interoperacyjności

Europejskie Ramy Interoperacyjności definiują poziomy interoperacyjności:

- Poziom prawny
  - ♦ Zapewnienie zgodności z wymaganiami prawa tworzonych rozwiązań.
  - ♦ W przypadku wymiany informacji z administracją publiczną w innych krajach zapewnienie, że wymiana informacji będzie się odbywała z poszanowaniem prawa tych krajów.
- Poziom organizacyjny
  - ♦ Zapewnienie, że procesy związane z projektami, jak i późniejsze procesy biznesowe, będą zapewniały osiągnięcie przyjętych i uzgodnionych celów w kontekście wszystkich organizacji biorących udział w projekcie.

- ♦ Dostosowanie procesów biznesowych organizacji współpracujących w ramach tych procesów.
- ♦ Ustanowienie z podmiotami współpracującymi protokołów ustaleń (Memorandum of Understanding - MoU).
- ♦ Ustalenie w zakresie świadczonych usług i otrzymywanych usług porozumień dotyczących jakości tych usług (Service Level Agreement).

• Poziom semantyczny
- ♦ Zapewnienie, że dane wymieniane pomiędzy organizacjami będą jednolicie interpretowane, a ich integralność będzie zapewniona.
- ♦ Zapewnienie możliwości pozyskiwania danych z zewnętrznych systemów, przy zapewnieniu ich poprawnej interpretacji.
- ♦ Ustalenie specyficznych struktur danych i ich publikacja.

• Poziom techniczny
- ♦ Zapewnienie, że wszystkie interfejsy będą wyspecyfikowane.
- ♦ Zapewnienie oparcia mechanizmów wymiany informacji opartych o przyjęte standy krajowe lub międzynarodowe.
- ♦ Zapewnienie łączności umożliwiającej świadczenie usług.
- ♦ Zapewnienie usług wymiany i integracji danych.
- ♦ Zapewnienie usług prezentacji danych.

Zbiorcza ocena projektów

W lipcu i sierpniu 2010 roku wykonana została ocena projektów realizowanych z VII POiG. Oceniono wszystkie projekty realizowane przez instytucje centralne, dla których instytucją pośredniczącą (nadzorującą projekt merytorycznie) jest MSWiA. Celem tej oceny było zestawienie podstawowych problemów, jakie występują w większości ocenianych projektów pod kontem interoperacyjności. W kolejnych punktach przedstawiam zbiorczą ocenę tych projektów w odniesieniu do wymienionych wyżej podstawowych warunków interoperacyjności.

Większość ocenianych projektów ma niewłaściwie zdefiniowane cele – niewskazujące nastawienia na użytkownika ani nieokreślające, czym będzie skutkowało przedsięwzięcie. Celem większości projektów jest zbudowanie systemu, a nie rozwiązanie problemu lub ulepszenie stanu. Skutkuje to trudnością w określeniu mierzalnych kryteriów realizacji przedsięwzięcia oraz trudnością w zdefiniowaniu użytkowników tworzonych rozwiązań informatycznych. W wyniku przeglądu projektów stwierdzono, iż spełnienie warunku nastawienia na użytkownika w realizowanych projektach jest praktycznie niemożliwe. Efektem może być zbudowanie systemów nierealizujących potrzeb ich rzeczywistych użytkowników.

Projekty pomijają wymagania integracji i dostępności. W trakcie badania dokumentacji projektów i założeń ich realizacji nie znaleziono wymagań wspierających dostępność dla osób niepełnosprawnych i starszych, co w przypadku systemów wspierających procedury administracyjne jest błędem istotnym. Pojedyncze z badanych projektów deklarowały nastawienie na użytkownika niepełnosprawnego, jednak przegląd dokumentacji nie wskazywał na żadne działania, które prowadziłyby do mierzalnych efektów w tym zakresie.

Większość projektów w obszarze bezpieczeństwa i prywatności odsyła do warstwy technologicznej oraz przewiduje wykonanie analiz i założeń dotyczących bezpieczeństwa oraz prywatności do wykonania na późniejszym etapie realizacji. Jest to zdecydowany błąd, gdyż struktura projektu i architektura rozwiązania na poziomie jej projektowania powinna uwzględniać założenia polityki bezpieczeństwa oraz określone wymogi dla obszaru prywatności. Wymogi analizy pozwalają dopiero w sposób kompetentny określić architekturę realizowanego systemu i proponowane technologie.

Problemem ocenianych projektów informatycznych jest to, że nie próbują upraszczać procedur administracyjnych i w większości przenoszą w świat elektroniczny procedurę papierową, bez analizy możliwości jej uproszczenia. Nie dość, że budowa rozwiązań skupia się na odtworzeniu procedur, to w większości projektów w dokumentacji brakuje odniesienia do procedur administracyjnych, jakie będą wspierane przez budowane systemy. Nie ma więc możliwości ich analizy, optymalizacji i zapewniania interoperacyjności na tym poziomie. Natomiast w kilku projektach zakłada się, że dopiero jak będzie zbudowany system, zrobi się analizy jego przydatności w procedurach administracyjnych.

Kultura polskiej administracji publicznej nie dopuszcza opinii publicznej, w tym użytkowników systemów, do możliwości wyrażenia swojej opinii na temat planowanych zmian, zgłaszania propozycji w zakresie zmian i ew. krytykowania przyjętych propozycji. W tym kontekście kryterium przejrzystości jest całkowicie obce wszystkim projektom, realizowane są one w całkowitym odizolowaniu od jakiegokolwiek wpływu użytkowników na ich realizację, łącznie z tym, że nie istnieje przejrzystość i wymiana informacji pomiędzy ocenianymi projektami. Istnieje więc realne zagrożenie, że będą poważne problemy na etapie wdrożenia i korzystania z realizowanych w projektach procedur i rozwiązań.

Zabezpieczenie informacji w EIF jest rozumiane jako: czytelność, wiarygodność i integralność w czasie i są dostępne przy zachowaniu bezpieczeństwa i poufności. – w tym kontekście wiele projektów w ogóle nie podejmuje działań mających na celu określenie, jakie informacje zbierają, w jakim celu i jakie procesy w związku z tym potrzebują dokumentować. Prowadzący projekty nie wychodzą w rozumieniu procesów i dokumentów poza procedury Kodeksu Postępowania Administracyjnego.

Większość projektów deklaruje iż w zakresie poziomu prawnego spełnia kryteria interoperacyjności. W praktyce, analizując szczegółowo projekty, widać, iż najczęściej jest to deklaracja oparta albo dopiero na planowanych zmianach prawnych, albo nie poparta szczegółową analizą tego problemu. Największe zagrożenia są widoczne w projektach, które deklarują zgodność z wymaganiami Ustawy o Informatyzacji podmiotów realizujących zadania publiczne i wydanych na jej podstawie przepisów wykonawczych. Warto zauważyć, że do dnia dzisiejszego większość rozporządzeń do ustawy o informatyzacji nie zostało opublikowanych, co stwarza realne zagrożenie dla realizowanych projektów.

Realizacja celów projektu wymaga wdrożenia mechanizmów, które pozwalają należycie kontrolować przebieg projektu, monitorować jego produkty, a przede wszystkim weryfikować, czy projekt nadal realizuje założone cele. Zarządzanie projektem powinno poza czynnością kontrolną i wydawaniem przeznaczonych na projekt środków zapewnić, że uzasadnienie dla realizacji projektu jest nadal w mocy, a w przypadku, gdy cele i produkty wymagają modyfikacji, je modyfikować. Większość projektów deklaruje, iż jest prowadzona zgodnie z metodyką projektową PRINCE 2. Takie działanie zwiększałoby znacznie szansę, iż realizowane projekty będą interoperacyjne organizacyjnie. Jednak w dużej liczbie projektów analiza przekazanej dokumentacji nie potwierdza tego oświadczenia, a nawet wskazuje, iż prowadzącym projekt brakuje wiedzy o wymaganiach tej metodyki.

W projektach, które wspominają o procedurach administracyjnych, brakuje najczęściej opisu sposobu uzgodnień organizacyjnych z właścicielami wspominanych procedur administracyjnych, nawet jeśli dotyczy to tej samej jednostki organizacyjnej. W większości projektów interoperacyjność organizacyjna jest zapewniana tylko w najbliższym

otoczeniu projektu, pomimo że często projekt będzie udostępniał dane zdecydowanie szerszemu kręgowi podmiotów publicznych.

W zakresie interoperacyjności na poziomie semantycznym większość projektów deklaruje korzystanie z Centralnego Repozytorium Wzorów, co umożliwi ujednolicenie struktur danych, wprowadzi jednolite wzory dla danych rodzajów dokumentów. Znaczące ryzyko stanowi jednak to, że cały czas brakuje przepisów wykonawczych dotyczących funkcjonowania repozytorium wzorów, a także brakuje mechanizmów wspierających ich tworzenie.

Wnioski sformułowane przez oceniających w obszarze interoperacyjności

Poniżej przytaczam wnioski sformułowane przez autorów badania:

1. Problematyka interoperacyjności w większości projektów traktowana jest deklaratywnie. Widać, że wymagania prawne i organizacyjne dotyczące tej problematyki są słabo znane.
2. Zdecydowanie największym zagrożeniem dla realizowanych projektów jest brak przepisów wykonawczych do Ustawy o informatyzacji podmiotów realizujących zadania publiczne, szczególnie dotyczących e-PUAP, zaufanego profilu, repozytorium wzorów.
3. Opóźnienia w uchwalaniu nowej Ustawy o podpisach elektronicznych, Ustawy o Dowodach Osobistych i w realizacji projektu pl.ID stwarzają też istotne zagrożenia w realizacji większości projektów, które opierają się na mechanizmach uwierzytelniania i autoryzacji przewidzianych w tych przepisach i projekcie.
4. Niezależnie od opóźnień, o których mowa we wniosku 3, zagrożenie dla realizowanych projektów stanowi brak publicznej informacji i nierealizowanie interoperacyjności organizacyjnej w projektach e-PUAP i pl.ID.
5. Większość zespołów projektowych nie wie, iż istnieje Portal Interoperacyjności prowadzony przez MSWiA i nie korzysta z tego narzędzia.
6. Zespoły projektowe wskazują często na brak wsparcia merytorycznego w zakresie interoperacyjności ze strony komórek organizacyjnych ministra właściwego ds. informatyzacji. Pojawia się oczekiwanie stworzenia mechanizmów wspierających powstanie zasobów informacyjnych współdzielonych przez zespoły projektowe, mającego być rodzajem „pamięci instytucjonalnej".
7. Projekty nie są między sobą koordynowane, a doświadczenia i praktyki nie są wymieniane pomiędzy projektami. Pojęcie re-używalności rozwiązań powstających w projektach jest obce i obserwuje się brak współpracy merytorycznej. Miejscem takiej współpracy powinna być instytucja ministra ds. informatyzacji, będącego instytucją pośredniczącą w ramach projektów VII POIG.
8. Wyraźnie widać oczekiwanie, iż konieczne jest zapewnienie zrębów strategicznych dla powstania architektury korporacyjnej administracji publicznej. Jej brak powoduje, iż nie ma systemowych mechanizmów koordynacyjnych, na czym najbardziej cierpi przyszła interoperacyjność tworzonych systemów.

Michał Tabor – dyrektor operacyjny Trusted Information Consulting Sp. z o. o., ekspert w zakresie podpisu elektronicznego, bezpieczeństwa informacji oraz zarządzania dokumentami elektronicznymi, michal.tabor@ticons.pl.

Wolne oprogramowanie w zamówieniach publicznych – kilka uwag na marginesie orzecznictwa Krajowej Izby Odwoławczej

Bohdan Widła

Na przestrzeni ostatnich kilkunastu miesięcy Krajowa Izba Odwoławcza wydała kilka orzeczeń, które dotyczyły wykorzystywania wolnego oprogramowania przez podmioty zobligowane do stosowania ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych. Dopuszczenie (lub wykluczenie) możliwości oferowania oprogramowania rozpowszechnianego w oparciu o wolne licencje powoduje liczne problemy prawne, zwłaszcza jeżeli przedmiot zamówienia obejmuje świadczenia, które są bardziej skomplikowane od dostawy standardowego oprogramowania „w pudełkach". Celem niniejszego artykułu jest krótkie omówienie tych problemów, w nawiązaniu do wydanych do tej pory orzeczeń KIO.

Wolne oprogramowanie jako produkt równoważny

Jeżeli przedmiot zamówienia jest stosunkowo nieskomplikowany (na przykład jeżeli zamówienie dotyczy standardowego oprogramowania użytkowego), podstawowym problemem, jaki może wystąpić, jest zagadnienie równoważności zaoferowanych produktów. Od dłuższego czasu w przypadku większości typów oprogramowania użytkowego na rynku występują zarówno rozwiązania oparte o „własnościowy" model licencyjny, jak i rozwiązania stanowiące wolne oprogramowanie. Nie wymaga większego komentarza sytuacja, w której zamawiający wprost wskazuje w specyfikacji istotnych warunków zamówienia (SIWZ), że wymaga dostarczenia oprogramowania pochodzącego od konkretnego producenta lub nie wprost, odpowiednio określając cechy produktu, wskazuje na konkretnego producenta. Będzie to zazwyczaj naruszenie art. 29 ust. 3 Pzp[1].

W tego typu stanie faktycznym zapadł wyrok KIO z 26 stycznia 2010 r. (KIO/UZP 1733/09). Zamawiający określił żądany produkt jako „Oprogramowanie MS Office 2007 SB PL OEM" i podał ogólną informację, iż „dopuszcza się zastosowanie materiałów równoważnych, których parametry nie są gorsze od wymaganych w SIWZ", nie precyzując jednak żadnych kryteriów równoważności. Odrzucono ofertę na dostarczenie pakietu OpenOffice HOME OEM CD, ponieważ według zamawiającego nie zapewniał on całkowitej kompatybilności z preferowanym oprogramowaniem. Izba przypomniała wielokrotnie wypowiadany w orzecznictwie pogląd, że równoważność „nie może oznaczać (...) tożsamości produktów, ponieważ przeczyłoby to istocie oferowania produktów równoważnych i czyniłoby oferowanie produktów równoważnych w praktyce niemożliwym do spełnienia". Zgodziła się natomiast z argumentami odwołującego, który wykazywał równoważność zaoferowanego przez siebie pakietu z pakietem preferowanym według treści SIWZ.

Ciekawsze są przypadki, w których zamawiający wskaże konkretnego producenta, dodając jednocześnie wyrazy „lub

1 Chyba że w konkretnym przypadku istnieją obiektywne przyczyny uzasadniające tak daleko idące ograniczenie konkurencji; zob. wyrok KIO z 30 marca 2010 r., KIO/UZP 377/10. Wydaje się jednak, że w przypadku standardowego oprogramowania użytkowego byłyby to możliwe tylko w bardzo nielicznych wypadkach.

równoważny" i określając kryteria równoważności[2], w ślad za dyspozycją art. 29 ust. 3 Pzp.

Wyrok KIO z dnia 28 września 2009 r. (KIO/UZP 1274/09) zapadł w tego rodzaju sytuacji. Zamawiający opisał przedmiot zamówienia jako pakiet biurowy „MS Office 2007 PL SB lub równoważny (…)". Wskazując kryteria równoważności stwierdził, że produkt równoważny powinien realizować „wszystkie funkcje przy pomocy tych samych klawiszy na klawiaturze oraz skrótów klawiszowych w trakcie jego obsługi. Musi zapewniać bezbłędną współpracę (w tym konwersje tabel) z MS Word, MS Excel". Oferta wykonawcy, który zaoferował pakiet Open Office PL Professional 2009, została odrzucona, ponieważ w trakcie przewidzianego w SIWZ badania kompatybilności pakiet ten nie funkcjonował poprawnie z przygotowanymi przez zamawiającego plikami. Testowano jednak nie tylko funkcjonalność związaną z konwersją tabel, ale także m.in. obsługę makr. KIO stwierdziła, że skoro na etapie formułowania opisu przedmiotu zamówienia zamawiający nie wskazał bardziej szczegółowych wymagań, nie może rozszerzać ich listy na etapie oceny ofert. Zgodnie z SIWZ kompatybilne z MS Office miały być funkcjonalności dotyczące wyświetlania tabel i zaoferowany pakiet wymogi te spełniał. Krajowej Izby Odwoławczej nie przekonał ani argument, że plik z tabelami otwierał się prawidłowo dopiero po zmianie rozszerzenia z *.docx na *.doc, ani stwierdzenie, że pracownicy zamawiającego nie radzą sobie z pakietem Open Office. KIO wytknęła także, że gdyby bardziej precyzyjne kryteria znalazły się już w SIWZ, to w praktyce spełniałby je tylko jeden produkt, a zatem dopuszczalność produktów równoważnych byłaby jedynie pozorna.

Ograniczenie dopuszczalności oprogramowania na wolnej licencji

Kolejnym problemem, który może mieć istotne znacznie także w bardziej skomplikowanych zamówieniach na systemy informatyczne, jest zagadnienie ograniczenia lub wyłączenia przez zamawiającego możliwości oferowania oprogramowania rozpowszechnianego na wolnej licencji.

W praktyce zamawiający rzadko wprost zakazują oferowania oprogramowania na wolnej licencji. Znacznie częściej istotne postanowienia umowy lub wzory umów umieszczane w SIWZ zawierają tak sformułowane wymagania dotyczące praw własności intelektualnej, że zastosowanie wolnej licencji jest albo wykluczone, albo trudno przesądzić, czy oferta obejmująca wolne oprogramowanie będzie zgodna z SIWZ. Najprostszą metodą określenia warunków licencyjnych, jaką może zastosować zamawiający, jest wskazanie we wzorze umowy pól eksploatacji utworu w rozumieniu art. 74 prawa autorskiego[3] wraz z podaniem rodzaju licencji (wyłączna, niewyłączna), zakresu terytorialnego i czasu jej trwania[4].

Tymczasem praktycznie każda wolna licencja nakłada na licencjobiorcę pewne dodatkowe obowiązki. Zwykle nie ograniczają

2 Zamiast wielu zob. wyrok KIO z 6 sierpnia 2009 r., KIO/UZP 967/09.

3 Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

4 Niewskazanie pól eksploatacji może niekiedy skutkować bezskutecznością licencji z uwagi na treść art. 41 ust. 2 prawa autorskiego, choć przepis ten coraz częściej interpretowany jest przez doktrynę liberalnie (zob. E. Traple, *Umowy o eksploatację utworów w prawie polskim*, Warszawa 2010, s. 39-48). Natomiast niewskazanie czasu trwania licencji i jej zakresu terytorialnego spowoduje wejście w to miejsce dyspozytywnego przepisu art. 66 ust. 1 prawa autorskiego. W konsekwencji zamawiający uzyska licencję na korzystanie z oprogramowania w państwie swojej siedziby (czyli w Polsce) przez 5 lat.

one „zwykłego" korzystania z programu, jednak mogą wpływać na działania związane z modyfikowaniem i rozpowszechnianiem. Obowiązki te mogą być bardzo rozbudowane, jak dzieje się to w przypadku licencji w modelu *copyleft* albo stosunkowo ograniczone, a w przypadku niektórych klauzul zbieżne z obowiązkami wynikającymi z bezwzględnie obowiązujących przepisów polskiego prawa autorskiego. Powstaje pytanie, czy zaoferowanie oprogramowania rozpowszechnianego na wolnej licencji, przy takim sformułowaniu postanowień wzorca umowy, może być podstawą do odrzucenia oferty wykonawcy jako sprzecznej z SIWZ (art. 89 ust. 1 pkt 2 pzp). Oczywiście rozstrzygnięcie sprzeczności oferty z SIWZ wymaga każdorazowego porównania treści oferty z treścią specyfikacji. Można jednak sformułować kilka ogólnych uwag.

Po pierwsze, jeżeli zamawiający nie wskazał w SIWZ pól eksploatacji wymienionych w art. 74 ust. 4 pkt 2-3 prawa autorskiego, dotyczących modyfikowania i rozpowszechniania, ewentualne obowiązki nakładane na zamawiającego w tym zakresie nie powinny wpłynąć na odrzucenie oferty, o ile w pozostałym zakresie treść licencji jest zgodna z SIWZ. Pominięcie tych pól może jednak narazić zamawiającego na zarzut braku zabezpieczenia praw pozwalających na uniknięcie przywiązania do jednego dostawcy (*vendor lock-in*).

Jeżeli te pola eksploatacji zostały wskazane we wzorze umowy, w konkretnym przypadku można argumentować, że w praktyce ograniczenia zawarte w tekście licencji często w żaden sposób nie ograniczają swobody zamawiającego w realizacji jego celów. Nasuwa się jednak kontrargument, iż skoro zamawiający wprost sformułował warunki licencji, to wykonawca musi udzielić mu licencji na tych warunkach i żadnych innych. Wykonawca może wtedy znaleźć się w sytuacji bez wyjścia. Jeżeli zaoferuje licencję innej treści, niż wskazano w SIWZ, jego oferta zostanie odrzucona. Jeżeli natomiast nie jest uprawniony z tytułu praw autorskich, a ma prawo do rozpowszechniania na mocy licencji typu *copyleft*, nie może zaoferować warunków zgodnych z wymaganiami zamawiającego pod rygorem utraty własnej licencji.

Po drugie, jeżeli zamawiający wprost przewidział we wzorze umowy odpowiedzialność za wady oprogramowania, wolne licencje, które zawierają jednoznaczne wyłączenie odpowiedzialności wykonawcy z tego tytułu, mogą być uznane za sprzeczne z SIWZ. Na marginesie warto wskazać, że wyłączenie rękojmi może powodować problemy związane ze zwrotem zabezpieczenia należytego wykonania umowy. Art. 151 ust. 2 pzp posługuje się bowiem pojęciem kwoty pozostawionej na zabezpieczenie roszczeń z tytułu rękojmi za wady i gwarancji jakości. Brak takich podstaw odpowiedzialności może więc dodatkowo uniemożliwić zamawiającemu zatrzymanie 30% wysokości zabezpieczenia.

Powstaje tu pytanie o zakres swobody wykonawcy w modyfikowaniu praw i obowiązków określonych we wzorcu wolnej licencji, na przykład przez wprowadzenie do umowy z zamawiającym odrębnej klauzuli ograniczającej zastosowanie postanowień danego wzorca licencji w stosunkach wykonawca-zamawiający. Niektóre licencje regulują tę kwestię wprost. Przykładowo GNU GPL dopuszcza przyjęcie odpowiedzialności za wady oprogramowania w zamian za dodatkowe wynagrodzenie. Sytuacja jest bardziej skomplikowana, jeżeli w tekście licencji brakuje jakichkolwiek wskazówek. Jeżeli bowiem z treści licencji wynika, że rozpowszechnianie oprogramowania dopuszczalne jest tylko z uwzględnieniem wyłączenia odpowiedzialności za wady oprogramowania, wykonawca może nie być uprawniony do rozpowszechniania oprogramowania na

innych zasadach. Należy natomiast dopuścić zobowiązanie wykonawcy do usuwania wad, jeśli wzorzec licencji zawiera wyłączenia odpowiedzialności odnoszące się do podmiotu innego niż sam wykonawca (na przykład do twórców oprogramowania będących osobami trzecimi). Powinno ono jednak być jednoznacznie sformułowane i objaśnione w treści oferty, aby nie było wątpliwości, jaka jest treść oświadczenia wykonawcy[5].

Po trzecie, łatwiej będzie obronić zaoferowanie wolnego oprogramowania, jeżeli zamiast precyzyjnego wzorca licencji zamawiający podał jedynie minimalne wymagania, jakie musi ona spełniać (minimalne uprawnienia, jakie musi mu przyznawać). Pewną wskazówką działającą na korzyść wykonawców oferujących wolne oprogramowanie może być treść wyroku KIO z 6 lipca 2010 r. (KIO/UZP 1244/10). Zamawiający ograniczył się do bardzo lakonicznego określenia wymagań co do licencji. Krajowa Izba Odwoławcza dopuściła natomiast zaoferowanie rozwiązania *open source*.

Należy ponownie podkreślić, że ocena dopuszczalności zaoferowania wolnego oprogramowania musi być dokonywana w odniesieniu do każdego przypadku osobno. Wydaje się jednak, że uprawniona jest teza, że wykonawcy łatwiej będzie wybronić zaoferowanie oprogramowania na wolnej licencji nieopartej o model *copyleft* aniżeli na licencji *copyleft*. W praktyce wykonawcy oferujący wolne oprogramowanie, jeżeli w SIWZ nie uregulowano wyraźnie przesłanek dopuszczalności jego zaoferowania, muszą liczyć się z odrzuceniem ich oferty. Skromne orzecznictwo dotyczące tej problematyki utrudnia oszacowanie ryzyka prawnego.

Na wykonawcy mogą także spoczywać pewne dodatkowe obowiązki. Przykładowo z uwagi na zasadę prowadzenia postępowania w języku polskim (art. 9 ust. 2 pzp) powinien on przedstawić tłumaczenie oryginalnego tekstu wolnej licencji, jeżeli w obrocie funkcjonuje on tylko w języku angielskim. Ponadto niektóre licencje[6] zabraniają licencjodawcy pobierania opłat licencyjnych, dopuszczając jedynie opłaty za usługi związane z oprogramowaniem czy też za nośnik. Pobieranie opłat wbrew temu zakazowi może skutkować dla niego utratą praw z licencji. Odpowiednie sformułowanie treści oferty w taki sposób, aby wykluczyć ryzyko naruszenia licencji, spoczywa na wykonawcy.

W literaturze wyrażano pogląd, iż zamawiający mają obowiązek dopuszczać do oferowania oprogramowania rozpowszechnianego w oparciu o wolne licencje z uwagi na zakaz dyskryminacji wykonawców oraz konieczność uniknięcia przywiązania do jednego wykonawcy[7]. Trzeba jednak przypomnieć, że w świetle rekomendacji Prezesa Urzędu Zamówień Publicznych w sprawie zamówień na systemy IT oprogramowanie „zamknięte" dostarczane w ramach zamówień publicznych nie może być tak „zamknięte", jak oprogramowanie dystrybuowane na wolnym rynku. Celem rekomendacji jest wskazanie zamawiającym działań, które muszą podjąć w celu ograniczenia ryzyka uzależnienia od jednego dostawcy. Rekomendacje nie nakazują przy tym dopuszczania w każdym postępowaniu oferowania

5 W orzecznictwie wypowiadano bowiem pogląd, iż oferta zawierająca sprzeczne zapisy powinna zostać odrzucona, zob. wyrok Zespołu Arbitrów z 24 kwietnia 2007 r., UZP/ZO/0-438/07. Ewentualne przygotowanie oferty w formie innej niż sugerowana przez zamawiającego w SIWZ, jako uchybienie wyłącznie formalne, nie daje natomiast podstaw do jej odrzucenia.

6 Sztandarowym przykładem może być GNU GPL.

7 Zob. K. Siewicz, *Prawne aspekty zamówień publicznych na oprogramowanie*, Poznań 2010, s. 13-17.

programów rozpowszechnianych na wolnych licencjach. Cel rekomendacji może być osiągnięty także przy odpowiednim dostosowaniu klauzul stosowanych w rozpowszechnianiu programów „własnościowych". Przeniesienie autorskich praw majątkowych lub odpowiednio szeroka licencja z zapewnionym dostępem do kodu źródłowego i pełnej dokumentacji oprogramowania, jak również transferem wiedzy dotyczącej systemu na kolejnego wykonawcę, mogą zapewnić możliwość udzielania dalszych zamówień w trybach konkurencyjnych, a więc uniknięcie zjawiska *vendor lock-in*.

Oczywiście zastosowanie wolnego oprogramowania w przytłaczającej większości przypadków spełni wymogi rekomendacji UZP. Nie stanowi to jednak podstawy do uznania obowiązku opisywania przedmiotu zamówienia tak, aby dopuścić wolne oprogramowanie. W każdym przypadku powinna być to świadoma decyzja zamawiającego, podjęta z uwzględnieniem wpływu stawianych w SIWZ wymogów co do licencji na konkurencyjność postępowania – między innymi na liczbę produktów dostępnych na rynku, spełniających kryteria zamawiającego, także te dotyczące licencji[8].

Wolna licencja jako wymóg zamawiającego

Czy jeżeli zamawiającemu zależy, aby otrzymać rozwiązanie bazujące na wolnym oprogramowaniu, może sformułować opis przedmiotu zamówienia tak, aby wykluczyć oprogramowanie rozpowszechniane w klasycznym modelu „własnościowym"?

Zagadnienie to było przedmiotem kolejnego wyroku Krajowej Izby Odwoławczej z 11 lutego 2010 r. (KIO/UZP 1853/09). Zamówienie dotyczyło wdrożenia niededykowanego systemu informatycznego. W SIWZ zastrzeżono, że oferowane przez wykonawców oprogramowanie bazodanowe musi być oprogramowaniem *open source*. Jeden z wykonawców zakwestionował to postanowienie. Zarzucił, że brak racjonalnych powodów dla takiego ograniczenia. Twierdził między innymi, że nie ma tu ryzyka braku kompatybilności z innymi elementami systemu, wartość funkcjonalna oprogramowania „własnościowego" jest przynajmniej taka sama, a w przypadku oprogramowania bazodanowego nie występuje ryzyko uzależnienia od jednego wykonawcy. Zamawiający stwierdził, że właśnie ryzyko uzależnienia od konkretnego wykonawcy zadecydowało o wprowadzeniu takiego wymogu do SIWZ. Powołał się przy tym na rekomendacje UZP w sprawie zamówień na systemy informatyczne.

Tym argumentem przekonał Krajową Izbę Odwoławczą, która uznała, że jest to obiektywna okoliczność uzasadniająca działania zamawiającego. KIO stwierdziła też, że nie ma wymogu zapewnienia każdemu wykonawcy z branży możliwości udziału w postępowaniu. Według KIO określenie *open source* nie wskazuje na konkretny produkt, tylko na grupę produktów. Na rynku funkcjonuje kilka systemów wykorzystujących opensource'owy silnik bazodanowy, więc nie zostały naruszone zasady konkurencji. Orzeczenie to wymaga szerszego komentarza.

Po pierwsze, nie sposób nie wytknąć KIO pewnej niefrasobliwości w posługiwaniu się terminologią dotyczącą wolnego oprogramowania. Izba stwierdziła bowiem, że „w przypadku systemu opartego na bazie danych open source użytkownik dysponuje oprogramowaniem jak właściciel, również w zakresie majątkowych praw autorskich", natomiast „komercyjne bazy danych są

8 W ostatniej części artykułu zasygnalizowane są niektóre problemy związane z przygotowywaniem opisu przedmiotu zamówienia uwzględniającego wolne oprogramowanie.

produktami typowo licencyjnymi, rozpowszechniane są bez kodu źródłowego, a autorskie prawa majątkowe oraz uprawnienia wynikające z licencji są zastrzeżone na rzecz autora (producenta), co powoduje, że rozbudowa systemu jest możliwa przez dokupienie dodatkowych licencji". Definicje te są oczywiście nieadekwatne – przede wszystkim błędnie sugerują, że wolne oprogramowanie nie jest rozpowszechniane w oparciu o licencje oraz że sytuacja prawna korzystającego z oprogramowania jest identyczna jak sytuacja uprawnionego z tytułu majątkowych praw autorskich[9].

Po drugie, zdaniem KIO obiektywne okoliczności uzasadniające ograniczenie w zakresie licencji mogą być związane z „zapewnieniem sobie swobodnego doboru wykonawców w przypadku ewentualnej potrzeby rozbudowy systemu, a także usług serwisowych (...) oprogramowania". Nie negując potrzeby zapobiegania uzależnieniu od jednego wykonawcy, należy postawić pytanie o adekwatność zastosowanego środka. Jak sygnalizowano powyżej, niezależność od wykonawcy można uzyskać także przez odpowiednie skonstruowanie postanowień umowy w sprawie zamówienia publicznego, bez odwołania do wolnych licencji.

W omawianym przypadku zamawiający wykazał co prawda, że na rynku istnieje kilka konkurencyjnych rozwiązań, jednak w konkretnych przypadkach ograniczenie wynikające ze wskazania wolnych licencji może być zbyt daleko idące. Nawet jeżeli ograniczenie do wolnych licencji nie wyłącza konkurencji w całości, to zamawiający nie powinni nieproporcjonalnie zawężać kręgu wykonawców mogących wziąć udział w ofercie, jeżeli ten sam skutek w postaci zapewnienia konkurencyjności przyszłych postępowań można osiągnąć za pomocą łagodniejszych środków.

Na marginesie można dodać, że omawiane orzeczenie może być uznane za wypowiedź w dyskusji co do trafności kategorycznych sformułowań zawartych w rekomendacjach UZP, zgodnie z którymi zamawiający powinien wymagać od wykonawcy przeniesienia autorskich praw majątkowych. Wypowiedź KIO sugeruje, że odpowiednio szeroka licencja spełnia zasadniczy cel rekomendacji.

Po trzecie, wydaje się, że sformułowanie „oprogramowanie *open source*" użyte przez zamawiającego w postępowaniu, w ramach którego zapadł komentowany wyrok, nie opisuje w dostatecznie precyzyjny sposób przedmiotu zamówienia, do czego obliguje art. 29 ust. 1 pzp. Przede wszystkim trudno przesądzić, jakie znaczenie zamawiający przypisuje określeniu „open source"[10]. Z braku szczegółowej definicji pojęcie to należałoby interpretować szeroko. Wykonawcy nie mogą ponosić negatywnych konsekwencji braku precyzji w opisie przedmiotu zamówienia[11], a zatem należałoby dopuścić do zaoferowania różnych licencji spełniających wymagania „open source". Dla oceny, czy dana licencja jest zgodna z wymaganym modelem, najbardziej

9 Posługiwanie się tak nieprawidłowymi definicjami dziwi zwłaszcza wobec powszechnej dostępności literatury na ten temat, zob. np. J. Barta, R. Markiewicz, *Oprogramowanie open source w świetle prawa*, Kraków 2004 czy też powoływaną wyżej pozycję: K. Siewicz, *Prawne aspekty zamówień publicznych na oprogramowanie*, Poznań 2010.

10 Nie wiadomo, czy zamawiający odnosi się do definicji opracowanej przez Open Source Initiative (http://www.opensource.org/docs/osd), czy posługuje się inną, własną definicją.

11 Wśród licznych orzeczeń zob. np. wyroki KIO z 16 czerwca 2008 r., KIO/UZP 533/08 i z 29 sierpnia 2008 r., KIO/UZP 844/08.

prawdopodobne wydaje się zastosowanie definicji wypracowanej przez Open Source Initiative[12].

Z punktu widzenia konkurencyjności postępowania brak precyzji zamawiającego mógłby być uznany za trafny. Dla uniknięcia wątpliwości i ewentualnych zarzutów nieprecyzyjnego sformułowania opisu przedmiotu zamówienia zamawiający powinni jednak wskazywać w SIWZ przynajmniej zasadnicze cechy licencji open source[13]. Z drugiej strony, po stronie zamawiającego powstaje ryzyko uzyskania oprogramowania na licencji, która wcale nie będzie zgodna z jego rzeczywistymi oczekiwaniami. Z punktu widzenia zamawiającego celowe jest zatem przeanalizowanie i wskazanie konkretnych wolnych licencji, których zastosowanie dopuszcza. W konkretnych wypadkach może się to wiązać z użyciem znaków towarowych, co pociąga za sobą dopuszczenie licencji równoważnych i wskazanie kryteriów równoważności (odnoszących się do zakresu uprawnień licencyjnych).

Wreszcie, ponownie należy zwrócić uwagę na problemy związane z odpowiedzialnością za wady oprogramowania, językiem postępowania czy dopuszczalnością opłat licencyjnych, omówione we wcześniejszej części artykułu.

Podsumowując

Wydaje się, że w orzecznictwie KIO ugruntował się pogląd o dopuszczalności oferowania wolnego oprogramowania jako produktu równoważnego wobec oprogramowania „zamkniętego". Orzecznictwo dotyczące bardziej skomplikowanych zamówień na systemy informatyczne dopiero się rozwija. Trudno sformułować jednoznaczne kryteria dopuszczalności ograniczania przedmiotu zamówienia tylko do oprogramowania własnościowego lub tylko do oprogramowania wolnego. W świetle treści rekomendacji UZP obydwa modele mają w systemie zamówień publicznych coraz więcej wspólnych cech. Zarówno postawienie wymogu udzielenia szerokiej licencji w modelu „własnościowym", jak i wymaganie zastosowania wolnej licencji, może doprowadzić do zapewnienia konkurencyjności przyszłych postępowań dotyczących rozwoju czy utrzymania systemu informatycznego. Zamawiający powinni jednak zwracać uwagę także na konkurencyjność „pierwotnego" postępowania. Także z punktu widzenia potrzeb zamawiających niezbędne jest dokonywanie przez nich świadomej oceny, jakich praw do korzystania z oprogramowania będą potrzebowali, a także czy i – przede wszystkim – na jakich zasadach dopuścić do przetargu wolne oprogramowanie. Konkurencja nie jest celem samym w sobie; podmioty publiczne muszą brać pod uwagę także inne istotne dla nich interesy.

Bohdan Widła - absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnik w kancelarii Maruta i Wspólnicy sp. j., aplikant radcowski.

12 Zob. powoływane orzeczenie w sprawie KIO/UZP 1244/10.

13 Odesłanie do źródeł takich, jak strona internetowa Open Source Initiative czy Free Software Foundation, nie będzie wystarczające z uwagi na obowiązek prowadzenia postępowania w języku polskim (art. 9 ust. 2 pzp).

Program Ramowy na rzecz Innowacyjności i Konkurencyjności a wspieranie rozwoju technologii informacyjnych i komunikacyjnych (CIP ICT PSP)

Dariusz Bogucki

Wprowadzenie

W ramach wielu programów finansowego wsparcia Wspólnoty na lata 2007-2013 warto zwrócić uwagę polskich instytucji finansowych na wspólnotowe programy ramowe. Uwaga biznesu koncentruje się przede wszystkim na programach krajowych. Programy ramowe są często pomijane w oficjalnych zestawieniach mechanizmów wsparcia dostępnych polskim przedsiębiorcom od 2007 r. Do takich programów należy *Program Ramowy na rzecz konkurencyjności i innowacji na lata 2007-2013* (CIP).

Interesująca jest historia tego Programu: Komunikat Komisji z dnia 2 lutego 2005 r. zatytułowany *„Wspólne działania na rzecz wzrostu gospodarczego i zatrudnienia – Nowy początek Strategii Lizbońskiej"* wskazywał jako jeden z niedostatków Strategii Lizbońskiej, jak to określono, „brak mostu pomiędzy badaniami i rynkiem". Komisja podjęła, co prawda w latach uprzednich, szereg inicjatyw w dziedzinie przedsiębiorczości, MŚP, konkurencyjności, przemysłu, innowacji, rozwoju ICT, technologii dla środowiska oraz inteligentnej energii, jednak okazały się one mało skuteczne.

Przyjęty w październiku 2006 r. Program Ramowy na Rzecz Konkurencyjności i Innowacji - CIP ma zapewnić spójność wszystkich podejmowanych przez Wspólnotę działań w odniesieniu do przedsiębiorczości, sektora MŚP, konkurencyjności przemysłu, innowacyjności (w szczególności technologii ekologicznych i zastosowań ICT) oraz rozwoju i promowania efektywności energetycznej i odnawialnych źródeł energii (inteligentnej energii), również w sektorze transportu.

CIP łączy działania zlokalizowane dotychczas w kliku odrębnych aktach prawnych w programy. W programie nie ma kwot przypisanych na dany kraj lub region, co oznacza tryb konkursowy wyboru najlepszych ofert na poziomie wspólnotowym. Inicjatywa jest komplementarna w stosunku do wspólnotowego programu ramowego na rzecz badań, rozwoju technologicznego i demonstracji (aktualnie jest to Siódmy Program Ramowy – FP7). Komplementarność oznacza, że CIP zajmuje się obszarem „wyników 7FP": skupia się na stymulowaniu innowacyjnych przedsiębiorstw, przyciąganiu kapitału podwyższonego ryzyka dla zakładania tego typu firm, zwłaszcza w obszarze innowacji ekologicznych i innowacji z obszaru technologii informacyjnych i komunikacyjnych (ICT) będących wynikami programów badań i rozwoju. Innymi słowy obejmuje wspieranie innowacji pozatechnologicznych i technologicznych, które wykroczyły poza końcowy etap demonstracji badawczej i są gotowe do wprowadzenia na rynek (testowanie innowacji do zastosowań rynkowych).

Program stworzono przede wszystkim z myślą o małych i średnich przedsiębiorstwach (MŚP). Jego zadaniem jest bowiem wspieranie działalności innowacyjnej (w tym innowacji ekologicznych), zapewnienie lepszego dostępu do środków finansowych oraz świadczenie na poziomie regionalnym usług wsparcia dla biznesu. Program ma zachęcać do szerszego i lepszego wykorzystania

technologii informacyjnych i komunikacyjnych (ICT) oraz wspomagać rozwój społeczeństwa informacyjnego, a także promować wzmożone wykorzystanie energii odnawialnej i efektywność energetyczną. Budżet Programu CIP dla wszystkich państw uczestniczących w Programie na lata 2007-2013 wynosi **3631,3 mln €.** Program ramowy składa się z trzech tzw. programów szczegółowych:

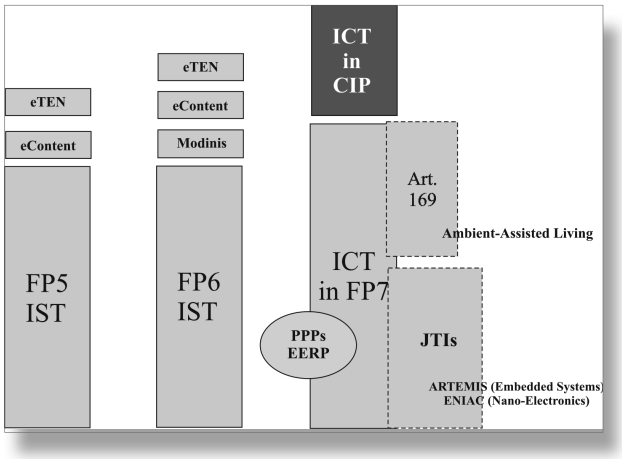
- **Program na Rzecz Przedsiębiorczości i Innowacji** (Entrepreneurship and Innovation Programme EIP) obejmujący działania finansowe i pozafinansowe na rzecz przedsiębiorczości, małych i średnich przedsiębiorców, konkurencyjności i innowacji, a w szczególności:
  - ułatwienie dostępu do finansowania przeznaczonego na rozpoczęcie i rozwój działalności MŚP i zachęcanie do inwestycji w innowacyjne przedsięwzięcia, w tym przedsięwzięcia eko-innowacyjne,
  - tworzenie środowiska sprzyjającego kooperacji wśród MŚP, zwłaszcza w obszarze współpracy zagranicznej, wspieranie innowacji w przedsiębiorstwach, w tym innowacji ekologicznych,
  - promocja kultury przedsiębiorczości i innowacji,
  - promocja i wspieranie reform administracyjnych i gospodarczych związanych z przedsiębiorczością i innowacyjnością.
- **Inteligentna Energia** - Program dla Europy (Intelligent Energy Europe Programme - IEE) obejmujący działania mające na celu poprawę efektywności energetycznej oraz racjonalne wykorzystanie zasobów energetycznych, promowanie nowych i odnawialnych źródeł energii oraz wspieranie dywersyfikacji jej źródeł.
- **Program na Rzecz Wspierania Polityki Dotyczącej Technologii Informacyjnych i Komunikacyjnych** (Information Communication Technologies - Policy Support Programme ICT-PSP) mający na celu wspieranie wdrażania technologii informacyjnych i komunikacyjnych, a także pobudzenie innowacji poprzez zwiększenie zakresu stosowanych technologii, któremu to programowi poświęcona jest zasadnicza część artykułu.

Zakres Programu na Rzecz Wspierania Polityki Dotyczącej Technologii Informacyjnych i Komunikacyjnych (ICT PSP)

Celem ICT PSP jest wsparcie działań zmierzających do **szybkiego wdrożenia innowacyjnych technologii informacyjnych i komunikacyjnych w gospodarce oraz pobudzenie innowacyjności poprzez zwiększenie zakresu stosowania i inwestowania w te technologie.**

Na cały program szczegółowy ICT PSP przewidziano budżet w wysokości **730 mln €**, a jego adresatami są: europejski przemysł z sektora ICT, innowacyjne MŚP oraz uczelnie wyższe, a także administracja publiczna.

Należy podkreślić, że idea programu europejskiego wspierającego implementację innowacyjnych technologii w obszarze ICT (a zwłaszcza wyników projektów badawczych) nie jest nowa (patrz poniższy rysunek). Już w trakcie 5 Programu Ramowego uruchomiono eContent – wspólnotowy program mający na celu stymulowanie rozwoju i wykorzystania europejskich zasobów cyfrowych w sieciach globalnych oraz promowanie różnorodności językowej oraz eTEN – wieloletni program rozwoju transeuropejskich e-usług. Równolegle z 6 Programem Ramowym obok eContent + i eTEN funkcjonował MODINIS – program monitorowania planu działań e-Europa 2005 i rozpowszechniania dobrych praktyk oraz poprawy bezpieczeństwa sieci i informacji. Dorobek tych programów został włączony do PCP ICT.



Rys. 1 *ICT w kolejnych Programach Ramowych Badań i Rozwoju i inicjatywy wspierające*
Źródło: Komisja Europejska DG INFSO

Ze względu na specyfikę grup docelowych wprowadzono podział działań PCP ICT na trzy grupy:

- stworzenie jednolitej, europejskiej przestrzeni informacyjnej i wzmacnianie rynku wewnętrznego produktów i usług informacyjnych, co obejmuje w szczególności projekty z obszarów:
  - ♦ zapewnienia łatwego dostępu do usług opartych na technologiach informacyjno-komunikacyjnych oraz tworzenia warunków odpowiednich dla szybkiej i właściwej realizacji konwergencji komunikacji i usług cyfrowych, przy zapewnieniu interoperacyjności, bezpieczeństwa i aspektów zaufania,
  - ♦ poprawy warunków dla rozwoju zawartości cyfrowej (ang. *digital content*) ze szczególnym naciskiem na wielojęzyczność i różnorodność kulturową,
  - ♦ monitorowania Europejskiego Społeczeństwa Informacyjnego poprzez gromadzenie danych i analizę rozwoju, dostępności oraz korzystania z usług komunikacji cyfrowej, w tym rozwoju Internetu, dostępu do połączeń szerokopasmowych,
- wspieranie innowacyjności poprzez zwiększenie zakresu stosowania technologii informacyjnych i komunikacyjnych oraz inwestycji w te technologie, a w szczególności:
  - ♦ promowanie innowacyjności w procesach, usługach i produktach, których istnienie umożliwia ICT, w szczególności w małych i średnich przedsiębiorstwach i sektorze publicznym, z uwzględnieniem wymagań dotyczących niezbędnych umiejętności zatrudnionych osób,
  - ♦ umożliwianie interakcji sektora publicznego i prywatnego, jak również partnerstwa na rzecz przyśpieszenia działań innowacyjnych oraz inwestycji w ICT,
  - ♦ promowanie i podnoszenie świadomości na temat możliwości i korzyści, jakie ICT oferują obywatelom i podmiotom gospodarczym oraz zachęcanie do debaty na poziomie europejskim na temat tendencji występujących w ICT,
- stworzenie społeczeństwa informacyjnego o charakterze integrującym oraz bardziej skutecznych i wydajnych usług leżących w interesie publicznym, a w szczególności:

- ♦ zwiększenie dostępności ICT oraz umiejętności ich wykorzystywania przez użytkowników,
- ♦ wzmacnianie zaufania i pewności, w szczególności w odniesieniu do kwestii prywatności związanych z użyciem ICT,
- ♦ poprawę jakości, skuteczności i dostępności usług elektronicznych w dziedzinach będących przedmiotem zainteresowania publicznego oraz uczestnictwa, jakie umożliwiają ICT, w tym interoperacyjnych ogólnoeuropejskich lub transgranicznych usług publicznych, określenie podstaw interesu publicznego i rozpowszechniania dobrych praktyk.

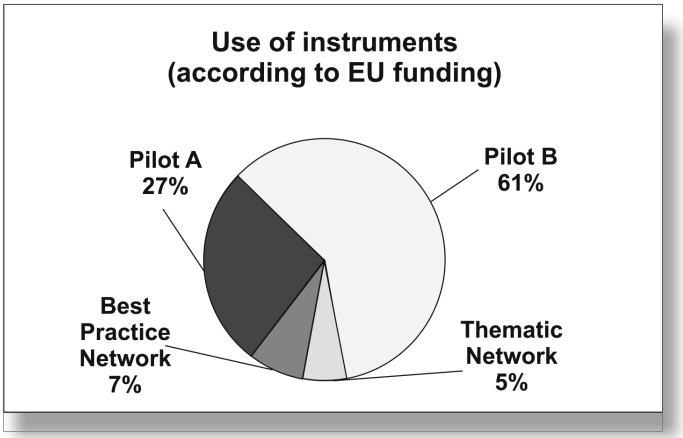
Wsparcie Programu ICT PSP

W ramach Programu przewidziano **3 typy instrumentów wsparcia**:

- **Projekty pilotażowe (Typ A)** - rozbudowa krajowych, regionalnych lub lokalnych inicjatyw zrealizowanych w Krajach Członkowskich lub Stowarzyszonych. Wkład wspólnotowy dla tego typu projektów: do 50% kosztów ściśle związanych z pracami koniecznymi do osiągnięcia celów interoperacyjności. Przeciętny budżet projektów: od 5 do 10 mln €. Wymogiem formalnym jest obecność w konsorcjum minimum 6 partnerów. Okres realizacji projektu pilotażowego Typu A wynosi do 36 miesięcy (w tym 12 miesięcy okresu pilotażowego).
- **Projekty pilotażowe (Typ B)** - stymulowanie wdrażania innowacyjnych produktów i usług bazujących na ICT. Wkład wspólnotowy dla tego typu projektów: do 50% kosztów związanych z wdrożeniem usługi pilotażowej. Przeciętny budżet projektów: od 2 do 3 mln €. Konsorcjum powinno łączyć minimum 4 podmioty z 4 różnych krajów członkowskich lub stowarzyszonych. Okres realizacji projektu wynosi od 24 do 36 miesięcy, w tym 12 miesięcy poświęcone jest na etap pilotażowy.
- **Sieci Tematyczne** - tworzenie forum wymiany doświadczeń i budowy konsensusu dla interesariuszy Społeczeństwa Informacyjnego. Wkład wspólnotowy dla tego typu projektów: do 100% kosztów bezpośrednich związanych z koordynacją i wdrożeniem sieci. Przeciętny budżet dla każdej sieci tematycznej: 300 do 500 tys. € i jest uzależniony od wielkości sieci:
  - ♦ roczny koszt koordynacji wynosi 3000 €/ partnera, gdy sieć zrzesza do 10 podmiotów,
  - ♦ 2000 €/partnera na każdego kolejnego partnera od 11 do 21 podmiotu, przy większych sieciach nie otrzymuje się dodatkowych dotacji,
  - ♦ koszt wdrożenia wynosi 3000 €/partnera,
  - ♦ budżet na podróże wynosi 5000 €/ partnera.

  Jednocześnie wymagany jest udział minimum 7 podmiotów z 7 różnych krajów członkowskich lub stowarzyszonych z UE. Przykładowe działania w projekcie Sieci Tematycznej to:
  - tworzenie forum wymiany dobrych praktyk pomiędzy organizacjami mającymi kluczowe znaczenie w danej dziedzinie a nabywcami innowacyjnych usług,
  - angażowanie rządów krajów członkowskich w celu wypracowania wspólnego podejścia lub rozwiązania w kwestii transgranicznych, interoperacyjnych usług,
  - opracowanie, wdrożenie i transfer wspólnych norm, standardów dla rozwiązań i usług elektronicznych,
  - wspieranie i udostępnianie wiedzy technicznej i wiedzy potrzebnej do wdrażania innowacyjnych narzędzi i usług na poziomie europejskim, przy jednoczesnym zapewnieniu ochrony prywatności itp.

Pewnym wariantem Sieci Tematycznej jest tzw. **Sieć Dobrych Praktyk (Best Practice Network),** która pojawiła się w 2009 roku



Rys. 2 *Wykorzystanie poszczególnych instrumentów wsparcia ICT PSP w latach 2007-2009*
Źródło: Komisja Europejska, Raport Implementacyjnego CIP za rok 2009

jako instrument przeniesiony z zakończonego w 2008 r. Programu eContentplus[1] i ma charakter tymczasowy (do 2011 r.). Zastosowanie tego instrumentu finansowego jest również ograniczone do projektów w tzw. Temacie 2 – Biblioteki cyfrowe (Digital Libraries).

Co ważne, w przypadku całego CIP obowiązują zasady finansowania ustalone przez UE dla programów badawczych i rozwojowych związane z przeniesieniem ryzyka na poziom Wspólnotowy: mówiąc kolokwialnie, środki wsparcia zasadniczo nie podlegają zwrotowi w przypadku niepowodzenia projektu (chyba że środki nie zostały wykorzystane zgodnie z przeznaczeniem).

Uczestnictwo w Programie ICT PSP

Ogólne zasady uczestnictwa w PSP ICT są bardzo podobne do innych programów UE, a zwłaszcza do uczestnictwa w 7 Programie Ramowym:

- Komisja Europejska ogłasza corocznie plan działania, który zawiera wyszczególnienie obszarów tematycznych projektów przewidywanych do wsparcia w danym roku. Obszary te są różne w kolejnych latach. W 2010 roku (w ramach tzw. Konkursu 4) takimi tematami były:

Temat 1: ICT na rzecz wydajności energetycznej i mobilności – budżet łączny 19 mln €: wydajność energetyczna w budownictwie społecznym, transporcie i wdrożenie usług alarmowych bazujących na numerze 112.
Temat 2: Biblioteki cyfrowe – 30 mln €: dalszy rozwój zasobów Europejskiej Biblioteki Cyfrowej Europeana oraz zwiększenie dostępu do publikacji naukowych.
Temat 3: ICT na rzecz zdrowia i społecznej spójności – 14 mln €: poprawa dostępu do usług medycznych.
Temat 4: Otwartość działań innowacyjnych na rzecz usług on-line w miastach – 15 mln €.
Temat 5: ICT na rzecz poprawy usług publicznych dla obywateli i przedsiębiorstw – 13 mln €: pilotażowe wdrożenia e-usług na szczeblu krajowym.
Temat 6: Wielojęzyczny Internet – 16 mln €: wsparcie dla rozwoju wielojęzycznych serwisów internetowych oraz infrastruktury.

1 Następcy programu eContent.

Każdy konkurs ma inny zakres tematyczny (inne dokumenty zaproszenia publikowane są przy ogłoszeniu konkursu). Tematyka zgłoszonego projektu musi korelować z tematyką otwartego konkursu, a nie któregoś z poprzednich. Projekty składane są bezpośrednio do Komisji Europejskiej w wersji elektronicznej poprzez system EPSS (Electronic Proposal Submission Service). Nie ma możliwości składania wniosków „papierowych".

- Projekty muszą mieć charakter współpracy międzynarodowej i rozwiązywać problemy wspólne dla kilku krajów lub całej Europy.
- Projekt przygotowuje międzynarodowe konsorcjum składające się z kilku organizacji – ich liczba jest uzależniona od schematu finansowego i działań w projekcie. Nie ma zakazu realizacji projektów „jednokrajowych", tym niemniej każdorazowo oceniany jest tzw. aspekt europejski jego realizacji.
- Projekty składane są wyłącznie na konkretne zaproszenie do składania wniosków (Call for Applicants), których może być ogłoszonych kilka w danym roku (praktycznie 1-2).
- Projekty oceniane są przez niezależnych ekspertów powoływanych przez Komisję Europejską ze zgłoszeń składanych do niej bezpośrednio drogą elektroniczną.

Program wspiera tzw. Krajowy Punkt Kontaktowy (działający od 1999 roku przy Instytucie Podstawowych Problemów Techniki PAN), którego działania koncentrują się na realizacji głównego celu, jakim jest zwiększanie polskiego udziału w programach ramowych KPK, ściśle współpracuje z Ministerstwem Nauki i Szkolnictwa Wyższego, Ministerstwem Gospodarki, Komisją Europejską, Parlamentem Europejskim, PARP. Do zadań KPK należy:

- promocja programu i prowadzenie strony internetowej zawierającej informacje nt. programu,
- udzielanie informacji beneficjentom programu oraz wsparcie w znalezieniu partnerów przedsięwzięcia (prowadzenie tzw. bazy partnerów),
- utrzymywanie stałej współpracy z właściwymi służbami Komisji Europejskiej.

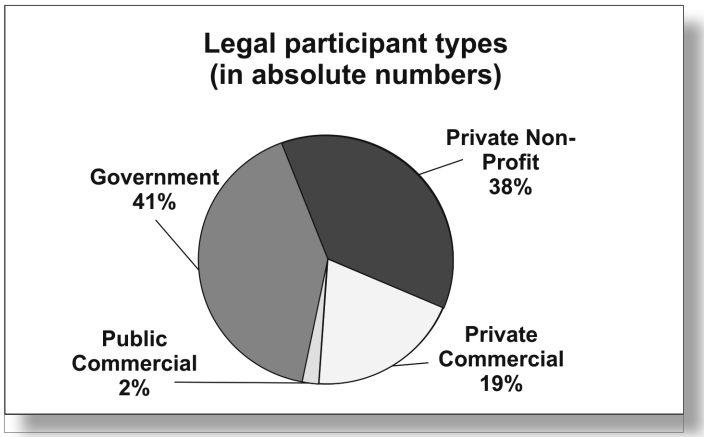
Tematy przewidywane do wspierania w ramach 5 Konkursu w 2011 roku mają zostać opublikowane przez Komisję wraz z planem działania na 2011 rok jeszcze w tym roku. Planowany termin uruchomienia konkursu to luty 2011.

Podsumowanie

Po okresie, kiedy polska branża ICT skoncentrowała się na pozyskiwaniu środków z funduszy strukturalnych, powoli wraca zainteresowanie „trudniejszym" finansowaniem z programów wspólnotowych, takich właśnie jak CIP PSP ICT. Jak się wydaje, głównym powodem nie jest wyłącznie obawa, że środki z funduszy strukturalnych będą znacząco mniejsze w kolejnym programowaniu (na lata 2014-2020).

Finansowanie z takich programów jak Program Ramowy na Rzecz Badań i Rozwoju czy właśnie Program Ramowy na rzecz Innowacyjności i Konkurencyjności (CIP), czy wspomniany Program AAL niesie bowiem szereg korzyści nieosiągalnych w programach krajowych. Główną jest możliwość współdziałania z partnerami z innych krajów europejskich. Pokazuje to poniższy wykres prezentujący uczestnictwo podmiotów różnych kategorii w projektach CIP PSP ICT.

Warto dodać, że jednym z filarów przedstawionej 06.10.2010 Strategii „Unia Innowacji" (jest to jedna z siedmiu strategii kierunkowych planu Europa 2020) ma być właśnie aktywne wspieranie procesu implementacji wyników badań w nowych, innowacyjnych rozwiązaniach rynkowych. Tak więc należy spodziewać



Rys. 3 Uczestnictwo różnych typów podmiotów w projektach PSP ICT w latach 2007-2009
Źródło: Komisja Europejska, Raport Implementacyjnego CIP za rok 2009

się, że obecny Program Ramowy na Rzecz Konkurencyjności i Innowacyjności będzie kontynuowany w perspektywie do 2020 roku.

Dr inż. Dariusz Bogucki - Dyrektor ds. Sektora Publicznego, EFICOM SA.

Zapraszamy do udziału

XVII edycja konferencji w cyklu
TECHNOLOGIE INFORMATYCZNE W MEDYCYNIE
ASPEKTY INFORMATYCZNE ORAZ PRAWNE ELEKTRONICZNYCH REJESTRÓW MEDYCZNYCH
24 lutego 2011 r., Warszawa

Prowadzenie obrad: Krzysztof Nyczaj

W PROGRAMIE:
- Interoperacyjność systemów informacyjnych w procesie informatyzacji ochrony zdrowia.
- Rejestr Usług Medycznych jako istotny element wspierania procesów analitycznych i decyzyjnych - zakres danych RUM.
- Platforma on-line udostępniania usług i zasobów cyfrowych - wspólna dla wszystkich rejestrów medycznych. Nowe regulacje prawne i wynikające z nich możliwości. Wizja e-usług w zakresie e-zdrowia.
- Modele rejestrów ochrony zdrowia w polskim systemie prawnym.
- Rejestr zakładów opieki zdrowotnej.
- Integracja rejestrów onkologicznych.
- Rola algorytmow i nowych technologii w procesach wsparcia decyzji i kwalifikacji w oparciu o doświadczenia Ewidencji RZS.
- Bezpieczeństwo danych elektronicznych w systemach informatycznych ochrony zdrowia.
- System informacji medycznej - omówienie podstawowych założeń ustawy o informacji w służbie zdrowia

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Potwierdzenie tożsamości w elektronicznym obrocie gospodarczym a elektroniczna administracja - część I

Izabela Adamska

W obrocie gospodarczym coraz bardziej powszechna staje się komunikacja elektroniczna. Dziś trudno wyobrazić sobie świat bez komputerów. Internet wkracza w różne sfery naszego życia, proponując nowe rozwiązania. Dzięki nieograniczonemu dostępowi do Internetu można załatwić codzienne sprawy: sprawdzić stan konta bankowego, zapłacić bieżące rachunki, zrobić zakupy, złożyć wniosek do urzędu, czy nawet zobaczyć się z bliskimi przebywającymi w innym kraju, a także zawierać umowy.

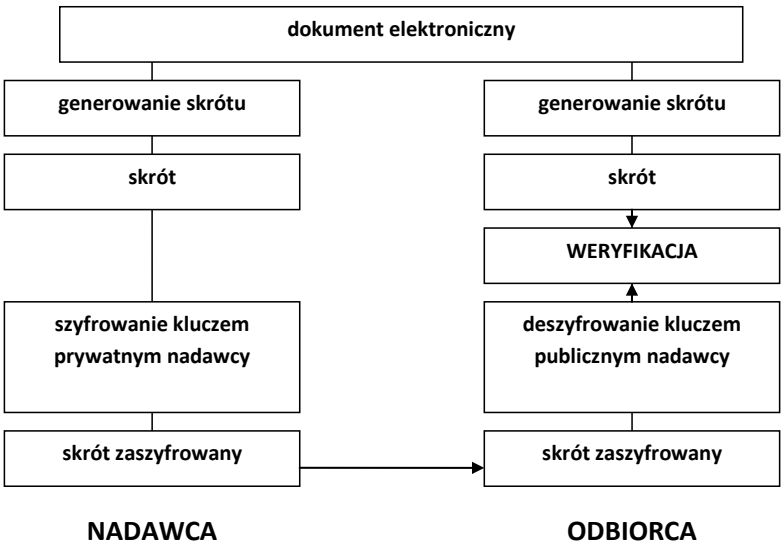
Zaufanie w obrocie gospodarczym ma zasadnicze znaczenie, jego podstawą są dokumenty uwiarygodniające kontrahenta, a następnie rzetelność wynikająca z osobistych kontaktów. Jednak dokumenty potwierdzające tożsamość osoby nie zawsze są gwarancją, że podpisujący posiada odpowiednie uprawnienie do reprezentacji firmy, może się bowiem tak zdarzyć, że pełnomocnictwo zostało już wycofane. Obecnie czas i koszty związane z ustaleniem autentyczności dokumentu oraz uprawnień osoby podpisującej często prowadzą do podjęcia znacznego ryzyka, a nawet do wycofania się z transakcji. Dlatego tak ważne jest zbudowanie wzajemnego zaufania w relacjach gospodarczych, co prowadzi do obniżenia ryzyka handlowego, a w konsekwencji do zwiększenia obrotów. Zapobiega to sytuacji, w której przechwycony dokument może zostać zmodyfikowany, a informacje w nim zawarte mogą zostać wykorzystane w sposób nieuczciwy w celu osiągnięcia pewnych korzyści. Pozornie niewinna zmiana treści może bowiem spowodować wymierne straty finansowe zarówno dla nadawcy, jak i dla odbiorcy dokumentu. Trudno jest podejmować ryzyko, nie wiedząc czy prowadzi się rozmowy z poważnym kontrahentem, czy też z niesolidną firmą.

Komunikacja elektroniczna znacznie usprawnia przepływ informacji zarówno w organizacji, jak i w kontaktach zewnętrznych, a wprowadzenie sposobów uwierzytelniania opartych o technologie podpisu elektronicznego jest skutecznym sposobem zagwarantowania pewności obrotu w sieci. Jest to ściśle związane z szybkością oraz niskim kosztem przesyłania dużej ilości informacji. Technologia podpisu elektronicznego funkcjonowała na długo przed wejściem w życie ustawy z dnia 18 września 2001 roku o podpisie elektronicznym (Dz. U. z 2001 r. Nr 130, poz. 1450). Właściwie we wszystkich programach pocztowych podpis elektroniczny służył do identyfikacji nadawcy wiadomości oraz do szyfrowania poczty, wykorzystując technologię PKI (Public Key Infrastructure). Zwykły podpis elektroniczny przez wiele lat był skuteczny i powszechnie używany przez instytucje finansowe i klientów tych instytucji - banki nadal korzystają z certyfikatów niekwalifikowanych do zabezpieczania transakcji. Powierzając oszczędności bankom, ufamy, że są one właściwie zabezpieczone. Podpis elektroniczny odbiega zdecydowanie od tradycyjnego sposobu uwierzytelniania dokumentu i jest nierozerwalnie powiązany z treścią podpisywanego dokumentu. Podpis elektroniczny to „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".

W zakresie odpowiedzialności prawnej jedynie dokument elektroniczny opatrzony bezpiecznym podpisem elektronicznym

weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu jest równoważny z dokumentem papierowym podpisanym własnoręcznie, a to oznacza, że umowa podpisana bezpiecznym podpisem elektronicznym staje się prawnie wiążąca. Nie można więc udostępniać certyfikatu kwalifikowanego służącego do składania podpisu elektronicznego osobie trzeciej, czy też używać certyfikatu innej osoby, ponieważ bezpieczny podpis elektroniczny jest przyporządkowany wyłącznie do osoby fizycznej składającej podpis – może ona działać w imieniu własnym lub jako przedstawiciel innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Już sama konstrukcja podpisu elektronicznego jest obecnie najskuteczniejszym sposobem zabezpieczania danych. Zastosowanie dwóch różnych kluczy – prywatnego i publicznego - do podpisywania i odczytywania informacji w postaci elektronicznej znacznie podnosi poziom bezpieczeństwa, uniemożliwiając tym samym zarówno modyfikację treści, jak również zapoznanie się z dokumentem. Do podpisania bezpiecznym podpisem elektronicznym służy klucz prywatny zapisany na karcie kryptograficznej i nierozerwalnie z nią związany, co oznacza, że tylko posiadacz karty może składać podpis przy jego użyciu. Dlatego też klucz prywatny powinien być właściwie zabezpieczony przed dostępem osób trzecich. Natomiast klucz publiczny może i powinien być udostępniany odbiorcy wiadomości, bowiem służy do sprawdzenia, kto podpisał dokument. Oprogramowanie i konstrukcja karty kryptograficznej gwarantują, że dane służące do składania podpisu elektronicznego nigdy nie opuszczą karty i nie mogą zostać w jakikolwiek sposób skopiowane bądź odtworzone. Karta chroniona jest kodem PIN, definiowanym najczęściej przez jej posiadacza, a ilość nieudanych prób dostępu jest ograniczona, co gwarantuje poufność tych danych nawet w przypadku zgubienia lub kradzieży karty. Zastosowanie kryptografii asymetrycznej uniemożliwia fałszowanie podpisów pod dokumentami elektronicznymi, co w przypadku dokumentów tradycyjnych jest stosunkowo łatwe.



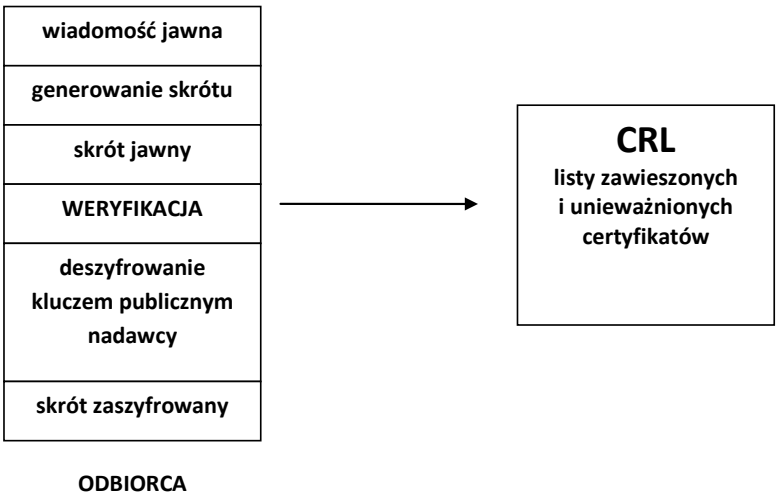
Rys. 1 Proces opatrzenia dokumentu podpisem elektronicznym
Źródło: opracowanie własne

Warto zwrócić uwagę na procedurę weryfikacji danych. Certyfikat można otrzymać na czas określony (na 12 lub 24 miesiące) po uprzednim przedstawieniu dokumentu potwierdzającego tożsamość. Dodatkowo „oprogramowanie po stronie odbiorcy usług certyfikacyjnych jest w stanie zweryfikować autentyczność i ważność certyfikatu. Weryfikacja taka sprowadza się do sprawdzenia daty ważności certyfikatu zapisanej w samym certyfikacie, sprawdzeniu ważności poświadczenia elektronicznego podmiotu, który wydał certyfikat oraz zweryfikowaniu, czy certyfikat nie został zawieszony lub unieważniony poprzez umieszczenie go na liście CRL" - podmiot świadczący usługi certyfikacyjne jest zobowiązany do publikacji list wydanych, zawieszonych oraz unieważnionych certyfikatów.

Dodatkowym zabezpieczeniem są szczególne wymagania dookreślone przez przepisy prawa, jakie musi spełniać kwalifikowany podmiot świadczący usługi certyfikacyjne. Dotyczą one zasad wydawania certyfikatów kwalifikowanych oraz wymogów technicznych użycia podpisu elektronicznego, jak również określają odpowiedzialność prawną i finansową. Obejmują między innymi:

- algorytmy kryptograficzne stosowane do generowania certyfikatów kwalifikowanych oraz bezpiecznych podpisów elektronicznych,
- długość kluczy stosowanych w celu uniemożliwienia odtworzenia klucza prywatnego odpowiadającego certyfikatowi kwalifikowanemu w czasie jego ważności,
- parametry bezpiecznego urządzenia do składania oraz weryfikacji podpisów elektronicznych.

Podpis własnoręczny złożony pod dokumentem papierowym zazwyczaj niewiele mówi o jego posiadaczu (nie dotyczy podpisów potwierdzonych notarialnie). To tylko ciąg znaków, z którego nie zawsze daje się odczytać nazwisko. W praktyce podpis elektroniczny jest



Rys. 2. Proces weryfikacji podpisu elektronicznego
Źródło: opracowanie własne

bezpieczniejszy i bardziej czytelny niż własnoręczny, całkowicie wyklucza dokonanie jakiejkolwiek zmiany w dokumencie elektronicznym po jego podpisaniu (integralność). Pozwala to na wykrycie każdej zmiany w treści dokumentu dokonanej już po jego podpisaniu, a unikalność podpisu elektronicznego gwarantuje, że nie zostanie on dołączony do innego dokumentu. Dodatkowo bezpieczny podpis elektroniczny jest sporządzany za pomocą bezpiecznych urządzeń, wobec których są stawiane dużo wyższe wymagania i które „powinny co najmniej:

1) uniemożliwiać pozyskiwanie danych służących do składania podpisu lub poświadczenia elektronicznego,
2) nie zmieniać danych, które mają zostać podpisane lub poświadczone elektronicznie oraz umożliwiać przedstawienie tych danych osobie składającej podpis elektroniczny przed chwilą jego złożenia,
3) gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ze złożeniem podpisu elektronicznego,
4) zapewniać łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian w urządzeniu do składania podpisu lub poświadczenia elektronicznego".

Izabela Adamska - pracownik administracji publicznej.

Proponujemy

WARSZTATY
PRAWO AUTORSKIE W E-BIZNESIE
16 lutego 2011 r., Warszawa

Każdy sprzedawca internetowy lub wydawca serwisu informacyjnego w Sieci porusza się wśród twórczości innych osób. Zdjęcia produktów, teksty ofertowe i artykuły prasowe, grafika - to wszystko może być utworem, który podlega automatycznej ochronie prawnej. Jeśli do tego dodać zastrzeżone znaki towarowe lub firmowe (loga i logotypy), czyli kategorie twórcze podlegające prawu własności przemysłowej, okazuje się, że działając zarobkowo w Internecie, powinniśmy przestrzegać szeregu norm prawnych, ale i etycznych.

To szkolenie odpowie na najważniejsze pytania: czym jest utwór w rozumieniu prawnoautorskim i kiedy podlega ochronie? Jakie dzieła nie podlegają prawu autorskiemu? Czym różnią się wynalazki i oznaczenia towarowe od książek i filmów (prawo własności przemysłowej a prawo autorskie)? Co wolno kopiować na swoich stronach WWW i jakie warunki muszą zostać spełnione? Jak chronić się (fizycznie, prawnie i mentalnie) przed kradzieżą własnej twórczości? Gdzie szukać darmowych, pełnowartościowych utworów (zdjęcia, teksty, grafiki) i w jaki sposób legalnie z nich korzystać?

Szkolenie prowadzi Pan Maciej Dutko.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

W oczekiwaniu na elektroniczne akty prawne

Anita Jackiewicz

Zasady i tryb ogłaszania aktów normatywnych oraz niektórych innych aktów prawnych, a także zasady i tryb wydawania dzienników urzędowych określa ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2010 r. Nr 17, poz. 95). W chwili obecnej akty prawne muszą być ogłaszane zarówno w formie papierowej, jak i elektronicznej, taki wymóg wynika z art. 2 wspomnianej ustawy w związku z art. 20a, który przewiduje formę elektroniczną aktu. Dzienniki urzędowe takie jak Dziennik Ustaw oraz Monitor Polski w formie elektronicznej dostępne są na stronach Rządowego Centrum Legislacji oraz Centrum Obsługi Kancelarii Prezesa Rady Ministrów. Dzienniki resortowe oraz akty prawa miejscowego dostępne są w formie elektronicznej na stronach BIP właściwych urzędów. Wyjątkiem są akty kierowane do ogłoszenia w Monitorze Polskim B, dla których została zastrzeżona wyłącznie postać papierowa (art. 20c).

Od dnia 1 stycznia 2012 r. planowana jest obszerna nowelizacja ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych. Autorem proponowanych zmian jest Rządowe Centrum Legislacji. Rada Ministrów w dniu 26 października 2010 r. przyjęła projekt ustawy o zmianie ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych oraz o zmianie niektórych innych ustaw (planowane zmiany dotyczyć będą również ustawy o Radzie Ministrów, ustawy o Narodowym Banku Polskim oraz ustawy o umowach międzynarodowych).

Podstawą opracowania tego projektu jest dążenie przez ustawodawcę do wdrożenia kolejnego etapu informatyzacji procesu ogłaszania aktów prawnych, który pozwoli na znaczące ułatwienia i uproszczenie dostępu do ogłaszanych w dziennikach urzędowych aktów prawnych. O tym, jak będzie w praktyce, będziemy mogli przekonać się w 2012 r., jeśli proponowane zmiany zostaną uchwalone. W uzasadnieniu projektu możemy dowiedzieć się, że dzięki realizacji proponowanych zmian Polska dołączy do grupy państw członkowskich Unii Europejskiej, które są najbardziej zaawansowane w procesie elektronizacji dostępu do prawa, takich jak Austria, Belgia, Dania, Hiszpania, Portugalia i Węgry.

Ustawodawca uzasadnia konieczność wprowadzenia formy elektronicznej względami usprawnienia procesu publikacji, zapewnienia powszechnego i nieskomplikowanego dostępu użytkownikom. Zmiany będą dotyczyły aktów publikowanych w takich dziennikach urzędowych, jak: Dziennik Ustaw Rzeczypospolitej Polskiej, Dziennik Urzędowy Rzeczypospolitej Polskiej „Monitor Polski", dzienniki urzędowe ministrów kierujących działami administracji rządowej, dzienniki urzędowe urzędów centralnych oraz wojewódzkie dzienniki urzędowe. Wynika to z nowo dodanego art. 2a projektu ustawy, który określa obowiązek publikacji aktów prawnych w formie dokumentu elektronicznego. Ponadto wprowadza się obowiązek prowadzenia odrębnej strony internetowej dla każdego dziennika urzędowego wydawanego w postaci elektronicznej.

Podstawą ogłoszenia aktu normatywnego lub innego aktu prawnego będzie akt w formie elektronicznej podpisany przez

upoważniony do wydania aktu organ bezpiecznym podpisem elektronicznym, w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.) weryfikowanym przy pomocy kwalifikowanego certyfikatu. Podstawą do ogłoszenia orzeczenia będzie jego odpis w formie dokumentu elektronicznego, który w swej treści będzie zawierał poświadczenie zgodności z oryginałem oraz będzie podpisany przez osobę upoważnioną do sporządzenia odpisu orzeczenia bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy kwalifikowanego certyfikatu, a także odpis orzeczenia w postaci papierowej. Powyższe zasady określa nowe brzmienie art. 15 ustawy.

Do ogłoszenia kierowane będą jedynie akty w formie dokumentu elektronicznego, opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy kwalifikowanego certyfikatu organu wydającego dziennik urzędowy, bez konieczności dołączania, jak obecnie, oryginału podpisanego przez organ wraz z trzema kopiami. Odmienne zasady dotyczyć będą:

1) aktów kierowanych do Monitora Polskiego B, który jak obecnie wydawany będzie w formie papierowej, więc przy kierowaniu aktów prawnych nie będzie wymagana forma dokumentu elektronicznego;
2) orzeczeń sądów i trybunałów, uchwał i obwieszczeń Państwowej Komisji Wyborczej oraz protokołów terytorialnych komisji do spraw referendum oraz aktów prawnych dotyczących stwierdzenia ważności wyboru Prezydenta Rzeczypospolitej Polskiej, wyborów do Sejmu i Senatu, wyborów do Parlamentu Europejskiego oraz ważności referendum ogólnokrajowego, w tym referendum zatwierdzającego zmianę Konstytucji, gdzie podstawą do ogłoszenia będzie odpis orzeczenia w formie dokumentu elektronicznego, zawierających w swojej treści poświadczenie zgodności z oryginałem oraz opatrzony bezpiecznym podpisem elektronicznym przy pomocy kwalifikowanego certyfikatu.

Powyższe zasady nie będą odnosiły się jedynie do Dziennika Urzędowego Rzeczypospolitej Polskiej „Monitor Polski B" oraz wyodrębnionych edycji dzienników urzędowych Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw zagranicznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu lub Szefa Centralnego Biura Antykorupcyjnego z aktami prawnymi zawierającymi informacje niejawne.

Istotna zmiana dotyczy także zasad ogłaszania tekstów jednolitych przez Marszałka Sejmu (art. 16). W chwili obecnej, jeżeli liczba zmian w ustawie jest znaczna lub gdy ustawa była wielokrotnie uprzednio nowelizowana i posługiwanie się tekstem jednolitym ustawy może być istotnie utrudnione, Marszałek Sejmu ogłasza tekst jednolity ustawy. Zgodnie z nową regulacja art. 16 Marszałek ogłasza tekst jednolity ustawy nie rzadziej niż raz na 12 miesięcy, o ile była ona nowelizowana, chyba że ustawa określi inny termin. Przepisy te będą odpowiednio stosowane do ogłaszania tekstów jednolitych aktów normatywnych innych niż ustawa. Teksty jednolite tych aktów ogłaszane będą przez organ właściwy do wydania aktu normatywnego a w przypadku:

1) regulaminów Sejmu i Senatu – odpowiednio marszałek Sejmu i Marszałek Senatu
2) aktów normatywnych Rady Ministrów – Prezes Rady Ministrów
3) aktów normatywnych Krajowej Rady Radiofonii i Telewizji – Przewodniczący Krajowej Rady Radiofonii i Telewizji.

Praktyka oraz działania naszego ustawodawcy w zakresie nowelizowania aktów prawnych będą najlepszym sprawdzianem

wprowadzanych zmian, gdyż w chwili obecnej wydawanie tekstów jednolitych nie odbywa się płynnie, a tym samym nie ułatwia lektury ustaw obywatelom. Przykładem mogą być ustawy podatkowe. Błędy w tekście jednolitym aktu prawnego polegające na niezgodności jego tekstu ogłoszonego w dzienniku urzędowym z tekstem aktu uwzględniającym wszystkie zmiany dokonane do czasu ogłoszenia tekstu jednolitego prostuje się w formie obwieszczenia (nowe brzmienie art. 18 ust. 1). Uchylony zostanie art. 19, który reguluje sposób redagowania dziennika urzędowego oraz zasady ustalania cen poszczególnych egzemplarzy.

Dzienniki urzędowe będą wydawane z zachowaniem pozycji w danym roku kalendarzowym (nowe brzmienie art. 20). Likwidacji ulegnie podział dziennika urzędowego na numery i strony, a więc istotne stanie się określenie nie tyle dnia wydania, ile dnia ogłoszenia aktu, którym będzie dzień ogłoszenia aktu na stronie internetowej organu wydającego dziennik urzędowy. W dotychczasowej praktyce istnieje konieczność przygotowania całego numeru dziennika urzędowego, w szczególności zebrania pewnej liczby aktów prawnych. Jak uzasadnia projektodawca, wprowadzenie postaci elektronicznej dzienników urzędowych stworzy możliwość skrócenia czasu potrzebnego do ogłoszenia aktu prawnego, co zapewni obywatelom łatwiejszy dostęp do aktów prawnych. Ogłaszanie aktów prawnych pod kolejnymi pozycjami, bez konieczności grupowania w kolejne numery dziennika urzędowego, może również rozwiązać problem wydawania w jednym dniu kilku numerów dziennika urzędowego.

Uchylony zostanie art. 20a, który stanowi obecnie podstawę do wydawania aktów w formie elektronicznej.

Rozszerzone zostaną zasady związane z archiwizacją aktów prawnych. Nowe brzmienie art. 20b nakłada na organ wydający dziennik urzędowy obowiązek przechowywania aktów normatywnych oraz innych aktów prawnych ogłaszanych w dzienniku właśnie w formie elektronicznej. Organ wydający Monitor Polski B będzie musiał przechowywać oryginały aktów ogłoszonych w tym dzienniku w postaci papierowej. Organ wydający Dziennik Ustaw i Monitor Polski powinien przechowywać po jednym egzemplarzu każdego z tych dzienników również w formie ich wydruków, poświadczonych za zgodność z oryginałem przez ten organ. Nowym rozwiązaniem będzie przekazywanie po jednym egzemplarzu Dziennika Ustaw oraz Monitora Polskiego przez organ je wydający Prezydentowi Rzeczypospolitej Polskiej oraz Bibliotece Narodowej w celu ich przechowywania. Ponadto gwarantuje się wieczyste przechowywanie tych dzienników w formie wydruków. Przewiduje się derogację art. 20c, który przewiduje wyjątek od postaci elektronicznej dla aktów kierowanych do ogłoszenia w Monitorze Polskim B.

W ustawie zmieniającej przewidziano również sytuację, w której brak jest możliwości ogłoszenia aktu w Dzienniku Ustaw, Monitorze Polskim lub dziennikach urzędowych ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych w postaci elektronicznej z przyczyny spowodowanej nadzwyczajnymi okolicznościami. W takim przypadku organ może wydać dziennik urzędowy w formie papierowej, stosując odpowiednio przepisy dotyczące wydawania dzienników urzędowych w formie elektronicznej, z tym że tak powinien ustalić warunki wydawania i rozpowszechniania dziennika, by mógł on być powszechnie i nieodpłatnie dostępny. Po ustąpieniu nadzwyczajnych okoliczności organ powinien udostępnić akt również w formie elektronicznej. Takie zasady przewiduje dodawany art. 23a.

Zmianie ulegają zasady wydawania dzienników urzędowych. Dotychczas kompetencje te Prezes Rady Ministrów zleca do Kancelarii Prezesa Rady Ministrów i Rządowego Centrum Legislacji. Nowe brzmienie art. 21 zakłada, że Dziennik Ustaw i Monitor Polski wydaje Prezes Rady Ministrów przy pomocy Rządowego Centrum Legislacji, natomiast w gestii Kancelarii Prezesa Rady Ministrów pozostaje wydawanie Monitora Polskiego B. Monitor Polski B będzie rozpowszechniany w prenumeracie oraz sprzedawany w stałych punktach sprzedaży prowadzonych przez Kancelarię Prezesa Rady Ministrów oraz w punktach sprzedaży mieszczących się w siedzibach niektórych organów administracji rządowej, sądów oraz innych jednostek. Cena będzie ustalana przez organ wydający. Postać papierowa przewidziana jest również dla wyodrębnionej edycji dziennika urzędowego z aktami prawnymi zawierającymi informacje niejawne a wydawanymi przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw zagranicznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu lub Szefa Centralnego Biura Antykorupcyjnego (art. 22 ust. 5).

Projekt zakłada, że akty normatywne i inne akty prawne podlegające ogłoszeniu będą ogłaszane w formie dokumentu elektronicznego w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.). Nałożenie na organy wydające dzienniki urzędowe obowiązku prowadzenia odrębnej strony internetowej wynika z konieczności zapewnienia tym dziennikom odpowiedniej szaty graficznej oraz wymagań technicznych. Nazwy „Dziennik Ustaw" i „Monitor Polski" oraz wzór graficzny winiety tych dzienników mogą być wykorzystywana jedynie przez organ wydający te dzienniki. Winieta obejmuje w szczególności nazwę dziennika urzędowego, wizerunek orła w koronie oraz miejsce i dzień ogłoszenia aktu prawnego. Nazwy oraz wzór graficzny nie będą mogły być wykorzystywane przez inne podmioty, w szczególności w celach handlowych w publikacjach, wydawnictwach lub innych formach upowszechniania aktów prawnych. Dotyczy to wszystkich dzienników urzędowych, wojewódzkich dzienników urzędowych oraz Monitora Polskiego B. Wzory graficzne będą określone w rozporządzeniu Prezesa Rady Ministrów. Takie zasady reguluje zmieniany art. 24.

W art. 25 uchylone zostaną ust. 1-3, które regulują zasady rozpowszechniania wojewódzkiego dziennika urzędowego.

Projektowana ustawa wprowadza również jako zasadę, iż zbiory dzienników urzędowych będą prowadzone jedynie w postaci elektronicznej – zmieniany art. 27. Tylko do zbiorów Dziennika Ustaw i Monitora Polskiego będzie wydawany skorowidz w postaci elektronicznej. Zbiór w formie papierowej będzie prowadzony dla Monitora Polskiego B oraz dla wyodrębnionej edycji dziennika urzędowego z aktami prawnymi zawierającymi informacje niejawne a wydawanymi przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw zagranicznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu lub Szefa Centralnego Biura Antykorupcyjnego.

Terenowe organy administracji rządowej oraz organy samorządu terytorialnego udostępnią w siedzibach i w godzinach pracy urzędów obsługujących te organy Dziennik Ustaw i Monitor Polski nieodpłatnie do wglądu lub do pobrania w formie dokumentu elektronicznego (nowe brzmienie art. 26). W analogiczny sposób udostępniane będą zbiory

dzienników urzędowych oraz zbiory aktów prawa miejscowego stanowionego przez powiat lub gminę. (art. 28, 28b). Wydawanie wydruków aktów normatywnych i innych aktów prawnych będzie odpłatne – zasadę taką wyraża nowe brzmienie art. 28a. Kierownik urzędu, w którym będą udostępniane do wglądu dzienniki urzędowe i zbiory aktów prawa miejscowego stanowione przez powiat lub gminę, będzie ustalał cenę arkusza wydruku normatywnego lub innego aktu prawnego tak, aby wydruki były powszechnie dostępne, a cena pokrywała wyłącznie koszty tych wydruków.

Przewidziana została również nowa delegacja dla Prezesa Rady Ministrów, który w drodze rozporządzenia określi wymagania techniczne dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne kierowane do ogłoszenia w dziennikach urzędowych oraz dla dzienników urzędowych wydawanych w postaci elektronicznej, a także środków komunikacji elektronicznej i informatycznych nośników danych używanych do udostępnienia dzienników urzędowych oraz zbiorów aktów prawa miejscowego stanowionych przez powiat lub gminę lub zawartych w nich aktów normatywnych i innych aktów prawnych.

W odniesieniu do umów międzynarodowych, których zasady ogłaszania określa ustawa z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz. U. Nr 39, poz. 443 z późn. zm.) proponowana nowelizacja tej ustawy pozostawia kierowanie umów międzynarodowych wraz z oświadczeniami rządowymi do ogłoszenia na dotychczasowych zasadach. Rozwiązanie takie wynika z faktu, iż w stosunkach międzynarodowych sporządzenie umowy w formie dokumentu elektronicznego opatrzonego bezpiecznym podpisem elektronicznym byłoby niezmiernie trudne do uzyskania. Stąd też do umów międzynarodowych stosuje się przepisy ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych jedynie w zakresie ich ogłoszenia w formie dokumentu elektronicznego w dzienniku urzędowym w postaci elektronicznej. Ponadto projektowana regulacja wprowadza zasadę, zgodnie z którą umowa międzynarodowa wraz z dotyczącymi jej oświadczeniami rządowymi, a w przypadku dokonania tłumaczenia – również z tekstem tego tłumaczenia na język polski - jest ogłaszana w formie dokumentu elektronicznego w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, z tym że podstawą do ogłoszenia jest oryginał dokumentu w postaci papierowej. Z kolei błędy w umowie międzynarodowej polegające na niezgodności między wersjami językowymi, w których umowę sporządzono, błędy w tłumaczeniu umowy międzynarodowej na język polski polegające na niezgodności tłumaczenia z umową międzynarodową w języku obcym, w którym umowę sporządzono oraz błędy w oświadczeniu rządowym dotyczącym tej umowy prostuje minister, który występował z wnioskiem o ogłoszenie tej umowy w dzienniku urzędowym.

W projekcie ustawy zmieniającej określono przepisy przejściowe dotyczące tekstów jednolitych aktów normatywnych obowiązujących w dniu wejścia nowelizacji. Będą one ogłaszane na dotychczasowych zasadach. Projektowana ustawa przewiduje też przepisy dostosowujące do nowych zasad dotyczących kierowania i ogłaszania aktów prawnych. W okresie trzech miesięcy od dnia wejścia w życie art. 1 pkt 3 projektowanej ustawy akty normatywne i inne akty prawne będą mogły być kierowane do ogłoszenia w dziennikach urzędowych na podstawie dotychczasowych przepisów. Natomiast w okresie

sześciu miesięcy od dnia wejścia w życie art. 1 pkt 3 akty prawa miejscowego stanowione przez powiat i gminę będą mogły być kierowane do ogłoszenia w wojewódzkim dzienniku urzędowym na podstawie dotychczasowych przepisów.

W celu zapewnienia odpowiednich warunków technicznych przy kierowaniu aktów do ogłoszenia projekt ustawy przewiduje, że przepisy wykonawcze wydane na podstawie art. 15 ust. 5 dotychczasowej ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych zachowają moc do dnia 31 grudnia 2011 r.

Jako datę wejścia w życie nowelizacji ustalono dzień 1 stycznia 2012 roku. Wydłużony termin ma ułatwić organom wydającym dzienniki urzędowe zakończenie procesu wydawania tych publikacji w postaci papierowej. Odrębne terminy wejścia w życie zostały przewidziane dla art. 1 pkt 2 projektu, który wprowadza zmiany w art. 9 ust. 2 dotyczącym listy aktów ogłaszanych w Dzienniku Ustaw. Dla art. 1 pkt 5 projektu, który wprowadza zmiany w art. 17 ustawy, a więc w zakresie prostowania błędów w umowach międzynarodowych oraz art. 4 projektu, który wprowadza zmiany w ustawie o umowach międzynarodowych przewidziano wejście w życie po upływie 14 dni do dnia ogłoszenia ustawy zmieniającej. Natomiast art. 1 pkt 3 projektu, który określa nowe brzmienie art. 15 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, a mianowicie określa podstawy do wydawania aktu normatywnego lub innego aktu prawnego w formie dokumentu elektronicznego, będzie obowiązywał od pierwszego dnia miesiąca następującego po miesiącu ogłoszenia ustawy zmieniającej. Taki termin wejścia w życie przewidziano dla art. 6 i 7 projektu, w którym określone są przepisy dostosowujące.

Anita Jackiewicz - prawnik z wykształcenia, specjalizuje się w prawie pracy i oraz prawie europejskim.

Polecamy

Seminarium prawno-podatkowe dla przedstawicieli jednostek ochrony zdrowia
NOWE ZASADY PODATKU VAT W OCHRONIE ZDROWIA
19 stycznia 2011 r., Warszawa

Ustawa, która wejdzie w życie 1 stycznia 2011 r., uchyla m.in. załącznik nr 4 do ustawy z 11 marca 2004 r., a tym samym reguluje na nowo zakres zwolnień od podatku VAT w publicznych i niepublicznych jednostkach ochrony zdrowia. Program niniejszego seminarium tworzy możliwość wyjaśnienia wielu kwestii prawnych, podatkowych i organizacyjnych związanych z tą sytuacją.

W PROGRAMIE:
- Nakaz stosowania VAT na niektóre usługi zdrowotne - ale które dokładnie?
- Nowe zasady opodatkowania usług medycznych.
- Aspekty praktyczne związane ze zmianą przepisów. Jak zabezpieczyć prawo do korzystania ze zwolnienia z VAT także po 1 stycznia 2011 r.? Jak zabezpieczyć pozycję podatkową placówki w sytuacji, gdy część lub całość świadczonych usług będzie podlegała/może podlegać VAT? Propozycje optymalizacji.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

e-Zdrowie - fakty i mity

Marcin Kędzierski

W długofalowym programie reform społeczno- gospodarczych określonym w Strategii Lizbońskiej, przyjętej przez Radę Europy w 2000 r., określono funkcje, jakie powinny spełniać techniki informacyjno-komunikacyjne (ang. *information and communication technologies*, ICT) dla rozwoju ochrony zdrowia. Przyszłe działania wspólnotowe w obszarze eZdrowia wyznaczają dwa strategiczne dokumenty: „eEurope 2005 - Information Society for All", zatwierdzony na szczycie w Sewilli oraz „eHealth Action Plan 2004". Dokumenty te zobowiązują państwa członkowskie UE do rozwijania usług ICT w ochronie zdrowia. Na podstawie wytycznych kierunkowych zawartych w tych dokumentach Centrum Systemów Informacyjnych Ochrony Zdrowia (CSIOZ), jako jednostka dedykowana w sprawach informatyzacji sektora zdrowotnego, opracowało założenia do „Programu Informatyzacji Ochrony Zdrowia". Na program składa się sześć kompatybilnych projektów informatycznych, z których dwa są obecnie w trakcie realizacji. Ich celem jest kompleksowe zastosowanie ICT w ochronie zdrowia w Polsce. W tym artykule skoncentruję się jedynie na obecnie realizowanych, tj.: projekcie „Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych zwany P1" oraz projekcie „Platforma Udostępniania On-line Przedsiębiorcom Usług i Zasobów Cyfrowych Rejestrów Medycznych zwany P2". Oba projekty są współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 w ramach Priorytetu VII Społeczeństwo Informacyjne – Budowa elektronicznej administracji.

Dla właściwego funkcjonowania systemów informacyjnych budowanych w ramach projektów P1 i P2 Ministerstwo Zdrowia zobowiązane jest do zapewnienia im podstaw prawnych. Podstawy te ma zapewnić projekt ustawy o systemie informacji w ochronie zdrowia, który 13 października 2010 r. został przekazany do Sejmu RP. Kilkuletnia historia projektu tej ustawy dowodzi, jak bardzo skomplikowane jest to zagadnienie i jak wiele obaw wyrażają różne środowiska społeczne w odniesieniu do przyszłościowego przetwarzania olbrzymiej ilości informacji zdrowotnych. Głównym założeniem tego dokumentu jest określenie organizacji i zasad działania systemu informacji w ochronie zdrowia, zwanego „systemem informacji - SIOZ", w którym przetwarzane będą dane niezbędne do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia. System, aby być w pełni efektywnym, będzie musiał objąć bazy danych tworzone przez podmioty obowiązane do ich prowadzenia, zawierające dane o:

- udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej,
- usługodawcach i pracownikach medycznych,
- usługobiorcach (czyli pacjentach).

System będzie gromadził i przetwarzał dane wrażliwe pacjentów, w szczególności:

- dane osobowe (stan cywilny i wykształcenie tylko w celach statystycznych),
- jednostkowe dane medyczne (czyli historia choroby pacjenta).

Kwestia danych wrażliwych pacjenta kwalifikuje się do tego, aby poświęcić jej osobny artykuł. Jest to temat szczególnie wrażliwy, zawiera bowiem informację o stanie zdrowia obywatela. Należy pamiętać, że nie zawsze

mamy do czynienia ze zwykłym przeziębieniem czy bólem zęba, ale może się zdarzyć, że np. z chorobą psychiczną czy wenerologiczną, a takie informacje pacjent ma prawo zachować wyłącznie dla siebie. Dotykamy tym samym wątku bezpieczeństwa danych, czyli umożliwienia przez pacjenta dostępu do jego danych tylko osobom do tego uprawnionym. Temat ten jest bezpośrednio powiązany z planowaną architekturą systemu i rozwiązaniami organizacyjnymi. Zarówno dostęp do danych medycznych, jak i zakres udostępnionych danych, będą zależne od usługobiorcy (autoryzacja dostępu do danych). W przypadku braku możliwości dokonania autoryzacji (przypadki nagłe, utrata przytomności itp.) usługodawca będzie mógł dokonać autoryzacji poprzez wprowadzenie do systemu danych na podstawie dowodu osobistego, paszportu lub innego dokumentu tożsamości usługobiorcy czy też dokumentu potwierdzającego uprawnienia do świadczeń opieki zdrowotnej określonego rodzaju. Zgłaszając uprzednio zastrzeżenie w systemie, pacjent będzie miał możliwość niewyrażenia zgody na dostęp do jego jednostkowych danych medycznych zgromadzonych w SIM. Autoryzacji usług medycznych dokonywał będzie każdorazowo pacjent, za pomocą nowego dowodu osobistego pl.ID. Nowy dowód pełnić będzie również rolę Karty Ubezpieczenia Zdrowotnego. O ile w Polsce podjęto decyzję o połączeniu dwóch dokumentów, o tyle w szeregu innych państw członkowskich UE z powodzeniem stosuje się dokumenty pojedynczego zastosowania. Pacjent w celu autoryzacji wykonanej usługi medycznej użyje do tego jednego z certyfikatów pl.ID. Pojawia się pytanie, jakiego dokumentu powinien używać pracownik medyczny np. lekarz? Czy do celów zawodowych powinien posługiwać się nowym dowodem osobistym, czy może powinien używać innego dokumentu, tzw. karty profesjonalisty, a może właściwym rozwiązaniem jest wykorzystanie elektronicznej Platformy Usług Administracji Publicznej (ePUAP)? Podobnych pytań, pozostających dzisiaj bez odpowiedzi, jest wiele, ale odpowiedzi na te pytania będą musiały się pojawić na etapie projektu technicznego SIM, a to już niedługo nastąpi.

System informacji w ochronie zdrowia będzie obsługiwany głównie przez Elektroniczną Platformę Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych oraz Platformę Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych. Platformy te będą korzystały z usług dostarczanych przez ePUAP. Centralnym systemem teleinformatycznym będzie System Informacji Medycznej (SIM). To SIM tak naprawdę będzie stanowił jądro SIOZ i będzie odpowiedzialny za przetwarzanie danych dotyczących udzielonych, udzielanych lub planowanych świadczeń opieki zdrowotnej, udostępnianych przez systemy teleinformatyczne usługodawców. W tym miejscu chciałbym uspokoić tych z Państwa, którzy pomyśleli, że aparat państwa będzie centralnie gromadził jednostkowe dane medyczne. Otóż absolutnie NIE!!! Dane te będą gromadzone w systemach teleinformatycznych usługodawców, natomiast SIM będzie posiadał jedynie odnośniki i referencje do danych zawartych w dokumentacji medycznej pacjenta. Prowadzenie dokumentacji medycznej w postaci elektronicznej możliwe jest już dzisiaj i wielu z usługodawców decyduje się na taką formę pracy. Od czterech lat placówki służby zdrowia mają możliwość tworzenia i archiwizowania dokumentacji medycznej w formie elektronicznej. Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej umożliwiło zakładom opieki zdrowotnej zastąpienie dokumentów papierowych elektronicznymi. Przepisy, wprowadzając takie rozwiązania, definiują także szereg dodatkowych zabezpieczeń dla dokumentacji, takich jak podpisy elektroniczne i znaczniki czasu. Ze względu na kondycję finansową placówek opieki zdrowotnej rozwiązania te stanowią główny hamulec zmian. I choć elektroniczna dokumentacja medyczna podczas jej tworzenia może być podpisana zwykłym podpisem elektronicznym, to w przypadku udostępniania jej na zewnątrz podmiotom i innym organom uprawnionym na podstawie odrębnych przepisów, a w razie śmierci pacjenta - osobie przez niego upoważnionej do uzyskiwania

dokumentacji w przypadku jego zgonu - musi być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą kwalifikowanego certyfikatu. I właśnie ten punkt jest piętą achillesową rozwiązania. Konieczność używania kwalifikowanych certyfikatów skutecznie odstrasza dyrektorów placówek opieki zdrowotnej od inwestowania w nowe technologie informacyjne. Zmiana konsultowanego rozporządzenia wprowadzającego nowe rodzaje dokumentacji medycznej przyniesie kilka pozytywnych zmian, w tym także odejście od dotychczasowych sposobów potwierdzania tożsamości na rzecz wymagań funkcjonalnych dla systemów usługodawców. Miejmy nadzieję, że będzie to zachętą i impulsem do zmiany formy prowadzenia dokumentacji medycznej przez kolejnych usługodawców. Należy bowiem podkreślić, iż projekt ustawy o systemie informacji w ochronie zdrowia zakłada, że od dnia 1 sierpnia 2014 roku dokumentacja medyczna prowadzona będzie wyłącznie w postaci elektronicznej. Wyzwanie to nie lada, zgodnie z art. 13 tegoż projektu będzie wymagać określenia:

- formatu elektronicznej dokumentacji medycznej udostępnianej przez usługodawców w SIM,
- warunków organizacyjno-technicznych zamieszczania i pobierania z SIM dokumentów elektronicznych,
- warunków organizacyjno-technicznych realizacji dostępu i pobierania danych przetwarzanych w SIM.

Samo ustrukturyzowanie dokumentacji medycznej, której rodzajów, a co za tym idzie także zakresu informacji, jest tak wiele, będzie dla Ministerstwa Zdrowia wiązało się z ogromnym nakładem pracy. Spójne komunikaty o właściwej strukturze logicznej to nadzwyczaj istotny element przyszłego systemu. Zwłaszcza że system informacji to nie tylko SIM i widoczna dla pacjenta jego funkcjonalność, jaką jest dostęp do historii choroby opartej o dane z elektronicznej dokumentacji medycznej wraz z prowadzoną terapią. To także współpraca SIM z szeregiem systemów dziedzinowych oraz rejestrów medycznych. Poprzez zastosowanie dedykowanych aplikacji udostępnione zostaną usługi wspierające dla usługodawców, płatników, aptek czy samego Ministra Zdrowia. Współpracujące systemy dziedzinowe, jak np.:

- System Rejestru Usług Medycznych Narodowego Funduszu Zdrowia,
- System Statystyki w Ochronie Zdrowia,
- System Ewidencji Zasobów Ochrony Zdrowia,
- System Wspomagania Ratownictwa Medycznego,
- System Monitorowania Zagrożeń,
- System Monitorowania Dostępności do Świadczeń Opieki Zdrowotnej,
- Zintegrowany System Monitorowania Obrotu Produktami Leczniczymi,
- System Monitorowania Kształcenia Pracowników Medycznych

będą stanowiły integralne części systemu, a ich operacyjna współpraca z SIM zapewni właściwe, sprawne funkcjonowanie całego systemu.

Niezwykle ważnym aspektem jest także funkcjonowanie w sektorze ochrony zdrowia różnych rejestrów medycznych i baz danych, które należy zintegrować. Dotychczas brakowało jasnej i precyzyjnej polityki w tym zakresie, przez co obecnie funkcjonuje szereg autonomicznych rozwiązań (różnych technicznie) niemogących ze sobą współpracować. Dlatego też w 2010 r. został opracowany dokument *„Kierunki informatyzacji ‚e-Zdrowie Polska' na lata 2010-2015"*, który został przyjęty przez Komitet Rady Ministrów ds. Informatyzacji i Łączności. Na potrzeby tego dokumentu oraz dla właściwego rozpoznania tego obszaru w 2010 roku Ministerstwo Zdrowia zleciło CSIOZ przegląd wszystkich funkcjonujących rejestrów medycznych. Wyniki tego przeglądu wyraźnie pokazują, iż w sektorze zdrowia funkcjonuje w tej chwili kilkadziesiąt różnych rejestrów medycznych. Uporządkowanie źródeł danych, tj. rejestrów medycznych, to jeden z podstawowych warunków efektywnego funkcjonowania systemu informacyjnego ochrony zdrowia. Integracja rejestrów medycznych przewidywana jest w projekcie P3 pod nazwą „Systemy związane z przebudową,

dostosowaniem, utrzymaniem i monitorowaniem rejestrów i innych zasobów ochrony zdrowia przez organy publiczne, w tym administrację państwową i samorządową – Platforma Rejestrów Ochrony Zdrowia (PROZ)", który znajduje się na liście rezerwowej projektów kluczowych POIG.

Przyjęty projekt ustawy o systemie informacji w ochronie zdrowia pozwoli Ministrowi Zdrowia na kompleksowe tworzenie i likwidację rejestrów medycznych, a także dostarczy podstaw prawnych dla ich funkcjonowania, także w odpowiednim rozporządzeniu określi procedury ich tworzenia i likwidacji, jak np.:

- w terminie 6 miesięcy od dnia wejścia w życie ustawy podmiot prowadzący rejestr/y będzie obowiązany przekazać ministrowi właściwemu do spraw zdrowia informacje o prowadzeniu oraz zakresie danych zawartych w rejestrze,
- w przypadku stwierdzenia zasadności utworzenia rejestru medycznego minister właściwy do spraw zdrowia w terminie 6 miesięcy tworzy rejestr medyczny,
- podmiot prowadzący do dnia wejścia w życie ustawy rejestr/y, jeśli nie otrzyma zgody w terminie 6 miesięcy, zmuszony będzie w ciągu miesiąca do zaprzestania ich prowadzenia oraz zniszczenia baz danych i nośników informacji w sposób uniemożliwiający ich wykorzystanie.

Minister właściwy do spraw zdrowia będzie tworzył i prowadził lub tworzył i zlecał prowadzenie rejestrów medycznych stanowiących uporządkowany zbiór danych i informacji o zachorowaniach, chorobach, stanie zdrowia, metodach leczenia, diagnozowania, monitorowania postępów w leczeniu oraz zagrożeniach związanych z występowaniem niektórych chorób.

Należy również zaznaczyć, iż ustawa jasno określa, że nadzór nad właściwym funkcjonowaniem systemu sprawuje minister właściwy do spraw zdrowia. Za administrowanie systemem informacji odpowiadać będzie jednostka właściwa w zakresie systemów informacyjnych ochrony zdrowia, która do dnia 31 marca będzie zobowiązana do przedłożenia sprawozdania z funkcjonowania systemu informacji w poprzednim roku.

Włączenie wszystkich obywateli w proces ochrony zdrowia pozwoli na znaczne obniżenie kosztów oraz kompleksowe monitorowanie udzielanych świadczeń zdrowotnych w czasie rzeczywistym. Będzie to możliwe dzięki takim funkcjom platformy e-Zdrowie, jak: EHR (elektroniczny rekord pacjenta), e-Recepty, rejestracja na wizytę on-line, elektroniczne skierowania, internetowe konto pacjenta, centralne zasoby słownikowe. Rozwój e-Zdrowia w Polsce wymaga prowadzenia spójnej polityki państwa we wdrażaniu powszechnie dostępnych usług medycznych na odległość, upowszechniania wartościowych treści na temat profilaktyki i ochrony zdrowia w internecie, jak i zapewnienia warunków dla podnoszenia poziomu wiedzy zdrowotnej u mieszkańców wraz z równoległym zdobywaniem nowych kwalifikacji i umiejętności przez pracowników sektora opieki zdrowotnej. Inicjatywy rozwijające usługi elektroniczne są również rekomendowane i w istotny sposób wspierane finansowo przez Unię Europejską. Jeśli tego teraz nie wykorzystamy, kolejna taka szansa może nam się już nie trafić. Jednak żeby tego dokonać, rozpoczęty przed laty proces informatyzacji sektora Zdrowia musi zakończyć się powodzeniem. Kluczem do sukcesów w projektach IT w administracji publicznej jest świadomość osób budujących systemy informacyjne, iż rozwiązania jakie tworzą, dedykują również dla siebie. Bez tej podstawowej świadomości brak będzie wystarczającego poziomu determinacji, który zapewni sukces i zadowolenie. Właśnie brak tej świadomości jest jednym z największych ryzyk projektowych.

Marcin Kędzierski - zastępca Dyrektora Departamentu Organizacji Ochrony Zdrowia w Ministerstwie Zdrowia.

Zmiany w podatku VAT a umowy w sprawie zamówienia publicznego. Problematyka wpływu stawki podatkowej do czasu zawarcia umowy w sprawie zamówienia publicznego

Wojciech Kaliński

W niedługim czasie nastąpi zmiana wysokości stawek podatku od towarów i usług VAT. Tego typu zmiany wywołują cały szereg konsekwencji o znaczeniu nie tylko gospodarczym, ale również i prawnym. Jedną z takich konsekwencji jest wpływ zmienionych przepisów podatkowych na postępowania oraz umowy zawierane w trybie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2010, Nr113, poz.759, ze zm.). Wiadomym jest, że zamówienia publiczne i umowy zawierane w następstwie tych procedur rządzą się specyficznymi zasadami, a możliwość zmiany zawartych w tym trybie umów jest istotnie ograniczona. Z drugiej strony sformalizowane zasady udzielania zamówień uniemożliwiają stosowane typowych w obrocie „prywatnym" zastrzeżeń dotyczących skutków ewentualnej zmiany przepisów podatkowych na treść oferty czy przyszłej umowy. Z tego względu warto przeanalizować, jakie konsekwencje prawne dla postępowań prowadzonych w trybie ustawy – Prawo zamówień publicznych oraz zawartych lub zawieranych na jej podstawie umów będą miały zmiany podatku VAT.

Zagadnienie zmiany umowy w sprawie zamówienia publicznego po zawarciu umowy w sprawie zamówienia publicznego zostało stosunkowo szeroko przeanalizowane w ramach opinii Urzędu Zamówień Publicznych dostępnej na stronie www.uzp.gov.pl. W niniejszym artykule zajmiemy się natomiast kwestią dopuszczalności uwzględnienia zmiany stawki podatku VAT do czasu zawarcia umowy w sprawie zamówienia publicznego, a zatem najpóźniej w chwili jej zawierania.

„Automatyczna" zmiana ceny w postępowaniu

Przetargi

W pierwszej kolejności należy zadać sobie pytanie, czy dopuszczalne jest uwzględnienie konsekwencji zmiany stawki podatku VAT w warunkach przetargu, a ściślej w ogłoszeniu o zamówieniu lub specyfikacji istotnych warunków zamówienia w taki sposób, by móc „automatycznie" uwzględnić zmianę podatkową w treści złożonych ofert. Problem ten dotyczył będzie w szczególności ofert złożonych przed nowelizacją przepisów podatkowych (a zatem takich, w których wykonawcy mieli obowiązek zastosować „stare", tj. dotychczasowe stawki podatkowe), jeżeli postępowanie nie zakończy się „ostatecznym" wyborem najkorzystniejszej oferty przed zmianą stawek VAT. W takim bowiem wypadku wykonawcy będą mieli obowiązek stosować inne stawki podatkowe przy konstruowaniu warunków oferty, inne zaś (najprawdopodobniej wyższe) przy wystawianiu faktur zamawiającemu. Stąd pojawia się pytanie, czy zamawiający może z góry w warunkach postępowania przewidzieć, że uwzględni zmianę wysokości podatku przy ocenie złożonych ofert, np. wyliczy najkorzystniejszą ofertę przy zastosowaniu wyższej stawki podatkowej?

Punktem wyjścia do dalszych rozważań musi być analiza stawki podatku VAT jako elementu cenotwórczego. Analizy takiej dokonał bardzo obszernie Sąd Najwyższy w uzasadnieniu uchwały z dnia 21 lipca 2006 r., sygn. III CZP 54/06, OSNC 2007/5/66, Biul. SN 2006/7/9, Wokanda 2006/12/6, M. Prawn. 2008/9/484, w której to uchwale przyjął tezę, iż „*podwyższenie z dniem 1 maja 2004 r. stawek podatku od towarów i usług za roboty budowlane, dokonane ustawą z dnia 11 marca 2004 r. o podatku*

od towarów i usług (Dz. U. Nr 54, poz. 535 ze zm.), nie uzasadnia - bez zmiany umowy zawartej przed dniem 1 maja 2004 r. - obowiązku zamawiającego zapłaty wynagrodzenia netto powiększonego o podatek od towarów i usług według podwyższonej stawki." Uzasadniając to stanowisko, Sąd Najwyższy zauważył, że: „*dla rozstrzygnięcia przedstawionego zagadnienia prawnego nie są bez znaczenia orzeczenia Sądu Najwyższego, które dotyczyły ‚cenotwórczego' charakteru podatku od towarów i usług. W orzeczeniach tych Sąd Najwyższy przyjmował zasadę, że podatek od towarów i usług jest podatkiem ‚cenotwórczym', co oznacza, iż wpływa na wysokość ceny, gdy towar lub usługa podlega opodatkowaniu. Należy wskazać na uzasadnienia uchwał z dnia 22 kwietnia 1997 r., III CZP 14/97 (OSNC 1997, nr 8, poz. 103) i z dnia 16 października 1998 r., III CZP 42/98 (OSNC 1999, nr 4, poz. 69) oraz wyroków z dnia 18 stycznia 2001 r., V CKN 193/00 (nie publ.) i z dnia 23 marca 2004 r., V CK 358/03 (nie publ.), z których nie wynika jednak, że wysokość podatku od towarów i usług bezwzględnie decyduje o wysokości ceny. Przeciwnie, w wyroku z dnia 23 stycznia 1998 r., I CKN 429/97 (OSNC 1998, nr 9, poz. 139) Sąd Najwyższy stwierdził, że podatek od towarów i usług jest elementem cenotwórczym, co oznacza tylko tyle, że sprzedawca towaru lub usługi, kalkulując cenę jest uprawniony do wliczenia do niej podatku od towarów i usług. O wysokości ceny, jaką zobowiązany jest zapłacić nabywca towaru lub usługi, decyduje jednak treść umowy ze sprzedawcą. Cena nie obejmuje podatku od towarów i usług, jeżeli umowa nie przewiduje jako elementu ceny tego podatku. Podobne stanowisko zostało wyrażone w wyroku z dnia 6 listopada 2002 r., I CKN 1158/00 (nie publ.). Z przytoczonych orzeczeń Sądu Najwyższego wynikają następujące wnioski. Po pierwsze, na gruncie poprzedniej ustawy z dnia 26 lutego 1982 r. o cenach (jedn. tekst: Dz. U. z 1988 r. Nr 27, poz. 195 ze zm.) oraz ustawy z dnia 8 stycznia 1993 r. o podatku od towarów i usług oraz o podatku akcyzowym (Dz. U. Nr 11, poz. 50 ze zm.) przyjmowano jednolity pogląd, że podatek od towarów i usług jest podatkiem „cenotwórczym" w tym sensie, iż sprzedawca towaru lub usługi, kalkulując cenę, był uprawniony do wliczenia do niej podatku od towarów i usług. Po drugie, o wysokości ceny, jaką nabywca towaru lub usługi obowiązany był zapłacić, decydowała treść umowy ze sprzedawcą. Cena nie obejmuje podatku od towarów i usług, jeżeli umowa nie przewiduje jako elementu ceny tego podatku. Po trzecie, w ramach swobody umów (art. 353[1] k.c.) strony mogą określić cenę, którą nabywca ma zapłacić sprzedawcy za towar lub usługę. Strony mogą się również swobodnie umówić co do tego, czy podatek od towarów i usług będzie elementem ceny za sprzedany towar lub usługę. Rozstrzygnięcie więc, czy strona zobowiązana jest do zapłacenia, jako elementu wynagrodzenia za wykonaną usługę, kwoty odpowiadającej podatkowi od towarów i usług należnemu od tej usługi, zależy od treści umowy zawartej przez strony. Po czwarte, art. 1 ust. 2 ustawy o cenach z 1982 r. umożliwiał przerzucenie w umowie na nabywcę ciężaru opodatkowania podatkiem od towarów i usług nabytego przez niego towaru lub usług, jednak przepis ten nie stanowił podstawy prawnej do dochodzenia od nabywcy ceny obejmującej podatek od towarów i usług, jeżeli umowa zawarta przez strony nie przewidywała jako elementu ceny tego podatku.*" Uzupełniając powyższe wywody, należy wskazać, iż Sąd Najwyższy uznał, że przytoczone rozważania zachowały aktualność także w świetle aktualnie obowiązujących przepisów.

Z przedstawionymi wywodami Sądu Najwyższego należy się zgodzić.[1] Zgodnie z brzmieniem art. 3 ust. 1 pkt 1 aktualnie obowiązującej ustawy dnia 5 lipca 2001 r. o cenach (Dz. U. Nr 97, poz.1050, ze zm.) cena oznacza

1 Por. stanowisko przedstawione w opinii prawnej Urzędu Zamówień Publicznych: Zmiana umowy w sprawie zamówienia publicznego w związku z ustawową zmianą stawki podatku od towarów i usług (VAT), dostępną na stornie internetowej www.uzp.gov.pl.

wartość wyrażoną w jednostkach pieniężnych, którą kupujący jest obowiązany zapłacić przedsiębiorcy za towar lub usługę; w cenie uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towaru (usługi) podlega obciążeniu podatkiem od towarów i usług oraz podatkiem akcyzowym. Jeśli zatem w świetle art. 2 pkt 1) pzp, pod pojęciem ceny na gruncie zamówień publicznych należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 ustawy z dnia 5 lipca 2001 r. o cenach (Dz. U. Nr 97, poz. 1050, z późn. zm.), to pojęcie „ceny", którym ustawodawca posługuje się na gruncie regulacji dotyczących zamówień publicznych oraz którym to pojęciem posługują się zamawiający w ogłoszeniach o zamówieniu oraz w specyfikacjach istotnych warunków zamówienia, obejmuje również stosowny podatek VAT. Z kolei przepisy ustawy – Prawo zamówień publicznych dają zamawiającym bardzo ograniczone kompetencje w zakresie możliwości ich wpływu na treść oferty złożonej przez wykonawców. Zgodnie bowiem z treścią art. 87 ust. 1 pzp w toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Niedopuszczalne jest prowadzenie między zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty oraz, z zastrzeżeniem ust. 1a i 2, dokonywanie jakiejkolwiek zmiany w jej treści. Możliwości te sprowadzają się do pięciu instytucji. Po pierwsze, zgodnie z art. 87 ust. 1a pzp, w postępowaniu prowadzonym w trybie dialogu konkurencyjnego w toku badania i oceny ofert zamawiający może żądać od wykonawców sprecyzowania i dopracowania treści ofert oraz przedstawienia informacji dodatkowych, z tym że niedopuszczalne jest dokonywanie istotnych zmian w treści ofert oraz zmian wymagań zawartych w specyfikacji istotnych warunków zamówienia. Bez wątpienia zarówno na gruncie tego ostatniego przepisu, jak i wcześniej cytowanego art. 87 ust. 1 pzp, zamawiający może domagać się od wykonawców wyjaśnienia, czy w złożonych ofertach skalkulowali oni wynagrodzenie w oparciu o aktualną stawkę podatku VAT, czy też wzięli już pod uwagę konieczność odprowadzenia w przyszłości wyższego podatku. Samo wyjaśnienie sposobu kalkulacji wynagrodzenia nie daje jednak podstawy do zmiany treści oferty, w szczególności podwyższenia wynagrodzenia o różnice w stawce podatkowej. Pojawia się więc pytanie, czy taką możliwość daje art. 87 ust. 1a w odniesieniu do dialogu konkurencyjnego? Przepis stanowi bowiem o możliwości sprecyzowania i dopracowania treści ofert (oraz przedstawienia informacji dodatkowych), z tym że niedopuszczalne jest dokonywanie istotnych zmian w treści ofert. Przepis ten zdaje się więc sugerować, że po złożeniu oferty dopuszczalna jest zmiana jej treści, o ile nie jest ona istotna. Z drugiej strony nieograniczone dopuszczenie takiej możliwości niosłoby ryzyko istotnych manipulacji treścią ofert i wynikami przetargów. Gdyby bowiem uznać, że wykonawca może podwyższyć oferowaną cenę o podwyżkę stawki podatku VAT, w sytuacji gdy różnice między cenami poszczególnych ofert byłyby większe niż podwyżki podatku, mogłoby to stanowić pokusę do zażądania dodatkowego wynagrodzenia nawet przez tych wykonawców, którzy w praktyce skalkulowani już w oferowanej cenie wyższy podatek. Dodatkowo gdyby zamawiający zwracał się do poszczególnych wykonawców o sprecyzowanie i doprecyzowanie ofert w różnym czasie (a nie ma prawnego obowiązku uczynić to jednocześnie), mechanizm ten mógłby służyć manipulowaniu wynikami przetargu. Z drugiej strony wydaje się, że analizy przedmiotowego przepisu nie można dokonywać w oderwaniu od jego zasadniczej części przyzwalającej zamawiającym na żądanie od wykonawców sprecyzowania i dopracowania treści ofert oraz przedstawienia informacji dodatkowych. Sprecyzowanie i dopracowanie[2] oferty to jednak nie każda jej dowolna zmiana. W szczególności nie mieści

2 Zgodnie z definicją ze Słownika języka polskiego PWN, termin „sprecyzować" oznacza „dokładnie, ściśle określić, uściślić coś", natomiast „dopracować" - „opracować coś starannie do końca".

się w tym pojęciu zmiana ceny. Trudno bowiem sprecyzować cenę poprzez jej podwyższenie (cena zasadniczo zawsze jest „sprecyzowana"), podobnie jak ją dopracować w taki sposób. Wydaje się, że uzasadnienia tej szczególnej możliwości ingerowania w treść oferty należy upatrywać w przesłance zastosowania dialogu konkurencyjnego wynikającej z art. 60b ust. 1 pkt 1 pzp: Zamawiający może udzielić zamówienia w trybie dialogu konkurencyjnego, jeżeli… nie jest możliwe udzielenie zamówienia w trybie przetargu nieograniczonego lub przetargu ograniczonego, ponieważ ze względu na szczególnie złożony charakter zamówienia nie można opisać przedmiotu zamówienia zgodnie z art. 30 i 31 lub obiektywnie określić uwarunkowań prawnych lub finansowych wykonania zamówienia. W trybie tym dopiero po negocjacjach z wykonawcami zamawiający jest wstanie określić szczegółowo przedmiot zamówienia, co powoduje, że dla wykonawców przygotowanie ofert jest szczególnie trudne. Art. 87 ust. 1a pzp daje zatem wykonawcom szanse na poprawę, a konkretnie sprecyzowanie, dopracowanie oferty, tudzież przedstawienie informacji dodatkowych, ale w zakresie technicznej strony oferty. Nie wydaje się natomiast, by na podstawie tego przepisu wykonawcy mogli podwyższyć cenę ofertową.

Druga możliwość ingerencji w treść oferty dotyczy poprawienia przez zamawiającego oczywistej omyłki pisarskiej. Ten przepis w większości przypadków nie może znaleźć zastosowania do zmiany wysokości ceny ofertowej w zakresie obejmującym skorygowanie wysokości stawki podatku VAT. W takim bowiem wypadku nie ma mowy o oczywistej omyłce pisarskiej, lecz ewentualnie o złej kalkulacji ceny (choć w szczególnych sytuacjach nie można z góry wykluczyć pomyłki w zakresie stawki jako pomyłki pisarskiej). W ten sam sposób przedstawia się kwestia trzeciego przypadku dopuszczalnej ingerencji zamawiającego w treść oferty, a mianowicie poprawianie oczywistych omyłek rachunkowych (art. 87 ust. 2 pkt 2 pzp). Także i czwarty przypadek dopuszczalnej ingerencji - inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty (art. 87 ust. 2 pkt 3pzp) - zasadniczo nie będą stanowić podstawy do podwyższenia ceny oferty w celu jej dostosowania do przyszłej stawki VAT. Zasadniczo, gdyż można sobie wyobrazić szczególną sytuację, w której zamawiający mógłby na tej podstawie skorygować cenę. Jeśli bowiem w warunkach specyfikacji istotnych warunków zamówienia zamawiający nakaże wykonawcom uwzględnienie w ramach cen ofertowych podwyższonych stawek podatku VAT, a następie, analizując treść oferty, stwierdzi, że wykonawca tego nie uczynił, mamy do czynienia z niezgodnością oferty ze specyfikacją istotnych warunków zamówienia. Przyjmując, że zmiana ceny w zakresie stawki podatku VAT nie musi wiązać z istotną zmianą oferty[3], dokonanie takiej zmiany oferty byłoby teoretycznie możliwe. Jednak w praktyce taka sytuacja jest mało prawdopodobna – zamawiający musiałby na podstawie analizy samej oferty stwierdzić, że w ramach wynagrodzenia netto[4] nie została uwzględniona przewidywana podwyższona stawka

3 Por. szerzej na ten temat - opinia UZP znajdująca się na stronie www.uzp.gov.pl.

4 A nie brutto – składając ofertę wykonawca musi bowiem zastosować stawkę podatku VAT zgodną z obowiązującymi przepisami, a zatem cenotwórcze aspekty przewidywanej zmiany stawki VAT winno się uwzględnić w cenie netto. W przeciwnym wypadku wykonawca naraża się na zarzut błędu w obliczeniu ceny w następstwie zastosowania niewłaściwej, w chwili składania oferty, stawki podatku VAT - tak Krajowa izba Odwoławcza w wyrokach z dnia 07.01.2010 KIO/UZP 1845/09; 18.02.2010 KIO/UZP 681/09; 09.06.2009 KIO/UZP 1940/09; 24.03.2009 KIO/UZP 282/09; 21.11.2008 KIO/UZP 1258/08; 15.07.2008 KIO/UZP 668/08. W orzecznictwie można jednak spotkać poglądy przeciwne – por. wyrok KIO z 12.08.2009 KIO/UZP 987/09 oraz z 20.07.2010 KIO/UZP 1427/10 i 1430/10.

podatku VAT. Jest to możliwe co najwyżej teoretycznie w razie zaistnienia jakiś szczególnych okoliczności.

Piątą możliwość swoistej korekty ceny ofertowej ustawodawca przewidział w art. 91 ust. 3a pzp, zgodnie z którym, jeżeli złożono ofertę, której wybór prowadziłby do powstania obowiązku podatkowego zamawiającego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami. Ponadto w przepisach art. 91 ust. 4-6 pzp przewidziano procedury postępowania, w tym zmiany cen ofertowych spowodowanych niemożnością wyboru najkorzystniejszej oferty oraz dodatkowo w ramach regulacji art. 91a i nast. pzp - aukcje elektroniczną jako mechanizm swoistego rodzaju „dogrywki" między wykonawcami, który to mechanizm również finalnie może doprowadzić do zmiany treści złożonych ofert, w tym do zmiany oferowanej ceny.

Analiza powyższych przepisów prowadzi do wniosku, że zmiana ceny podanej w ofercie wykonawcy jest możliwa tylko w szczególnych przypadkach, w których przepis dopuszcza taką możliwość. W pozostałych sytuacjach zmiana ceny ofertowej stanowiłaby naruszenie zasad udzielania zamówień publicznych. Konstatacja ta prowadzi do wniosku, że niedopuszczalne było postanowienie specyfikacji istotnych warunków zamówienia, w którym do porównania złożonych ofert zamawiający przeliczyłby ceny ofertowe o wskaźnik wzrostu stawki podatku VAT. Również nie wydaje się możliwe, by zamawiający mógł uwzględnić zmianę stawki podatku VAT w ramach wzoru matematycznego, w oparciu o który ustala punktację poszczególnych ofert w ramach kryterium ceny. Dodanie do wzoru takiego przeliczenia stawki podatku VAT oznaczałoby coś więcej niż tylko przedstawienie w postaci wzoru kryterium oceny ofert, a na to przepisy ustawy nie pozwalają. Dodatkowo przeliczenie stawki podatku VAT mogłoby doprowadzić do całkowitego wypaczenia wyników przetargu, jeżeli uznamy, że stanowisko Krajowej Izby Odwoławczej[5] stwierdzające, że zamawiający nie jest uprawniony do weryfikowania prawidłowości zastosowanych przez wykonawców stawek podatku VAT i winien brać pod uwagę ceny brutto, jest prawidłowe. W takim bowiem przypadku zamawiający zmieniałby ceny tylko tych ofert, w których wykonawcy zastosowali zmieniające się stawki podatku VAT, bądź też stosowałby różne współczynniki w zależności od przyjętej przez wykonawcę stawki podatkowej.

Zamówienia z wolnej ręki

W przypadku zamówieniu z wolnej ręki sytuacja przedstawia się zdecydowanie prościej. Wraz z zaproszeniem do negocjacji zamawiający przekazuje informacje niezbędne do przeprowadzenia postępowania, w tym istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy lub wzór umowy (art. 68 ust. 1 pzp). Wykonawca uczestniczący w tym trybie postępowania nie ma obowiązku złożenia oferty, a zainteresowane strony prowadzą negocjacje zmierzające do zawarcia umowy w sprawie zamówienia publicznego. Wielu zamawiających domaga się jednak od wykonawców złożenia oferty, która następnie stanowi punkt wyjścia do dalszych negocjacji. Praktyka ta, jakkolwiek nieprzewidziana przepisami ustawy, nie jest z nią sprzeczna. Tyle że oferta w zamówieniu z wolnej ręki nie wywołuje

5 Wyrok KIO z 12.08.2009 KIO/UZP 987/09 oraz z 20.07.2010 KIO/UZP 1427/10 i 1430/10.

tak daleko idących konsekwencji prawnych, jak ma to miejsce w przypadku przetargu. Oferta taka jest w istocie jedną z wielu propozycji negocjacyjnych, które pojawią się w toku negocjacji. Nie jest ona porównywana, jej ewentualne uchybienia nie wpływają na dalsze uczestnictwo wykonawcy w postępowaniu (pomijając aspekt wykluczenia z postępowania w związku z treścią art. 68 ust. 2 pzp), może być zmieniona w toku negocjacji. Tak więc negocjując warunki umowy w sprawie zamówienia publicznego, możliwe jest uzgadnianie wszystkich aspektów tej umowy, łącznie z wysokością wynagrodzenia wykonawcy i wysokości zastosowanej przy jego kalkulacji stawki podatku VAT. Jeśli więc okaże się w toku negocjacji, że stawka podatku VAT może ulec zmianie, albo że umowa zostanie zawarta w terminie, który powodować będzie konieczność rozliczeń z zamawiającym w oparciu o zmienioną stawkę podatkową, okoliczność ta może zostać uwzględniona w toku negocjacji bez konieczności zamieszczenia szczególnych zapisów w zaproszeniu do negocjacji.

Zmiana stawki podatkowej przy zawieraniu umowy

Przetargi

Kolejne zagadnienie wymagające analizy to kwestia dopuszczalności uwzględnienia zmiany stawki podatkowej w chwili zawierania umowy w sprawie zamówienia publicznego. Rozważenia wymagają tu dwie kwestie: 1) sytuacja, w której wykonawcy składali oferty w oparciu o inną stawkę podatkową niż ta, która będzie obowiązywała przy rozliczeniu umowy (co do zasady - wystawieniu faktury VAT) oraz 2) sytuacja, w której wykonawcy lub wykonawca zastosował inną stawkę podatku niż obowiązująca w chwili składania ofert.

Zmiana stawki przed zawarciem umowy, a po złożeniu ofert

Analizując sytuację, w której zmiana stawki podatkowej następuje w pomiędzy złożeniem oferty a podpisaniem umowy, wyróżnić można dwie grupy zdarzeń: pierwszą, w której wykonawcy nie wiedzieli o możliwej zmianie stawki podatkowej oraz druga, w której o zmianie takiej i jej dacie wiedzieli. Jeśli chodzi o pierwszą z możliwości, ma ona zasadniczo charakter teoretyczny, zważywszy na przebieg procesu legislacyjnego w zakresie zmian stawek podatkowych. Z drugiej jednak strony nie można zapominać o sytuacjach, w których zmiany podatkowe następować będą w oparciu o zmiany aktów wykonawczych oraz o przypadki bardzo długiej procedury oceny ofert, związanej np. z kilkukrotnym przedłużaniem terminu składania ofert. W takiej sytuacji może zdarzyć się, że oferta została złożona przy uwzględnieniu innej stawki podatkowej niż ta, która winna być zastosowana przy zawieraniu umowy. Oczywiście wniosek ten musi opierać się na informacjach, które można znaleźć w treści oferty (podanie przez wykonawcę w ofercie zastosowanej stawki podatkowej, czy zamieszczenie w ofercie informacji o cenie netto i brutto, które pozwalają na jednoznaczne wyliczenie wysokości stosowanej stawki podatkowej[6]). Jeśli na podstawie oferty nie można byłoby ustalić wysokości zastosowanej stawki podatkowej, ustalenia dokonywane na podstawie późniejszych informacji wykonawcy mogą zostać potraktowane jako naruszenie zasad udzielania zamówień oraz element negocjacji ceny z wybranym wykonawcą i to na niekorzyść zamawiającego.

Jedynym przepisem, jaki reguluje relację treści oferty do treści umowy zawieranej w rozstrzygnięciu przetargu, jest art. 140 ust. 1 i 3 pzp. Zgodnie z tym przepisem 1. - zakres

6 Co zasadniczo nie będzie mogło znaleźć zastosowania w przypadku, gdy w ramach przedmiotu zamówienia różne części świadczenia wykonawcy podlegają opodatkowaniu różnymi stawkami podatkowymi.

świadczenia wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie oraz 3. - umowa podlega unieważnieniu w części wykraczającej poza określenie przedmiotu zamówienia zawarte w specyfikacji istotnych warunków zamówienia. Zmiana stawki podatku VAT na „aktualniejszą" nie zmienia zakresu świadczenia wykonawcy (pozostaje ono tożsame), ani też nie wykracza poza zakres przedmiotu zamówienia. Tym samym uwzględnienie zmiany stawki podatkowej na etapie zawierania umowy nie stanowi naruszenia art. 140 pzp.

Z powyższych względów wydaje się, że uwzględnienie zmiany stawki podatkowej na etapie zawierania umowy byłoby, w świetle obowiązujących przepisów, dopuszczalne, zwłaszcza, mając na uwadze wywody zawarte w opinii dostępnej na stronach internetowych Urzędu Zamówień Publicznych, z których wynika, że po zawarciu umowy zmiana wynagrodzenia spowodowana zmianą stawki podatku VAT stanowi nieistotną zmianę umowy w sprawie zamówienia publicznego. Z tego względu ewentualna wykładnia zmuszająca do zawierania umowy na warunkach wynikających wprost z oferty, a następnie dokonywania zmiany zawartej umowy niezwłocznie po jej zawarciu, przy jednoczesnym niedopuszczaniu dokonania takiej samej zmiany na etapie zawierania umowy, nie wydaje się racjonalnie uzasadniona.

Oczywiście dokonanie takiej zmiany uznać należy za niedopuszczalne w sytuacji, w której zmiana taka – gdyby zastosować ją na potrzeby oceny ofert - mogłaby skutkować zmianą w zakresie wyboru najkorzystniejszej oferty, o ile z warunków przetargu nie wynikałoby, że mechanizm ten zostałby zastosowany do każdego wybranego wykonawcy oraz przy założeniu, że wszyscy wykonawcy zastosowali nieaktualną stawkę podatku VAT. Czynność taka oznaczałby bowiem manipulację wynikami przetargu, co w kontekście nierównego traktowania uczestników postępowania skutkowałoby naruszeniem przepisów dotyczących udzielania zamówień i zaistnieniem podstawy do unieważnienia zawartej umowy.

Jeśli chodzi o drugą z przedstawionych grup możliwości, tj. taką, w której wykonawcy, składając oferty, wiedzieli o zmieniającej się stawce VAT, zasadniczo nie różni się ona istotnie od pierwszej z grup. Również i w tym przypadku, co do zasady, wykonawcy winni złożyć ofertę zgodną z przepisami (w tym podatkowymi) obowiązującymi w chwili składania ofert. Nie jest bowiem teoretycznie wykluczone, że do wyboru najkorzystniejszej oferty i zawarcia umowy w sprawie zamówienia publicznego dojdzie jeszcze przed zmianą przepisów podatkowych. Istotne jest, by specyfikacja istotnych warunków zamówienia określała jasne zasady, w jaki sposób wykonawcy winni kalkulować oferty i jakie stawki podatkowe zastosować. Uniknie się w ten sposób sytuacji, w której część wykonawców uwzględni w oferowanej cenie zmiany stawek podatkowych, a część nie.

Zmiana stawki przed złożeniem ofert

Przypadek, w którym wykonawca składa ofertę przy zastosowaniu nieaktualnej stawki VAT w sytuacji, gdy winien był zastosować stawkę nową, należy traktować w zależności od rodzaju i przyczyn popełnionego uchybienia. Jeżeli zmiana podatkowa polega na tym, że określony produkt „przesuwa się" z jednej obowiązującej stawki podatkowej do innej, traktować raczej należy jako błąd w obliczeniu ceny. Na podstawie oferty nie sposób bowiem ustalić, czy jest to oczywista omyłka wykonawcy, czy też „manewr" służący obniżeniu ceny oferowanego towaru lub usługi. Oczywiście orzecznictwo KIO nie wyjaśnia, jak w takim wypadku winien postąpić zamawiający. Dominująca do niedawna linia orzecznictwa traktowała takie uchybienie jako błąd w obliczeniu ceny, skutkujący odrzuceniem oferty. Ostatnio zaczyna się

jednak pojawiać pogląd odmienny, uznający, że zastosowanie prawidłowej stawki podatku VAT to problem wykonawcy, a zatem błędnie obliczony podatek obniży po prostu dochód wykonawcy z danego projektu. W zależności od przyjętej koncepcji zamawiający winien albo odrzucić ofertę, albo poddać ją zwykłej ocenie. Jeśli zamawiający wybrał drugie rozwiązanie, nie może jednak, co do zasady, przyjąć przy zawieraniu umowy innej stawki podatkowej niż wskazana w ofercie. Skoro bowiem ryzyko zastosowania błędnej stawki podatku VAT obciąża wykonawcę, nie ma podstaw do niweczenie tego ryzyka na etapie zawierania umowy.

Nie jest natomiast wykluczone, by zastosowania złej stawki podatkowej nie można było potraktować jako omyłki rachunkowej. Będzie to jednak możliwe jedynie w przypadku, gdy z innych części oferty wynikać będzie, że powinna była zostać zastosowana inna stawka podatkowa niż ostatecznie przyjęta w ofercie.

W sytuacji, w której uchybienie wykonawcy polega na zastosowaniu „nieistniejącej" stawki podatkowej, czyli najczęściej zastosowaniu „starej", uchylonej już stawki zamiast stawki „nowej", tego typu błędy raczej należy traktować jako oczywiste omyłki i przeliczać oferowane ceny na potrzeby oceny i porównania ofert zgodnie z zasadami określonymi w art. 87 ust. 2 pkt 2 pzp.

Zamówienia z wolnej ręki

W przypadku zamówień z wolnej ręki analizowany problem w praktyce nie występuje. Ewentualne hipotetyczne sytuacje, w których strony osiągnęłyby całkowity kompromis przy kalkulowaniu ceny przy zastosowaniu błędnych stawek podatku VAT, a kwestia ta zostałaby podniesiona bezpośrednio przed zawarciem umowy w sprawie zamówienia publicznego, należy traktować analogicznie jak w przypadku sytuacji omówionych na przykładzie przetargów.

Najbliższe miesiące pokażą najprawdopodobniej szereg problemów związanych ze zmianami podatku VAT na gruncie systemu zamówień publicznych. Rozważając różne drogi „wyjścia" z tych problemów należy jednak pamiętać, że co do zasady zmiana umowy w sprawie zamówienia publicznego czy też uwzględnienie innej stawki podatkowej przy zawieraniu umowy nie jest obowiązkiem, lecz prawem zamawiającego. Dlatego wykonawcy muszą liczyć się z tym, że w razie sporu w większości przypadków nie będą mieli roszczenia do zamawiającego o zmianę umowy.

Dr Wojciech Kaliński - asystent w Katedrze Prawa Cywilnego Uniwersytetu Jagiellońskiego, wspólnik w kancelarii Maruta i Wspólnicy sp. j.

Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne – część IV

Wojciech Kaliński

Rekomendacja 1: planowanie rozwoju systemów informatycznych w organizacji Zamawiającego

Przechodząc do omawiania poszczególnych rekomendacji Urzędu Zamówień Publicznych, zaczynamy od pierwszej z nich, dotyczącej planowania rozwoju systemów informatycznych. Urząd wskazuje, że u źródła jej powstania leży uniknięcie budowy rozwiązań wadliwych, do których zalicza się:

- powstanie systemów wyspowych / brak interoperabilności systemów, tj. zdolności systemów do wymiany danych z innymi systemami,
- pokrywanie się funkcjonalności odrębnych systemów,
- rozproszenie i/lub powielenie zbiorów danych lub ich części prowadzące do niespójności,
- powstanie systemów niespójnych funkcjonalnie w efekcie stopniowego, nieprzemyślanego dodawania coraz większej liczby funkcji pozostających w luźnym związku z zasadniczym zadaniem systemu.

Z powyższymi zastrzeżeniami nie sposób się nie zgodzić. Brak odpowiedniego planowania rozwoju systemów informatycznych może rzeczywiści prowadzić do chaotycznych, nieprzemyślanych działań i tworzenia rozwiązań niezależnych od tego, co do tej pory zrobiono w ramach struktur zamawiającego, tudzież tworzenia rozwiązań, które w przyszłości nie będą mogły być rozwijane jako zalążek bardziej złożonych i rozbudowanych systemów, które realizować będą kolejne zadania spoczywające na zamawiającym. Z tego względu tworzenie rozwiązań informatycznych, które są zamknięte i nie mogą dokonywać wymiany danych, pokrywają swoje funkcjonalności itp., rzeczywiście należy uznać za błąd. Jedyne co należałoby dodać do powyższych wniosków, to stwierdzenie, że przedmiotowe działania należy uznać za wadliwe, o ile nie wynikają z uzasadnionych i obiektywnych przyczyn. W szczególnych bowiem przypadkach brak interoperabilności może być efektem pewnej strategii, czy wynikać z obiektywnych potrzeb zamawiającego. W takim przypadku, o ile decyzja o takiej właśnie konstrukcji systemu została poprzedzona odpowiednimi analizami, trudno postawić będzie zamawiającemu zarzut niewłaściwego postępowania. Raz jeszcze należy jednak podkreślić, że takie sytuacji powinny mieć miejsce zupełnie wyjątkowo, być dobrze umotywowane i nie mogą prowadzić do powstania zasady.

Rekomendacja 1.1.

Na bazie powyższych zastrzeżeń powstała pierwsza z rekomendacji, rekomendacja organizacyjna, zgodnie z którą zamawiającym zaleca się opracowanie tzw. polityki rozwoju systemów informatycznych, czyli dokumentu, który winien określać zasady, jakimi zamierza kierować się zamawiający w rozwoju systemów informatycznych. Rekomendacje UZP zawierają stosunkowo szczegółowe wytyczne dotyczące zawartości takiego dokumentu, jak np. zasady kształtowania architektury systemu; zasady określania i egzekwowania wymagań jakościowych, wymagania względem zdolność systemów do wymiany danych z innymi systemami (interoperabilność systemów), zakres praw przenoszonych przez wykonawcę na zamawiającego w toku realizacji zamówień na systemy informatyczne itp. Sama rekomendacja i zawarte

w niej zalecenia raczej nie powinny budzić zastrzeżeń. Stworzenie w ramach organizacji zamawiającego spójnych zasad dotyczących wymagań stawianych systemom informatycznym, uporządkowanie w tym zakresie wewnętrznej polityki zamawiającego jest działaniem jak najbardziej pożądanym. Z tego względu w odniesieniu do tej rekomendacji należy przedstawić bardziej ogólne uwagi. Po pierwsze, z punktu widzenia wykonania omawianej rekomendacji nie ma znaczenia, czy stworzony przez zamawiającego dokument będzie określony jako polityka rozwoju, czy w jakikolwiek inny sposób. Sformułowania rekomendacji zdają się bowiem sugerować, że chodzi o stworzenie konkretnie nazwanego opracowania. Istotna jest jednak jego merytoryczna zawartość, a nie nazwa. Jeśli więc zamawiający dysponują odpowiednimi dokumentami, lecz inaczej nazwanymi, stanowiącymi część większej całości itp., skupić winni się na ustaleniu, czy zawiera on wszystkie niezbędne elementy wymagane rekomendacjami UZP, a nie jego wyodrębnianiu czy zmianie nazwy.

Druga ogólna uwaga wiązać się będzie z analizą kolejnych rekomendacji, sprowadzając się w tym momencie do stwierdzenia, że zapisy polityki z jednej strony winny zawierać racjonalne wymagania, z drugiej zaś nie powinny stanowić wewnętrznego gorsetu paraliżującego działania struktur zamawiającego. Wprowadzenie zbyt rygorystycznych zasad bądź reguł, które nie będą nadawały się do zastosowania w określonych sytuacjach lub w przypadku pewnych systemów informatycznych, może powodować z jednej strony brak zainteresowania wykonawców organizowanymi przez zamawiającego przetargami, z drugiej zaś obawy w organizacji zamawiającego przed zmianą zbyt daleko idących wymagań zawartych w polityce. Wszystko to powoduje, że polityka winna być pisana w oparciu o dobrą wiedzę dotyczącą rynku IT tak, by zarówno stanowiła istotny element rozwojowy organizacji zamawiającego, jak i nie była hamulcem tego rozwoju oderwanym od rzeczywistości rynkowej. W tym ostatnim przypadku źle napisana polityka może stanowić wygodne uzasadnienie dla nierozstrzygniętych postępowań przetargowych, a w skrajnym przypadku pośrednim uzasadnieniem stosowania trybu zamówienia z wolnej ręki na podstawie art. 67 ust. 1 pkt 4 pzp (*w prowadzonych kolejno postępowaniach o udzielenie zamówienia, z których co najmniej jedno prowadzone było w trybie przetargu nieograniczonego albo przetargu ograniczonego, nie wpłynął żaden wniosek o dopuszczenie do udziału w postępowaniu, nie zostały złożone żadne oferty lub wszystkie oferty zostały odrzucone na podstawie art. 89 ust. 1 pkt 2 ze względu na ich niezgodność z opisem przedmiotu zamówienia, a pierwotne warunki zamówienia nie zostały w istotny sposób zmienione).*

Rekomendacja 1.2.

Od „polityki rozwoju systemów informatycznych" należy odróżnić drugi dokument, którego opracowanie zalecane jest w rekomendacjach UZP, a mianowicie „planu rozwoju systemów informatycznych". Plan, zgodnie z rekomendacjami, „*jest w stosunku do ‚polityki' dokumentem o charakterze wykonawczym i powinien zawierać m.in.: określenie portfeli projektów z zakresu informatyzacji, określając ich wzajemne uzależnienia i powiązania, budżet projektów i ich portfeli oraz zasoby organizacji niezbędne do ich realizacji, harmonogram realizacji projektów i ich portfeli*" itp. Rekomendacja 1.2. jest więc ścisłą kontynuacją zaleceń zawartych w rekomendacji 1.1. Oczywiście nie ma przeciwwskazań, by wszystkie wymagane elementy zawrzeć nie w dwóch, a jednym dokumencie. Istotne jest bowiem to, by w ramach struktur zamawiającego istniał dokumentu regulujący kwestie

wskazane w rekomendacjach 1.1. i 1.2., a jak on się będzie nazywał, czy będzie to jeden, czy więcej dokumentów, nie ma absolutnie znaczenia. Nie jest również konieczne, by dokumenty (dokument) te zostały opracowane przez samego zamawiającego. Możliwe jest ich opracowanie zarówno przy współudziale zewnętrznych konsultantów, czy wręcz zlecenie jego opracowania zewnętrznej firmie w przypadku, gdy zamawiający nie dysponuje dostateczną wiedzą lub niezbędnymi zasobami. Jeśli opracowanie polityki lub projektu nie będzie realizowane siłami zamawiającego, istotne jest zagwarantowanie sobie przez zamawiającego, by uczestniczący w projekcie konsultanci byli maksymalnie niezależni od producentów i dostawców rozwiązań informatycznych, tak by opracowane przez nich dokumenty były w jak największym stopniu neutralne technologicznie i nie preferowały żadnych konkretnych rozwiązań. W przeciwnym wypadku może dojść do naruszenia zasady konkurencyjności i równego traktowania wykonawców oraz do uzależnienia zamawiającego od określonego rodzaju technologii bądź rodzaju rozwiązań. Jeśli nawet sytuacja nie doprowadzi do konieczności udzielania zamówień z wolnej ręki, czyli uzyskania efektu całkowicie przeciwstawnego założeniem rekomendacji, to skutkiem może być konieczność dokonywania przetargów w wąskiej grupie dystrybutorów określonego producenta, co również nie jest rozwiązaniem optymalnym.

Rekomendacja 1.3.

Ta ostatnia spośród rekomendacji dotyczących planowania rozwoju systemów informatycznych w organizacji Zamawiającego może budzić najwięcej wątpliwości. Zgodnie z jej treścią „*planując udzielanie zamówień na dalszy rozwój istniejących już systemów informatycznych lub administrację nimi, należy uwzględnić czas niezbędny na przejęcie wiedzy przez nowego wykonawcę. Okres przekazywania wiedzy powinien zostać wyraźnie określony i wskazany w SIWZ i umowie z wykonawcą w adekwatnym do tego zadania okresie czasu poprzedzającym zakończenie umowy.*" Szczegółowa analiza tej problematyki zostanie przedstawiona w rekomendacji regulującej sposób realizacji tego obowiązku. W tym miejscu należy jedynie zasygnalizować, że przekazywanie wiedzy między wykonawcami konkurującymi miedzy sobą jest w praktyce ogromnie problematyczne. Żaden z wykonawców nie jest bowiem zainteresowany przekazywaniem części swojego know-how innemu podmiotowi, zwłaszcza takiemu, z którym konkuruje w różnych postępowaniach. Problemu nie rozwiązuje nawet argument, że obowiązek przekazania wiedzy dotyczyć będzie konkretnego wykonawcy, który wygrał postępowanie u danego zamawiającego. Trzeba bowiem pamiętać, że uzyskanie wiedzy nt. rozwiązań konkurenta w ramach jednego przetargu i jednego projektu stwarza szanse na złożenie konkurencyjnej oferty w innych postępowaniach, gdzie rozwiązania obydwu konkurentów ścierają się z sobą. Ponadto, postawienie wymagania przekazania wiedzy między dotychczasowym a ewentualnym nowym wykonawcą oznacza, że w ramach oferowanej ceny wykonawcy kalkulować muszą koszt przekazania wiedzy nowemu wykonawcy, a w kolejnym przetargu startujący uczestnicy uwzględniają w ramach ceny oferty koszty „nabycia" stosownej wiedzy od swego poprzednika. Takie rozwiązanie powoduje jednak stworzenie nie do końca konkurencyjnych warunków postępowania. Dotychczasowy wykonawca nie musi bowiem kalkulować w ramach swojej oferty kosztów „przekazania" wiedzy, a zatem może zaoferować niższą cenę. Co prawda, koszty przekazania wiedzy, co do zasady, nie są duże, jednak w sytuacji, gdy ceny oferowane przez wykonawców nie są znacząco różne, brak konieczności kalkulacji jednego z elementów

cenotwórczych może mieć istotne znaczenie. Inny problem wiąże się ze sposobem zrealizowania rekomendacji UZP w zakresie przekazywania wiedzy. Kwestia ta zostanie omówiona w ramach dalszych rekomendacji. Wymóg rekomendacji uwzględniania czasu niezbędnego na przejęcie wiedzy przez nowego wykonawcę oznacza dla zamawiających po pierwsze większe koszty zawieranych umów, po drugie konieczności odpowiedniej organizacji procesu przetargowego. Jak zauważa się w rekomendacjach: „*przejęcie wiedzy o konstrukcji i działaniu systemu informatycznego jest zawsze procesem wymagającym odpowiedniej ilości czasu, zależnej przede wszystkim od wielkości i złożoności systemu, ale także wielkości zespołu, umiejętności i doświadczenia oraz od sprawnego przepływu informacji od dotychczasowego wykonawcy. W skrajnych przypadkach jest to proces trwający wiele miesięcy.*" Mając na uwadze te uwarunkowania, zamawiający muszą ogłaszać przetargi na tyle wcześnie, by rozstrzygać postępowania i zawierać umowy z nowymi wykonawcami nawet na kilka miesięcy przed zakończeniem umowy łączącej zamawiającego z dotychczasowym wykonawcą. To uwarunkowanie wskazuje na jeszcze jeden mechanizm „antykonkurencyjny" wynikający z rekomendacji UZP. Otóż kalkulując cenę ofertowa w kolejnym przetargu dotychczasowy wykonawca, który ma zawartą umowę z zamawiającym, wie, że jeśli nie wygra, nie będzie musiał przekazywać wiedzy. W efekcie potencjalny koszt przekazania wiedzy kolejnemu wykonawcy dotychczasowy wykonawca może sobie zaliczyć na poczet ceny nowej oferty, znajdując kolejną pozycję pozwalającą zaoszczędzić pewnych wydatków. W efekcie przedstawione uwarunkowania pokazują, że pewne założenia rozszerzenia konkurencyjności postępowań o udzielenie zamówień publicznych mogą powodować wręcz odmienne skutki.

Dr Wojciech Kaliński - asystent w Katedrze Prawa Cywilnego Uniwersytetu Jagiellońskiego, wspólnik w kancelarii Maruta i Wspólnicy sp. j.

Zapraszamy do udziału

WARSZTATY
METODY POMIARU ROI/TCO W PRAKTYCE INWESTYCJI INFORMATYCZNYCH

Wiedza dotycząca ROI/TCO to dziś podstawowy drogowskaz w trudnym świecie inwestycji IT. Każdy dyrektor i menedżer zajmujący się problematyką zakupów informatycznych musi rozstrzygać dziś o tym, czy warto dokonać inwestycji, jakie są alternatywne opcje uzyskania efektów, jaki jest całkowity koszt rozważanego przedsięwzięcia.

Zależność jest prosta. Im więcej na IT wydaje Twoja firma, tym Twoje decyzje inwestycyjne silniej wpływają na wartość spółki. Czy Twoją firmę stać na błędne decyzje w inwestycjach IT? Jeśli odpowiedź brzmi „nie", gorąco zapraszamy do uczestnictwa w naszym szkoleniu. Poznasz na nim koncepcje i narzędzia, dzięki którym będziesz realnie podnosił wartość firmy. Efekty Twoich rekomendacji mają mierzalny wpływ zarówno na Twoją firmę, jak i na Twoją karierę – przekonasz się na naszym warsztacie.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Wyrok Krajowej Izby Odwoławczej z 2 marca 2010 r., sygn. akt KIO/UZP 184/10

Wojciech Kaliński

1. (...) Nie jest dopuszczalne i możliwe zawarcie z góry w specyfikacji istotnych warunków zamówienia i we wzorze umowy zastrzeżenia, iż umowa obejmuje zakres prac, który obojętnie z jakich przyczyn został pominięty na etapie projektowania. Lub też obejmuje bez obustronnego porozumienia zakres wszelkich prac dodatkowych czy zamiennych, wynikający z ujawnionych w trakcie budowy wad projektu oraz wynikających ze znacząco odmiennych warunków geologiczno-gruntowych niż zakładane przy opracowaniu dokumentacji projektowej. Taki rozszerzony zakres zamówienia i postanowienia umowy byłyby nieważne z mocy art. 140 ust. 3 ustawy Pzp w związku z art. 58 §1 K. c. jako wykraczające poza określenie przedmiotu zamówienia w SIWZ.

2. Izba nie podziela poglądu zamawiającego, iż wykonawca dobrowolnie może przejąć wszelkie obowiązki ustawowe spoczywające na drugiej stronie umowy, a więc i odpowiedzialność. Skrajnie prowadziłoby to do zawarcia umowy jednostronnie zobowiązującej. Przepis art. 473 §1 K.c. odnosi się do rozszerzenia odpowiedzialności strony umowy za nienależyte wykonanie własnego zobowiązania. Natomiast nie dotyczy to przejęcia odpowiedzialności za projektanta i za wady opracowanej przez projektanta dokumentacji (w sytuacji, gdy projektant nie jest stroną danej umowy) i z wykonawcą robót nie wiąże go żaden stosunek umowny, w oparciu o który wykonawca mógłby poszukiwać rekompensaty z tytułu przyjętej wobec inwestora odpowiedzialności za skutki wad projektu.

Przedmiotowy wyrok stanowi kolejne rozstrzygnięcie Krajowej Izby Odwoławczej w kwestii dotyczącej dopuszczalnej treści umowy w sprawie zamówienia publicznego. Rozstrzygniecie o tyle istotne, że po raz kolejny Izba podjęła się oceny wzoru umowy w zakresie dopuszczalnego opisu przedmiotu zamówienia. Izba przyjęła bowiem za niedopuszczalny zapis, zgodnie z którym *nie jest dopuszczalne i możliwe zawarcie... zastrzeżenia, iż umowa obejmuje zakres prac, który obojętnie z jakich przyczyn został pominięty na etapie projektowania,* albowiem tak rozszerzony zakres zamówienia byłby nieważny na podstawie art. 140 ust. 3 pzp. Należy zauważyć, że Krajowa Izba Odwoławcza, przyjmując przedmiotową tezę, postawiła pod znakiem zapytania znaczenie regulacji art. 632. §1 kodeksu cywilnego, zgodnie z którym, jeżeli strony umówiły się o wynagrodzenie ryczałtowe, przyjmujący zamówienie nie może żądać podwyższenia wynagrodzenia, chociażby w czasie zawarcia umowy nie można było przewidzieć rozmiaru lub kosztów prac.

To sformułowanie przepisu w sposób pośredni wskazuje, że dodatkowe, nieprzewidziane pierwotnie prace mieszczą się w zakresie przedmiotu umowy, mimo iż nie zostały wcześniej skalkulowane. Tymczasem teza zawarta w orzeczeniu Krajowej Izby prowadzi do odmiennych wniosków. Jakkolwiek formalnie treść wyroku Krajowej Izby odnosi się do innego aspektu prawnego niż art. 632 k.c., to jednak wbrew pozornym różnicom oba zagadnienia dotyczą tego samego zagadnienia prawnego. Jeśli bowiem zgodnie z art. 632 k.c. przyjmujący zamówienie nie może żądać podwyższenia wynagrodzenia, chociażby w czasie zawarcia umowy nie można było przewidzieć rozmiaru lub kosztów prac, to oznacza, że wykonawca – przyjmujący zamówienie winien: po pierwsze wykonać dodatkowe, nieprzewidziane prace w ramach zawartej umowy, a po drugie – winien wykonać te prace w ramach dotychczasowego wynagrodzenia. Tym samym teza Krajowej Izby wskazująca, że niesprecyzowane prace, jakie będzie trzeba wykonać w ramach ewentualnych prac, nie mieszczą się w przedmiocie zamówienia, wydaje się iść zbyt daleko. Powszechne przyjęcie przedmiotowej tezy oznaczałoby, że zastosowanie przepisów kodeksu cywilnego dotyczących wynagrodzenia ryczałtowego nie znajduje uzasadnienia na gruncie przepisów prawa zamówień publicznych. Powstaje więc pytanie, czy stanowisko takie można by przyjąć, uznając, że ustawa – Prawo zamówień publicznych stanowi lex specialis w stosunku do przepisów kodeksu cywilnego? Teoretyczne postawienie takiej tezy wydaje się stosunkowo łatwe. Jednak w praktyce zagadnienie to jest znacznie bardziej skomplikowane. Nie należy zapominać, że ustawa – Prawo zamówień publicznych reguluje kwestie cywilno-prawne w stosunku do regulacji kodeksu cywilnego jedynie szczątkowo. Po pierwsze przewiduje istotne modyfikacje w zakresie sposobu zawarcia umowy (tryby postępowań), po drugie reguluje kwestie przesłanek zmiany umowy. I wreszcie po trzecie, co w analizowanym orzeczeniu wydaje się najistotniejsze, reguluje problematykę spójności przedmiotu zamówienia z treści umowy w sprawie zamówienia publicznego. O ile sama treść art. 140 ust. 3 pzp, na którą powołała się Krajowa Izba, wydaje się nie budzić specjalnych wątpliwości (umowa podlega unieważnieniu w części wykraczającej poza określenie przedmiotu zamówienia zawartych w specyfikacji istotnych warunków zamówienia), o tyle pojawia się zasadnicze pytanie, czy problem przedstawiony w orzeczeniu Izby rzeczywiście prowadzi do wykroczenia poza określenie przedmiotu zamówienia? Problem bowiem w tym, że czym innym jest nieprecyzyjne określenie przedmiotu zamówienia, a czym innym określenie przedmiotu zamówienia w sposób ogólny. Różnica sprowadza się do dwóch kwestii: w pierwszym przypadku nieprecyzyjne określenie przedmiotu zamówienia skutkuje niemożnością jednoznacznego ustalenia, co winno być zbudowane, a zatem co jest tak naprawdę przedmiotem zamówienia. W drugim przypadku przedmiot zamówienia jako taki jest jednoznacznie opisany (np. wybudowanie budynku), lecz nie do końca jest wiadomym, w jaki sposób winno zostać to zrealizowane, a więc jakie prace okaże się konieczne do osiągnięcia założonego w SIWZ rezultatu. Zastosowanie art. 110 ust. 3 pzp jest możliwe w przypadku, gdy zakres przedmiotu zamówienia jest sprecyzowany w sposób dostateczny, natomiast zamawiający domaga się dodatkowych świadczeń, które poza ten zakres wykraczają. Jeśli natomiast opis przedmiotu zamówienia jest ogólny i zamawiający wymaga, by wykonawca zrealizował wszystkie prace, jakie okażą się konieczne do osiągnięcia celu, jakim jest wybudowanie budynku, pojawia się pytanie nie tyle o naruszenie art. 140 ust. 3 pzp, ale o kwestię naruszenia art. 29 ust. 1 pzp, a zatem przepisu, zgodnie z którym „przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania

i okoliczności mogące mieć wpływ na sporządzenie oferty." Bezspornie bowiem przepisy ustawy – Prawo zamówień publicznych stawiają dalej idące wymagania niż przepisy kodeksu cywilnego w zakresie opisu przedmiotu umowy czy też przedmiotu postępowania przetargowego. W tym więc zakresie stanowią one lex specialis w stosunku przepisów kodeksu. Jednak niedostatecznie przygotowany opis uwarunkowań pozwalających na prawidłowe przegotowanie oferty nie powinien być dokonywany w aspekcie naruszenia art. 140 ust. 3 pzp, lecz w kontekście naruszenia przez zamawiającego art. 29 ust. 1 pzp. Obydwa zarzuty sprowadzają się do zaatakowania zapisów specyfikacji istotnych warunków zamówienia. O ile teza Krajowej Izby prowadzi do nakazania zamawiającemu usunięcia spornych zapisów z opisu przedmiotu umowy, o tyle stanowisko autora niniejszej publikacji prowadziłoby do nakazania zamawiającemu uzupełnienia specyfikacji istotnych warunków zamówienia o niezbędne, brakujące dane. O ile zatem pierwsze rozwiązanie leży w interesie wykonawców (nie muszą oni wykonywać prac dodatkowych i mogą liczyć na ewentualne zamówienia uzupełniające lub dodatkowe, a zamawiający nie osiągnie zamierzonego rezultatu), o tyle druga interpretacja jest korzystniejsza dla zamawiających, nakazując uzupełnienie dokumentu SIWZ o niezbędne dane, które pozwolą wykonawcom zrealizować projekt zgodnie z założeniami zamawiającego. Z tego względu drugie rozwiązanie wydaje się spójniejsze z systemem zamówień publicznych i przepisami dotyczącymi dyscypliny budżetowej.

Proponujemy

WARSZTATY

ODPOWIEDZIALNOŚĆ INSTYTUCJI FINANSOWYCH WZGLĘDEM KONSUMENTA A PRZETWARZANIE DANYCH OSOBOWYCH ZE SZCZEGÓLNYM UWZGLĘDNIENIEM AML I ROZLICZEŃ TRANSGRANICZNYCH

25 stycznia 2011 r., Warszawa

Dlaczego warto wziąć udział w warsztatach?
W przeciwieństwie do większości warsztatów na rynku pozwala zdobyć kompetencję, utrwalić wiedzę i to w spojrzeniu przekrojowym, a nie segmentującym problemy.

Warsztat kierowany jest do: ABI, koordynatorów AML (walki z praniem pieniędzy), osób odpowiedzialnych za budowanie oferty dla linii detalicznych w bankach i instytucjach finansowych oraz prawników.

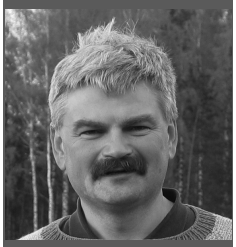
Warsztaty poprowadzi: mecenas Piotr Bodył Szymala.

W PROGRAMIE

- Ryzyko prawne w kontekście odpowiedzialności instytucji finansowych względem konsumenta, ze szczególnym akcentem na nowe regulacje w Dyrektywie PSD.
- Odpowiedzialność instytucji finansowych za nadmiarowe przetwarzanie danych osobowych.
- Odpowiedzialność instytucji finansowej za naruszenie ustawy o ochronie danych osobowych w procesie AML (walki z praniem pieniędzy).

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki



Edwin Bendyk

Julian Assange – Robin Hood społeczeństwa informacyjnego

Julian Assange, twórca serwisu WikiLeaks, coraz bardziej upodabnia się do Robin Hooda. Zabiera tym, co mają i rozdaje tym, którzy nie mają. W epoce feudalnej przedmiotem redystrybucji było złoto grabione przez pachołków monarchy. Dziś cenniejsza od złota jest informacja, więc to ona jest źródłem władzy i potęgi, a wszelkie próby naruszenia monarszego monopolu na gromadzenie informacji budzą gniew. I jak w średniowieczu Robin Hood, tak dziś Assange spodziewać się może jednej kary – banicji i pościgu już do końca życia.

Nie mam zamiaru uromantyczniać postaci twórcy WikiLeaks, serwisu, który od dłuższego czasu sprawia kłopoty, głównie Stanom Zjednoczonym. Nie mogę się jednak też zgodzić ze sporą częścią argumentacji wytaczanej przeciwko Assangemu, postaci coraz bardziej demonizowanej. Ewentualne rozprawienie się z nim w sposób legalny lub po cichu i zamknięcie WikiLeaks nie zmieni problemu zasadniczego. Relacji między informacją i władzą.

Na długo zanim Assange wpadł na pomysł swojego serwisu władze Stanów Zjednoczonych napędzane antyterrorystyczną histerią po 11 września 2001 r. wpadły na pomysł stworzenia Information Awareness Office. Kierownictwo placówki objął admirał John Poindexterr i zaczął rozwijać inicjatywę Total Information Awareness. Jej celem było zbudowanie gigantycznego systemu zbierania i analizy danych na temat mieszkańców USA i wszystkich osób na świecie mogących mieć z USA cokolwiek wspólnego, by w ten sposób wykrywać w zarodku terrorystyczne zagrożenie.

Projekt napotkał ostrą krytykę z wielu perspektyw, od politycznej po techniczną. Skupmy się na tej ostatniej – absurdalność takich pomysłów jak TIA doskonale pokazuje Corry Doctorow w książce „Little Brother" (ukaże się po polsku na początku przyszłego roku). Kanadyjski pisarz science-fiction opisuje USA po drugim ataku terrorystycznym, tym razem na San Francisco. Kongres uchwala Patriot Act II i zaczyna się totalna inwigilacja obywateli oraz tworzenie ich profili na podstawie zgromadzonych danych z cyfrowych śladów. Nie pomaga to w niczym w łapaniu terrorystów, skutecznie natomiast służy utrudnianiu życia rzeszy obywateli, których profile wzbudzają podejrzenie. Cóż, popełniają różne grzeszki, lecz terrorystami nie są.

Doctorow pisze o „paradoksie wyniku fałszywie pozytywnego". Otóż, jeśli metoda analizy jest skuteczna w 99 proc., oznacza to, że spośród 100 osób można jedną fałszywie wskazać jako terrorystę. W mieście milionowym daje to 10 tys. niesłusznie podejrzanych.

Ilu może być terrorystów nawet w najbardziej dla terrorystów sprzyjającym okresie w takim mieście jak np. San Francisco? Dziesięciu? By do nich trafić metodą TIA, na jednego terrorystę trzeba by przebadać tysiąc osób. A podejrzenie o terroryzm to nie byle jakie podejrzenie, oznacza praktycznie zawieszenie wielu praw obywatelskich podejrzanego.

Oczywiście, sytuację taką można tłumaczyć wyższą koniecznością, odpowiedzialnością państwa, etc. Assange poszedł znacznie dalej niż Doctorow ośmieszający bezpieczniacką logikę w swej książce. Twórca WikiLeaks pokazał, że państwo, nawet tak wydawałoby się sprawne i technologicznie zaawansowane jak Stany Zjednoczone, powinno trzymać się z dala od podobnych pomysłów. Oczywiście, Assange nie atakuje polityki inwigilacyjnej służb specjalnych, tylko z lubością ujawnia tajemnice państwe. W ten sposób kompromituje ideę państwowego monopolu na informację – to nie Assange jest niebezpieczny, niebezpieczne są struktury państwa, które w aurze tajności chciałyby gromadzić jak najwięcej informacji o swoich obywatelach oraz tajnych działaniach, a po prostu nie jest w stanie sprostać elementarnym procedurom bezpieczeństwa danych. A co by się stało, gdyby wyciekły informacje gromadzone przez służby bezpieczeństwa na temat swoich obywateli? Czy po aferze WikiLeaks ktokolwiek może zapewnić, że informacje te są rzeczywiście bezpieczne? Być może już jakiś szeregowy Manning Bis kopiuje je na prywatny dysk, by udostępnić np. serwisowi Redwatch?

Eliminacja Assangego nie wyeliminuje więc problemu zasadniczego. Czas na poważnie rozpocząć publiczną dyskusję o zakresie informacji, zwłaszcza informacji tajnych, do jakich ma prawo państwo. Ostatni przeciek depesz dyplomatycznych ujawnia bowiem nie tylko porażające niechlujstwo i brak odpowiedzialności agend państwa, lecz także pokazuje, jak wątła jest tego państwa „inteligencja". Umberto Eco, komentując to wydarzenie, zdziwił się najbardziej banalnością treści dyplomatycznej korespondencji. Większość z depesz nie zawiera niczego nowego w porównaniu do tego, o czym już wcześniej donosiły media. To tylko aura tajności dodaje tym banalnym analizom wagi, lecz nie zwiększa ich poznawczej wartości.

Assange przekłuł więc za jednym zamachem dwa balony, pokazując, że w społeczeństwie informacyjnym informacja w rękach organów państwa nie jest kuteczną bronią, lecz bardzo niebezpiecznym narzędziem. Rozjuszył tym szeryfa z Nottingham, który podobnie jak w oryginalnej opowieści o Robin Hoodzie jest jednocześnie groźny i żałosny. A problem mamy oczywiście wszyscy, nie tylko ów szeryf i wyjęty spod prawa Robin Hood.

Bibliografia prawa nowych technologii informacyjnych styczeń 2009 - styczeń 2010

Wojciech R. Wiewiórowski

Fuglewicz P., Nowak J. S., *Społeczne aspekty informatyki,* Polskie Towarzystwo Informatyczne Oddz. Górnośląski, Katowice 2007 (książka ukazała się w 2009 r.), s. 166

Gacki G., *Prawo do e-głosowania*, „IT w Administracji" 2009/7/13-17

Gałach A., Wójcik R., *Zarządzanie bezpieczeństwem informacji w sektorze publicznym,* C.H.Beck, Warszawa 2009, s. 128

Gałek A., *Wirtualne walne*, „Lex-Press" 2009/8

Ganczar M., *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, CeDeWu.pl, Warszawa 2009, s. 198

Gawrysiak P., *Licencje wolnego oprogramowania*, „Zeszyty Prawnicze UKSW" 2008/1/193-202

Giaro M., *Cywilnoprawne pojęcie pisemności w społeczeństwie informacyjnym*, „Państwo i Prawo" 2009/10

Gienas K., *Czy prawo autorskie tworzy bariery w dostępie do informacji?* „Elektroniczny Biuletyn Naukowy Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE)" 2009/1 http://cbke.prawo.uni.wroc.pl/modules/Publikacje/e-Bulletin/2009_1/Czy_prawo_autorskie.pdf

Gienas K., *Naruszenia praw autorskich w związku z funkcjonowaniem serwisów Web 2.0*, „Radca Prawny" 2009/6/48-53

Gienas K., *Obrót prawami autorskimi w handlu elektronicznym*, „Prawo Nowych Technologii - regulacje, interpretacje, praktyka" 2008/4

Gienas K., *Praktyczne problemy ochrony oprogramowania w świetle prawa autorskiego*, „Przegląd Prawa Handlowego" 2009/6

Gienas K., *Prawne aspekty funkcjonowania bibliotek cyfrowych,* „Palestra" 2009/9-10/88-94

Gienas K., *Prawnoautorskie aspekty miniaturek fotografii (thumbnails) tworzonych przez wyszukiwarki internetowe* [w:] Barta J. [red.] *Zagadnienia prawa własności intelektualnej. Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej. Zeszyt 105*, Wolters Kluwer Warszawa 2009, s. 49-59

Gienas K., *Systemy Digital Rights Manegement w świetle prawa autorskiego*, Oficyna Wolters Kluwer, Warszawa 2008, s. 306

Gienas K., *Sztuka współczesna a prawo autorskie*, „Jurysta" 2008/11-12/19-20

Gienas K., *Utwór multimedialny jako szczególna forma twórczości,* „Edukacja Prawnicza" 2009/11/25-27

Gienas K., *Uwagi o ochronie „utworów technicznych"*, „Monitor Prawniczy" 2009/7/386-390

Gienas K., *Wirtualizacja w prawie,* „Computerworld" 2009/22/22

Gienas K.*, Zabezpieczenia techniczne utworów a dozwolony użytek na tle prawa wspólnotowego i polskiego*, „Europejski Przegląd Sądowy" 2009/12/9-14

Gnitecki R., Kubiszewski P., *ePUAP krok po kroku*, „IT w Administracji" (bezpłatny dodatek) 2009/12, s. 48

Golat R., *Prawo Internetu dla praktyków*, ODDK, Gdańsk 2009, s. 250

Golat R., *Programy komputerowe w prawie cywilny i podatkowym. Zagadnienia praktyczne*, ODDK, Gdańsk 2005, s. 246

Gołaczyński J. [red.], Kowalik-Bańczyk K., Majchrowska A., Świerczyński M., *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Oficyna Wolters Kluwer, Warszawa 2009, s. 200

Gołaczyński J. [red.], Jaroszek A., Szostek D., Sielicki D., Kotecka S., Kaczmarek B., Zalesińska A., Walaszczyk A., Zawiślańska A., Goździaszek Ł., Pęcherzewski P., Skórniak P., Góra D., *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, Oficyna Wolters Kluwer, Warszawa 2009, s. 272

Gołaczyński J., Goździaszek P., *Elektroniczne postępowanie upominawcze* [w:] Barczewski M., Grajewski K., Warylewski J. [red.] *Prawne problemy wykorzystywania nowych technologii w administracji publicznej i w wymiarze sprawiedliwości. III Konferencja WPiA Uniwersytetu Gdańskiego oraz Wolters Kluwer Polska - Gdańsk, 20-21 października 2008,* Wolters Kluwer, Warszawa 2009, s. 13-26

Gołaczyński J., *Informatyzacja postępowania cywilnego w prawie polskim* [w:] Gołaczyński J. [red.] *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, Oficyna Wolters Kluwer, Warszawa 2009, s. 194-252 [rozdział w monografii]

Gołaczyński J., *Informatyzacja postępowania cywilnego w wybranych państwach (Finlandia, Estonia, Niemcy, Austria, Stany Zjednoczone, Wielka Brytania, Francja)* [w:] Gołaczyński J. [red.] *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, Oficyna Wolters Kluwer, Warszawa 2009, s. 36-177 [rozdział w monografii]

Gołaczyński J., *Informatyzacja współpracy sądowej w sprawach cywilnych i handlowych w Unii Europejskiej* [w:] Gołaczyński J. [red.] *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, Oficyna Wolters Kluwer, Warszawa 2009, s. 13-35 [rozdział w monografii]

Zamówienie prenumeraty kwartalnika

„Czas informacji"

WYŚLIJ FAKSEM 22 871 85 56 lub 22 870 69 95

PRENUMERATA NA ROK 2011

Zamawiamy prenumeratę kwartalnika „**Czas Informacji**"

okres trwania prenumeraty (ilość egzemplarzy)	ilość zamawianych prenumerat	**cena**
prenumerata roczna 2011 od numeru 5/2011 - 4 kolejne numery		340 zł +VAT
prenumerata półroczna numer 5/2011 i 6/2011		200 zł +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, Krzysztof Głomb, Xawery Konarski
Tomasz Kulisiewicz, Marcin Maruta, dr Grzegorz Sibiga
Piotr Waglowski, dr Wojciech Wiewiórowski

sekretarz redakcji: Monika Handzelewicz
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

Reklama: Karolina Popek
reklama@czasinformacji.pl

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

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

nakład: 500 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.

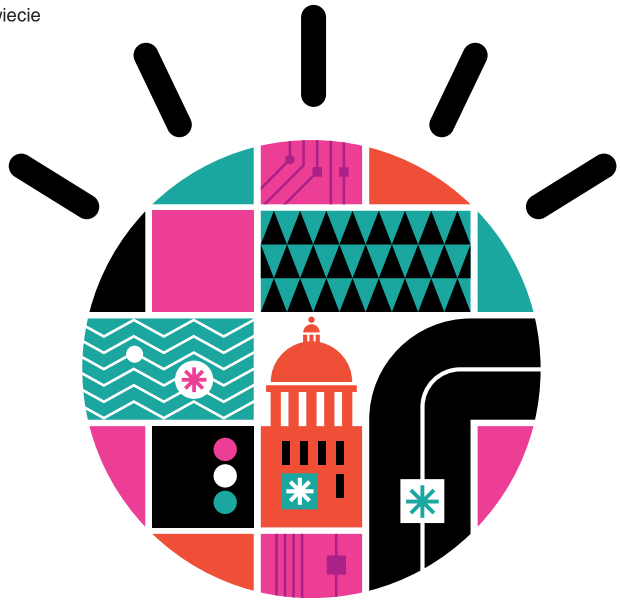
wydawca:

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

rada naukowa:

prof. dr hab. Jacek Gołaczyński
prof. dr hab. Remigiusz Kaszubski
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.



Inteligentna administracja publiczna w mądrzejszym świecie

Samorządy i rząd podejmują próby wdrożenia inteligentnych rozwiązań w transporcie, energetyce, zarządzaniu zasobami wodnymi, telekomunikacji i w innych systemach. Wszystko w celu usprawnienia gospodarki i poprawy życia obywateli. Przy tak ambitnym wyzwaniu nasuwa się pytanie: czy działanie państwa może być oparte na inteligentnych rozwiązaniach?

Rolą inteligentnej administracji publicznej nie jest wyłącznie regulowanie wydajności systemów gospodarczych i społecznych. Jeśli staną się sprawnie działającymi instytucjami wchodzącymi w interakcję z obywatelami, społecznościami lokalnymi i biznesem, będą bodźcem do aktywnego działania na rzecz wzrostu, innowacji i postępu. Jest wiele do zrobienia. Od wyeliminowania skostniałych struktur departamentów, opóźnień w procesach decyzyjnych, aż po wprowadzenie przejrzystości działań i odpowiedzialności. Zmiany już są widoczne, a podejmowane przez rządy na całym świecie starania zaczynają przynosić skutek.

Dzięki współpracy prowadzonej z lokalnymi społecznościami, a także w ramach poszczególnych departamentów, inteligentna administracja odznacza się większą przejrzystością i odpowiedzialnością. Efektywne zarządzanie zasobami daje ludziom dostęp do informacji o decyzjach, które mają bezpośredni wpływ na ich życie.

W Wielkiej Brytanii na przykład, innowacyjna firma Southwest One zapewnia usługi integrujące role kilku urzędów: Rady Hrabstwa Somerset, Rady Miasta Taunton Deane oraz wydziału policji w Avon i Somerset. W Albuquerque rozwiązania Business Intelligence o 2000% podniosły wydajność struktur odpowiedzialnych za miejskie raporty i przygotowywanie informacji kierowanych do obywateli.

Inteligentna administracja publiczna ma bezpośredni wpływ na wzrost gospodarczy. Usprawniając i upraszczając skomplikowane procesy minimalizuje uciążliwość wymogów w zakresie sprawozdawczości, które są szczególnie dokuczliwe dla małych firm. Departament Pracy, Licencji i Regulacji stanu Maryland umożliwił odnawianie licencji zawodowych przez Internet, a w celu weryfikacji osób posiadających ważne licencje udostępnił ich bazę. Belgijski Crossroads Bank for Social Security zautomatyzował 42 stanowiska dla pracowników, co pozwoliło na likwidację 50 różnych papierowych formularzy. W rezultacie w 2008 roku 23 miliony deklaracji ubezpieczeniowych zostało wypełnionych elektronicznie. Dzięki temu belgijskie firmy działają wydajnie i mogą zaoszczędzić do 1,7 miliarda euro rocznie.

Fundamentalnym zadaniem inteligentnej administracji publicznej jest planowanie działań i wdrażanie projektów w pełni skoncentrowanych na obywatelu. Rządy pracują nad usprawnieniem przepływu towarów, zakładają nowe placówki, które świadczą zwiększoną liczbę usług, a także umożliwiają dokonanie najpotrzebniejszych operacji za pośrednictwem Internetu. Tak, jak robi to australijski Centrelink, który wspomaga rząd w świadczeniu usług związanych z ważnymi kwestiami w życiu obywateli: małżeństwem, narodzinami dziecka czy opieką nad ludźmi w starszym wieku. Japońskie miasto Kioto stworzyło stronę internetową, która umożliwia każdemu, niezależnie od języka, którym się posługuje, dostęp do informacji miejskiej.

Zdarzają się przypadki, w których prowadzone działania decydują o życiu lub śmierci. W czasie wielkich pożarów w Kalifornii władze zdecydowały się na wykorzystanie portalu społecznościowego Twitter oraz serwisu Mapy Google. Za ich pośrednictwem (osoby pozbawione prądu używały telefonów komórkowych) informowano obywateli o akcjach ewakuacyjnych i ratunkowych, a także na bieżąco przedstawiano aktualną sytuację w regionach zagrożonych żywiołem.

W czerwcu 2009 firma IBM zorganizowała w Berlinie pierwszą z serii konferencję Inteligentne Miasta, podczas której wizjonerzy i liderzy z całego świata dzielili się pomysłami dotyczącymi inteligentnej opieki zdrowotnej, inteligentnego zarządzania ruchem, inteligentnego zarządzania zasobami wodnymi, inteligentnego zarządzania energią itd. Za najbardziej obiecujące innowacje uznano te, które bezpośrednio wspierają działanie administracji publicznej. Razem zbudujmy mądrzejszy świat.

Jak zacząć, dowiesz się na: **ibm.com**/swiat/pl/rzad

IBM, logo IBM, ibm.com są zarejestrowanymi znakami towarowymi lub znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach. Aktualna lista znaków towarowych IBM dostępna jest na www.ibm.com/legal/copytrade.shtml.
© Copyright IBM Corporation 2010. Wszelkie prawa zastrzeżone.